An International ICT R&D Journal Sponsored by ZTE Corporation

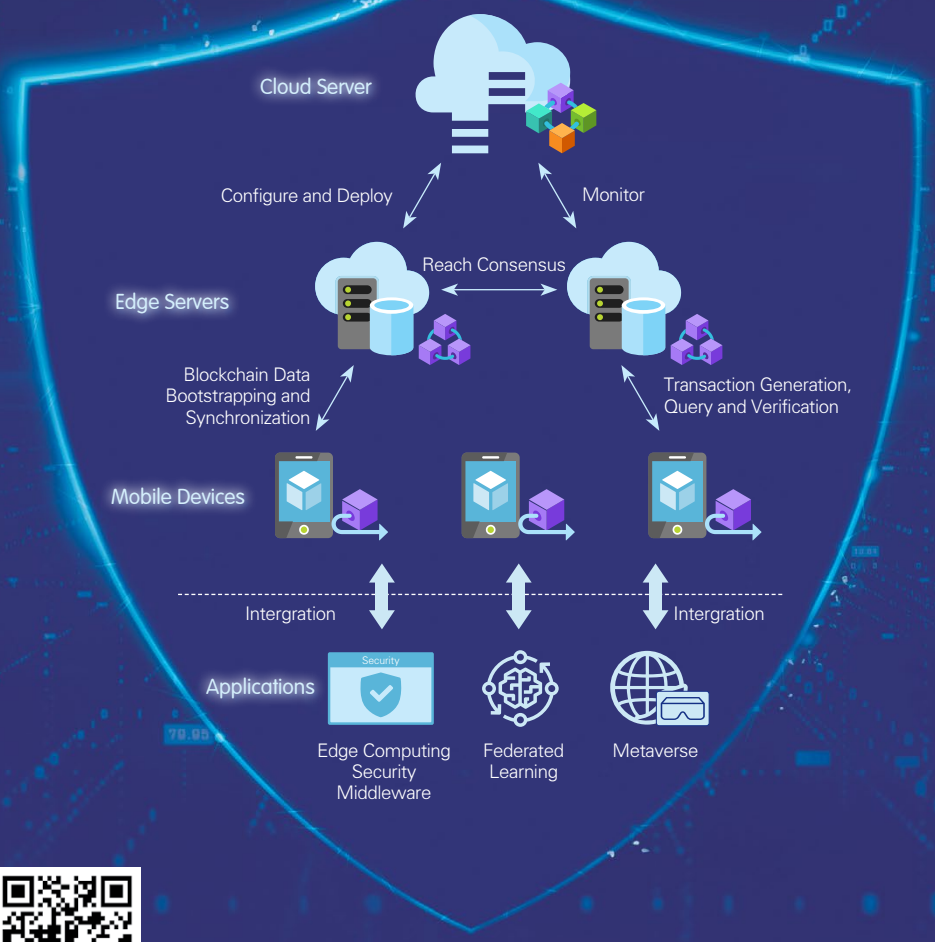
ISSN 1673-5188
CN 34-1294/TN

ZTE COMMUNICATIONS

中兴通讯技术(英文版)

December 2022, Vol. 20 No. 4

Special Topic: Wireless Communication and Its Security: Challenges and Solutions



ISSN 1673-5188
12>
9 771673 518222

The 9th Editorial Board of ZTE Communications

CONTENTS

ZTE COMMUNICATIONS
December 2022 Vol. 20 No. 4 (Issue 81)

Special Topic ▶ Wireless Communication and Its Security: Challenges and Solutions

Review ▶

CONTENTS

ZTE COMMUNICATIONS
December 2022 Vol. 20 No. 4 (Issue 81)

Research Paper

Roundup

Serial parameters: CN 34–1294/TN*2003*q*16*115*en*P*¥ 20.00*2200*13* 2022-12

REN Kui, WANG Zhibo

Editorial: Special Topic on Wireless Communication and Its Security: Challenges and Solutions

Guest Editors >>>

REN Kui is a professor and the Dean of School of Cyber Science and Technology at Zhejiang University (ZJU), China, where he also directs the Institute of Cyber Science and Technology. Before that, he was SUNY Empire Innovation Professor at State University of New York at Buffalo, USA. He received his PhD degree in electrical and computer engineering from Worcester Polytechnic Institute, USA. Prof. REN's current research interests include data security, IoT security, AI security, and privacy. He received many recognitions including Guohua Distinguished Scholar Award of ZJU, IEEE CISTC Technical Recognition Award, SUNY Chancellor's Research Excellence Award, Sigma Xi Research Excellence Award, NSF CAREER Award, etc. Prof. REN has published papers extensively in peer-reviewed journals and conferences and received the Test-of-Time Paper Award from IEEE INFOCOM and many Best Paper Awards, including ACM MobiSys, IEEE ICDCS, IEEE ICNP, IEEE Globecom, ACM/IEEE IWQoS, etc. His h-index is 87, with a total citation exceeding 41 000 according to Google Scholar. Prof. REN is a Fellow of ACM and IEEE. He is a frequent reviewer for funding agencies internationally and serves on the editorial boards of many IEEE and ACM journals. Among others, he currently serves as Chair of SIGSAC of ACM China Council, a member of ACM ASIACCS steering committee, and a member of S&T Committee of Ministry of Education of China.

WANG Zhibo is a professor of the School of Cyber Science and Technology at Zhejiang University, China. He received his BE degree in automation from Zhejiang University in 2007, and his PhD degree from the Department of Electrical Engineering and Computer Science from University of Tennessee, Knoxville, USA in 2014. His research interests include Internet of Things, AI security, edge intelligence and security. He has published more than 100 papers in top-tier journals and conferences, such as *ToN*, *JSAC*, *CCS*, Mobicom, S&P, INFOCOM, ICCV and CVPR. He serves as an editor of *IEEE Transactions on Cloud Computing*, and the TPC member of many flagship conferences including INFOCOM, WWW, ICDCS, AAAI, KDD and IWQoS. He is the recipient of the National Science Foundation for Excellent Young Scholars, the best student paper award of FUSION 2019, and the outstanding paper award of IEEE HPCC 2019. He is a senior member of IEEE and CCF and a member of ACM.

Recent years have witnessed the phenomenal growth of wireless technologies and applications on a massively large scale since the fifth generation (5G) wireless technologies were proposed as a key propellent to meet the increasing demands of future networks. Going further, the sixth generation (6G) wireless technologies have already been under preparation. However, wireless communication technologies are faced with new opportunities as well as challenges.

On the one hand, emerging technologies provide fundamental issues including higher system capacity, higher data rate, lower latency, higher security, and improved quality of service (QoS), which enables the application of wireless communication technologies in the Internet of Things (IoT) scenarios such as industry, automobile, drone, port, and subway. On the other hand, these new technologies will also introduce new vulnerabilities, which lead to new threats to the security of wireless communication systems. Concerns about security have triggered research in this domain to build up a highly effective safeguard.

The goal of this special issue is to stimulate discussions around open problems of security issues in wireless communication. Focusing on wireless communication and its security, this special issue receives both theoretical and application-based contributions which demonstrate both the challenges and solutions with the rapid development of wireless technologies and applications.

The call-for-papers of this special issue have brought excellent submissions in both quality and quantity. After two-round reviews, five excellent papers have been selected for publica-

DOI:10.12142/ZTECOM.202204001
Citation: K. Ren and Z. B. Wang, "Editorial: wireless communication and its security: challenges and solutions," *ZTE Communications*, vol. 20, no. 4, pp. 1–2, Dec. 2022. doi: 10.12142/ZTECOM.202204001.

tion in this special issue which is organized as follows. We assembled five papers with a balanced selection between theoretical research and practical engineering: three of them carry out comprehensive surveys and the other two propose novel mechanisms. The topics addressed in this special issue cover a broad range, including security in edge blockchains, data collection with local differential privacy (LDP) for mobile devices, security technologies in 6G, federated learning (FL) for secure 6G, and physical layer security for mmWave communication. The detailed information is as follows.

The first paper titled "Security in Edge Blockchains: Attacks and Countermeasures" is the first survey that discusses the attacks and countermeasures of edge blockchains. In this paper, the authors summarize the three-layer architecture of edge blockchains (i. e. blockchain management, blockchain consensus, and blockchain lightweight client) and point out the inherent vulnerabilities of edge blockchains. On this basis, they also summarize the security issues caused by the deployment of vulnerable edge blockchain devices and networks. To be specific, seven specific attacks on edge blockchain components and the corresponding countermeasures are concretely demonstrated in detail. At last, the authors discuss the future directions for researchers to design and implement secure edge blockchains.

Titled "Utility-Improved Key-Value Data Collection with Local Differential Privacy for Mobile Devices", the second paper proposes a utility-improved data collection framework with LDP to deal with key-value data generated by mobile devices. This paper focuses on the problem of limited utility caused by excessive privacy protections and achieves personalized privacy protection by dividing the key-value data into sensitive and non-sensitive parts. The authors validate the mechanism based on two real datasets and prove in experiments that the proposed mechanism can provide better utility and simultaneously protect privacy.

The third paper titled "Key Intrinsic Security Technologies in 6G Networks" provides a general overview of 6G intrinsic security in the industry. In this paper, the authors not only review key security technologies in 5G and security technology enhancement in 5G-Advanced evolution but also analyze the vision and requirements of 6G intrinsic security. Although the technical systems and standards of 6G intrinsic security have not yet reached a unified understanding in the industry, this paper still pays close attention to the disruptive impact that intrinsic 6G security may bring and preliminarily focuses on the key technologies of 6G intrinsic security, including the massive equipment connection security technology, physical layer security technology, and blockchain technology.

Aiming to solve the problem that limited energy restricts the popularization of UAV-enabled FL applications, the fourth paper titled "Air-Ground Integrated Low-energy Federated Learning for Secure 6G Communications" proposes an air-ground integrated low-energy federated learning framework. In this paper, the authors optimize the deployment of unmanned aerial vehicles (UAVs) with a deep Q-network approach to minimize the overall energy consumption of the application communication. This paper shows in the experiment that the proposed method can reduce energy consumption while maintaining the quality of the FL model.

The fifth paper titled "Physical Layer Security for MmWave Communications: Challenges and Solutions" presents a comprehensive overview of physical layer security (PLS) issues in mmWave Communication. In this paper, the theoretical foundation of PLS and the most typical PLS techniques are briefly introduced together with the typical PLS performance metrics secrecy rate, and outrage probability. Several schemes based on these techniques are discussed in detail to compare their advantages and constraints in the mmWave environment and to point out the future direction for researchers.

As demonstrated above, we have briefly introduced the main content of this special issue and given a general overview of the five papers collected in the issue. We would like to express our sincere gratitude to all the authors for their valuable contributions. In the meanwhile, we also want to show our appreciation to all the reviewers for their timely and insightful comments on the submissions. This special issue would not be possible without their help and collaboration. We hope that this special issue can serve as an informative and significant collection to lay a solid foundation for future research works about wireless communication and its security.

Security in Edge Blockchains: Attacks and Countermeasures

CAO Yinfeng, CAO Jiannong, WANG Yuqin, WANG Kaile, LIU Xun
(Department of Computing, The Hong Kong Polytechnic University, Hong Kong SAR 852, China)

DOI: 10.12142/ZTECOM.202204002
https: //kns.cnki.net/kcms/detail/34.1294.TN.20221111.1503.004.html, Published online: November 14, 2022
Manuscript received: 2022-09-16

Abstract: Edge blockchains, the blockchains running on edge computing infrastructures, have attracted a lot of attention in recent years. Thanks to data privacy, scalable computing resources, and distributed topology nature of edge computing, edge blockchains are considered promising solutions to facilitating future blockchain applications. However, edge blockchains face unique security issues caused by the deployment of vulnerable edge devices and networks, including supply chain attacks and insecure consensus offloading, which are mostly not well studied in previous literature. This paper is the first survey that discusses the attacks and countermeasures of edge blockchains. We first summarize the three-layer architecture of edge blockchains: blockchain management, blockchain consensus, and blockchain lightweight client. We then describe seven specific attacks on edge blockchain components and discuss the countermeasures. At last, we provide future research directions on securing edge blockchains. This survey will act as a guideline for researchers and developers to design and implement secure edge blockchains.

Keywords: blockchain; edge computing; security; survey

Citation (IEEE Format): Y. F. Cao, J. N. Cao, Y. Q. Wang, et al., "Security in edge blockchains: attacks and countermeasures," *ZTE Communications*, vol. 20, no. 4, pp. 3 - 14, Dec. 2022. doi: 10.12142/ZTECOM.202204002.

1 Introduction

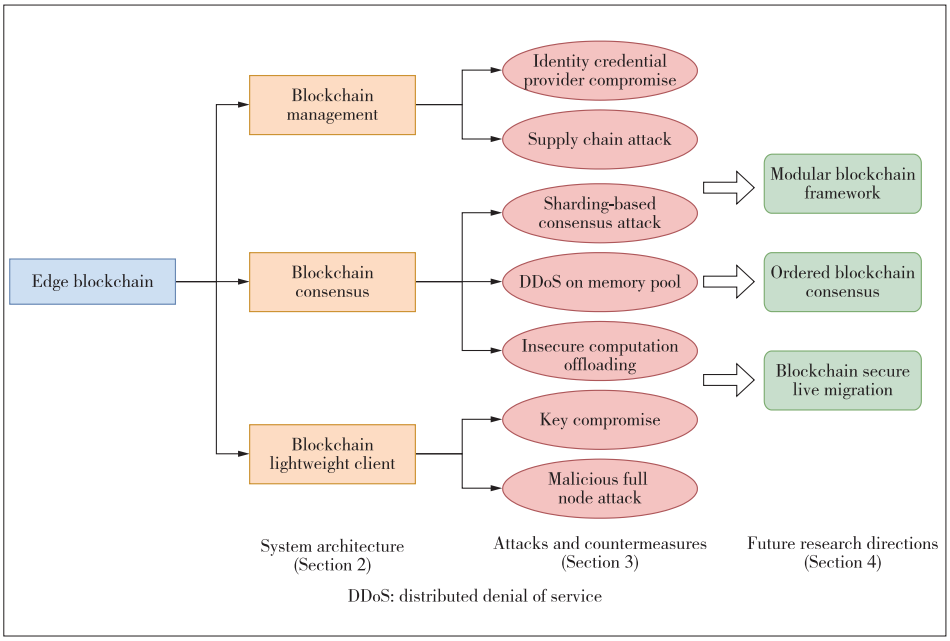
Edge computing has developed rapidly in recent years and raised wide interest from both industry and academia[1]. As a new computing model, edge computing extends cloud computing to the network edge and utilizes rich computation, storage, and networking resources on large-scale distributed devices. In edge computing, the optimization techniques on resource allocation and scheduling are extensively studied, enabling computation tasks to be divided and offloaded to the optimal edge devices according to different constraints. As a result, edge computing plays an important role in maintaining low latency, supporting heterogeneity, and improving applications' quality of service (QoS), such as virtual reality, distributed machine learning, wireless sensing, and robotics.

At the same time, the concept of edge blockchains has also been proposed. It refers to the blockchains deployed on edge computing infrastructures. Edge blockchains inherit favorable features from edge computing, like data privacy, scalable computing resources, and distributed topology. Thereby, edge blockchains are more suitable for large-scale applications than traditional blockchains hosted on the cloud or on-premise machines. For example, applications like blockchain-based federated learning, blockchain-based security middleware in the Internet of things (IoT), and metaverse essentially rely on edge blockchains[2 - 4].

However, the security in edge blockchains is not well understood in existing works. Specifically, in the works alleged "blockchain-based edge computing"[2, 5 - 6], the edge blockchains are typically assumed to be secure and trusted. On the contrary, in real implementation, it is challenging to protect and keep the edge blockchain networks functioning in edge environments for many practical reasons, like vulnerable low-end edge devices, unstable networks, and centralized provider corruption. Thus, it is desired to analyze the critical security issues facing edge blockchains.

To fill this gap, we investigate and evaluate the security in edge blockchains systematically. Our survey essentially differs from previous blockchain security surveys and provides more practical details[7 - 9]. As shown in Fig. 1, we start by describing the motivation and summarizing the system architecture and applications of edge blockchains to provide readers with a brief overview in Section 2. Then in Section 3, we discuss the core components of an edge blockchain, e.g., blockchain management, blockchain consensus, and blockchain

This work was supported by the Research Institute for Artificial Intelligence of Things, The Hong Kong Polytechnic University, HK RGC Collaborative Research Fund (CRF) under Grant No. C2004-21GF.



▲ **Figure 1. Structure of this survey**

lightweight clients, in terms of potential attacks and countermeasures. Finally, we point out the challenging issues and future directions for securing edge blockchains in Section 4.

2 Overview of Edge Blockchains

2.1 Motivations

In recent years, the blockchain technology and its applications have received extensive attention from the research community and industry[10]. Blockchain is a decentralized ledger-based Byzantine fault tolerant (BFT) consensus system. Under a bounded number of adversary environments, blockchain nodes can reach chain-linked agreements on incoming transactions with traceability, immutability, and transparency. Besides, the consensus procedure does not rely on a trusted third party (TTP), making blockchain systems trustless and hard to tamper with.

Nowadays, the blockchain technology is still facing several bottlenecks, thus seriously restricting its application scenarios and making it inaccessible in the real world. Among them, blockchain's decentralization, scalability, and security are considered the most significant and recognized as a trilemma[11]. Generally speaking, existing works cannot well satisfy all three properties together.

• Decentralization. Making blockchain run without trust depends on a small group of centralized actors with specialized rights.

• Scalability. Processing numerous transactions in the network simultaneously with low latency.

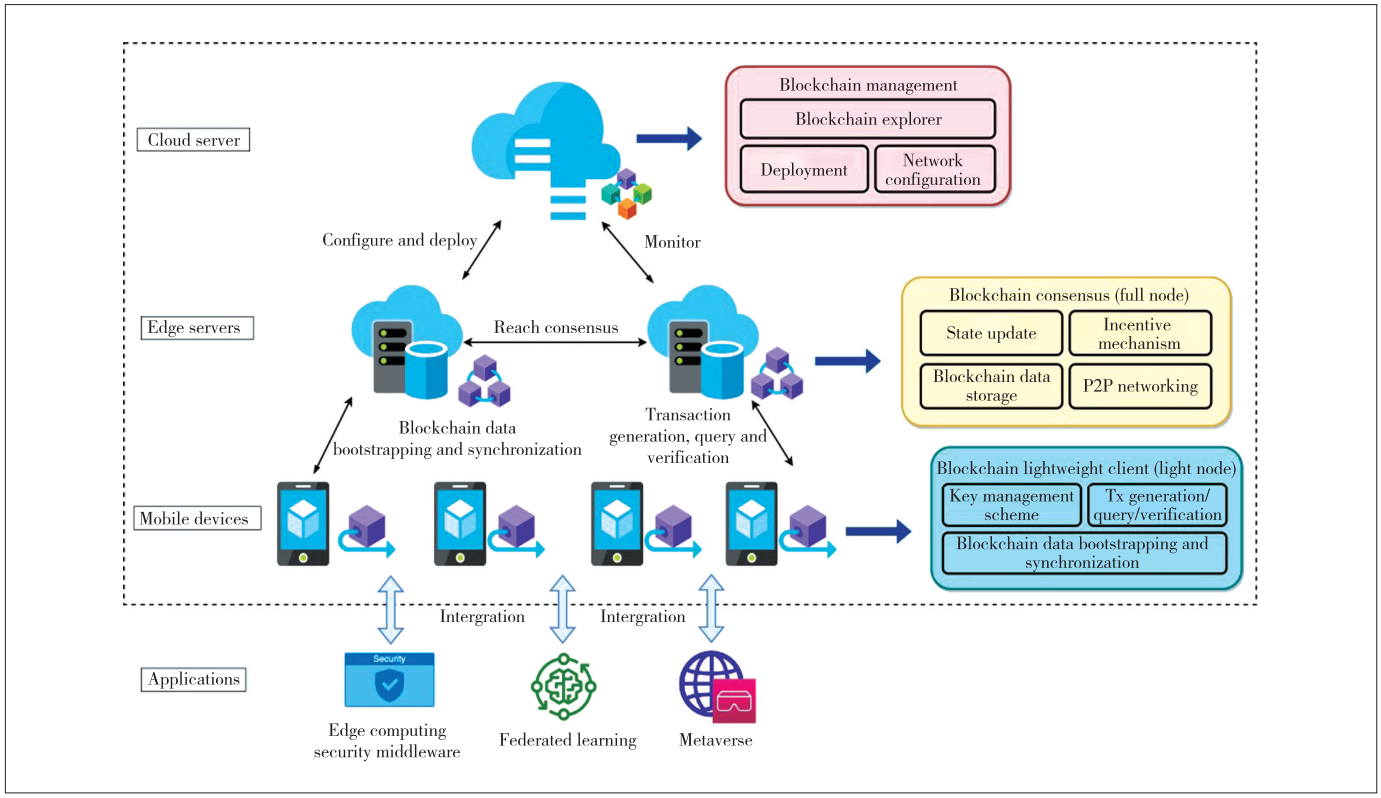
• Security. Resisting a certain percentage of Byzantine nodes that can conduct arbitrary adversary behaviors.

Although blockchain theoretical advancement keeps appearing, some researchers have begun to focus on infrastructure-level solutions to improving blockchain performance. Edge computing shares a similar system architecture with blockchain and can provide the needed computing resources for blockchain systems, which can be a promising option[12–13]. By employing edge computing as blockchain infrastructures to realize edge blockchains, blockchain trilemma can be further resolved simultaneously in terms of the above-mentioned properties. In particular, 1) for keeping decentralization, edge computing physically guarantees the hierarchical and decentralized architecture of blockchain. Edge computing has a layered architecture with a large-scale distributed edge device network to keep the on-device blockchain nodes from centralization. 2) For improving scalability, edge computing has rich computation, storage, and networking resources accomplished with automatic optimization of resource allocation and scheduling. These resources can be utilized by blockchain to realize a large-scale blockchain network. 3) For enhancing security, edge computing provides permission environments with data privacy guarantees, reducing Byzantine nodes' risks and thus relaxing the blockchain security assumption for better performance. In conclusion, edge blockchains can offer better decentralization, scalability, and security with lower latency for applications than normal blockchains deployed on public cloud environments or distributed individual devices.

2.2 Architecture

To comprehensively analyze and understand edge blockchains, we first present their architecture, components, and functionalities. Based on the existing literature and platforms, we find that the edge blockchain system architecture typically follows a three-layer pattern including a cloud server layer, an edge server layer, and a mobile device layer, with different blockchain components and functionalities, as shown in Fig. 2. To be specific, we conclude each layer's components and functionalities as follows:

• Cloud server layer: blockchain network management. The cloud server in edge computing has knowledge of network specifications and attached edge devices connectivity. Therefore, the cloud servers are typically set to configure, deploy, and monitor the edge blockchain networks to reduce management costs.



▲**Figure 2. System architecture of a typical edge blockchain which follows a three-layer pattern with different blockchain components and functionalities**

• Edge server layer: blockchain consensus for incoming transactions. Edge servers are close to the data source and provide more computing resources than mobile devices. Thus, it is reasonable to deploy blockchain full nodes at this layer to have sufficient resource support for updating ledger states and incentive nodes, storing blockchain data, and communicating with other nodes.

• Mobile device layer: blockchain lightweight client (light node) for transaction operations (generation, query, and verification). Edge applications interact with blockchain through numerous transactions from large-scale mobile devices. Deploying the interfaces for transaction operations and maintaining partial blockchain data (blockchain data bootstrapping and synchronization) at this layer can significantly reduce the latency and improve QoS. Besides, the key management schemes for protecting signing keys are also integrated to support transaction operations.

2.3 Applications

Edge blockchains feature high QoS and security guarantees in edge environments. In the current stage, edge blockchain solutions are application-specific, which means that they are typically embedded with applications to improve their performance. Here we summarize the three representative types as follows.

• Security middleware for edge computing[2, 14 – 15]. Edge blockchains can be utilized as security middleware to tackle security issues in the edge computing infrastructure. For instance, detecting unstable or low-performance edge devices and designing strategies to avoid using these devices are challenging research issues in the edge resources optimization area. To address these issues, reputation systems with incentive mechanisms can be built upon edge blockchains. They record the status of edge devices and provide trusted reference information for strategy design and decision making in edge optimization algorithms. Besides, other efforts like secure data sharing methods, authentication schemes, and control systems based on edge blockchains are also proposed to enhance edge computing security.

• Edge-based federated learning[3, 16 – 17]. Edge-based federated learning is a distributed machine learning scheme that collects closed-source data to train global models in a privacy-preserving and personalized manner. However, due to the self-voluntary ways to contribute to model updates, malicious behaviors may occur and affect the quality of global models, e.g., poison attacks. To this end, blockchain is proposed to provide failure tolerance ability, malicious behavior detection, and incentive mechanisms for securing and boosting federated learning.

• Metaverse[4, 18 – 19]. Metaverse is a trendy edge application aiming to build a virtual world with immersive experience. Edge-based VR and blockchain-based economic systems are

two critical techniques for the metaverse. Edge blockchains provide lower latency, better decentralization, and better personal data privacy than blockchains in the cloud, thus making the metaverse scalable and trusted.

2.4 Challenges

Deploying blockchains at the edge will bring extra challenges, especially from security aspects. On the one hand, vulnerable edge devices, unstable network conditions, and physical accessibility expose many attack interfaces on edge blockchains to adversaries. On the other hand, designing sufficient and efficient security solutions on resource-constrained edge devices is challenging.

For example, efficient and secure key management is challenging in edge blockchains. Traditional methods like using custodial wallet software require considerable computing resources on edge devices, which are also insecure since external attackers can access the devices. Ideal solutions should be lightweight but also can prevent such kinds of attacks. Another example can be the task-offloading feature of edge computing. Offloading tasks to arbitrary nodes in blockchain networks is risky since the blockchain nodes do not trust each other. Malicious nodes could collect the offloaded tasks to gain illegal benefits and launch attacks by forging identities.

3 Attacks and Countermeasures

In this section, we describe the critical security issues and attacks of edge blockchains in each layer. We also present and analyze the state-of-the-art countermeasures for reference in each subsection. We summarize these contents with brief descriptions in Table 1.

3.1 Blockchain Management

Blockchain management aims to configure, deploy, and monitor edge blockchain networks. In edge blockchains, such procedures are typically implemented by centralized service providers, e.g., Blockchain-as-a-Service (BaaS) platforms, due to cost-effective concerns[20-23]. These platforms provide the tools or software development kits (SDKs) to define the blockchain network in client software, access control, deployment methods, etc. For example, AWS Blockchain Template is a tool for configuring cloud-based Ethereum[24] or hyperledger fabric networks[25].

3.1.1 Identity Credential Provider Compromise

In edge blockchains or other consortium blockchains, identity credentials are required to authenticate the participation legality of users or organizations. Identity credentials can be certificate authority/public key infrastructure (CA/PKI) certificates and public/private key pairs, which are generated and assigned to blockchain nodes. These credentials specify the vote right, communication channels, and data access. For popular frameworks in edge blockchains, like Hyperledger Fabric, X.509 CA-based Membership Service Provider (MSP) is responsible for participation identity management; in IBM blockchain, blockchain identities are associated with Azure Active Directory, a unified access control mechanism in Azure Cloud[26]. In edge blockchain literature, similar mechanisms are also applied to authenticate edge devices that run blockchain nodes[27-29]. However, due to the centralized nature of this procedure, blockchain management procedures in edge blockchains are vulnerable to many attacks, even to traditional cyber attacks.

Although nodes themselves keep the credentials, the issue, update, and revoke operations are typically performed by centralized providers (e.g., blockchains using CA/PKI), which is risky to adversaries. Existing works show that if such providers are compromised, many other level attacks may be conducted and further damage the blockchain networks[30-31]. Malicious providers can manipulate and subvert identity management by making legal credentials invalid, refusing to issue, and even issuing illegal credentials to launch a Sybil attack. Eventually, malicious providers will control the full blockchain networks and could launch arbitrary attacks.

State-of-the-Art countermeasures focus on making blockchain identity management decentralized and transparent. In Geth (Proof of Authority consensus mode) and Tendermint, new validators are elected to have vote rights by original validators, which are initially from the hard-coded genesis block[32-33]. This way increases the difficulty for adversaries to compromise since it is equivalent to tamper the entire blockchain. The substantial verification, update, and revocation operations are also on-chain. Some works extend similar ideas and construct new identity blockchains, which are specifically designed for managing identities on other blockchains[34-36].

▼Table 1. Attacks and countermeasures on edge blockchain components

Components	Attacks	Countermeasures	Related Works
Blockchain management	Identity credential provider compromise	Decentralization and transparent identity management	Refs. [30-36]
	Supply chain attack	Threat detection system and automated code analysis	Refs. [39-48]
Blockchain consensus	Sharding-based consensus attack	Atomic commit and order-fairness consensus	Refs. [59, 62-65]
	DDoS on a memory pool	Increase of the costs of malicious transactions	Refs. [66-72]
	Insecure computation offloading	Secure multi-party computation	Refs. [13, 76-79]
Blockchain lightweight client	Key compromise	New recovery operations on blockchain and robust key management	Refs. [86-92]
	Malicious full node	Reputation system and game-theoretic approach	Refs. [82, 93, 95]

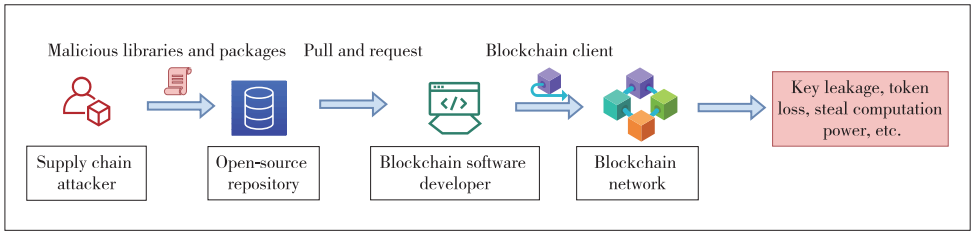
DDoS: distributed denial of service

3.1.2 Supply Chain Attack

In practice, blockchain nodes are implemented by blockchain client software like Geth[32] and Bitcoin Core[37]. These blockchain clients are developed or orchestrated from multiple libraries, packages, and dependencies, providing consensus, blockchain data storage, APIs, wallet functionalities, etc. Due to the nature of decentralization and trust concerns, their blockchain components are usually supplied by open-source projects. For example, Geth involves Web3.js library to provide APIs for blockchain, and smart contract interactions[38].

A supply chain attack (e.g., a third-party attack, a value-chain attack, or a backdoor breach) aims to inject malware or malicious hardware by hiding in upstream supplied system components to damage software. Historic attacks were mainly launched by suppliers in traditional information and communications (ICT) technology areas. However, recent accidents show that it can also affect blockchain since blockchain projects are mostly built by open-source dependencies to increase transparency. As shown in Fig. 3, attackers may upload predesigned malicious libraries and packages to open-source repositories by compromising blockchain managers, and then deliver them to blockchain software developers. Users will be compromised when they run crafted blockchain software like wallets[39]. Likewise, there is so-called mining malware that pretends to be normal browser plugins, executable programs, and miner tools, stealing the computation power of devices to obtain benefits[40]. In edge blockchains, such attacks are noteworthy since the blockchain clients running on edge devices are provided and maintained in a similar way. Even worse, edge blockchain networks are dynamic, and edge devices frequently join and leave the networks by installing the blockchain client software from different sources. These processes expose additional attack interfaces for supply chain attacks.

The preventive solutions try to eliminate the risks from both the upstream components supplier side and the device side[41–43]. On the one hand, researchers and developer communities use various security mechanisms to assert the projects hosted in open-source repositories. Many scoring and threat detection and analysis systems like OpenSSF Metrics and OpenSSF Scorecard are built to provide an overview of the security status for developer reference[44–45]. They calculate the scores according to the code maintenance status, vulnerability existence, and programming specification as metrics. On the other hand, the automated code analysis project, and services for detecting blockchain software and smart contracts are emerging[46–48]. They can check sensitive codes and functions like money transfer, deploying contracts, and making signatures by semantics formalization. This way is more active than the former but may bring huge additional development costs.



▲ **Figure 3. Supply chain attacks in blockchain: attackers can inject malicious scripts into libraries and packages to damage blockchain networks**

3.2 Blockchain Consensus

Consensus is a core component of blockchain systems that refers to the continuous agreement protocol on blocks/transactions among multiple blockchain nodes. Blockchain consensus can reach an agreement and update node states under the existence of Byzantine nodes. Byzantine nodes can behave arbitrarily to achieve malicious targets except by breaking cryptography primitives, and they can also cooperate. For example, Byzantine nodes can keep silent to pretend to crash or corporately send fake messages to foolish honest nodes. Currently, there are mainly two types of blockchain consensus: the Nakamoto style and the traditional BFT style. Nakamoto style consensus includes Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA)[37, 49, 32], etc, which rely on external validity rules like mining power, stocks, and authority to reach agreements. BFT style consensus purely concerns the votes on broadcasted values, like practical Byzantine fault tolerance (PBFT), HotStuff, and Honey badger[50–52]. Besides, blockchain consensus is also highly related to hardware, blockchain data structure, networking algorithms, and blockchain lightweight client design[53–54].

Consensus is a vulnerable component due to the complexity and non-deterministic procedures. Existing attacks focus on breaking two consensus features as follows:

• Consistency (safety): If any two honest nodes in the blockchain network maintain two blockchains, they should be on the same chain.

• Liveness: If the honest nodes receive a transaction, the transaction should be included in all blockchains maintained by honest nodes after the consensus procedure.

Literally speaking, if the attack breaks consistency, there will be unexpected blockchain forks or double spending events. If the attack breaks liveness, the consensus will halt and no agreement has been reached for incoming transactions.

3.2.1 Sharding-Based Consensus Attack

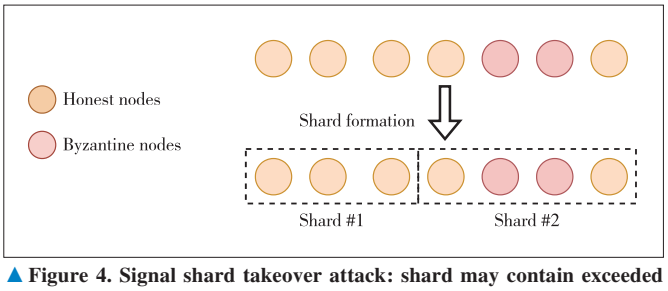
In edge blockchain networks, the numerous edge devices require the blockchain consensus to be scalable to maintain high Transaction per Second (TPS). However, the theoretical limitations make the communication complexity hard to be sub-quadratic (BFT style consensus). Sharding is a celebrated and preferred technique to deal with scal-

ability issues in edge computing[55 - 57]. Generally speaking, sharding splits the blockchain networks into several pieces, where each piece individually deals with transaction consensus and data storage. This way can reduce the communication to nearly linear as well as the storage cost[58 - 59].

However, in practice, the transaction may be related to multiple shards, which brings extra security issues. For example, in the unspent transaction output (UTXO) model, the outputs of a transaction must be equal to (or smaller than) its input. If the inputs come from different shards, nodes in one shard cannot verify the validity of this transaction for they have no knowledge of other shards. In the account/balance model, the transaction is still probably from different shards when the shard number increases. Thus, a cross-shard consensus protocol as the coordinator is needed to deal with this situation. The typical solution is using the atomic commit (AC) protocol to implement this coordinator. However, existing works show that existing coordinators are vulnerable to various attacks, including transaction forging attacks, message withholding attacks, publish-revert attacks, and replay attacks, which can break the liveness and safety of sharding-based consensus[60 - 61]. Generally speaking, these attacks leverage the knowledge difference and message delay during the AC process, further cheating or isolating the honest shard chains.

Another fundamental security issue of sharding-based consensus is committee selection for shard formation. Traditional blockchain consensus assumes that the number of Byzantine nodes is under a certain percentage (security boundary), e.g., 50% for PoW and 33% for PBFT. When the blockchain network is splitted into reveal shards, the number of Byzantine nodes may exceed security boundaries in particular single shards. This issue is also called a signal shard takeover attack. For example, a blockchain network runs PBFT with seven nodes, where five nodes are honest and two nodes are Byzantine. If the network manager randomly selects committees in shards as shown in Fig.4, the second shard will be compromised since there are more than 33% Byzantine nodes. This situation comes from the uncertainty of Byzantine nodes, making managers hard to decide which node is honest.

For the first security issue, researchers try to design new AC protocols that have extra features like termination. It requires all involved shards on a cross-shard transaction to eventually decide on it. Besides, in real implementation, a "garbage collection" is used for dealing with uncompleted cross-shard transactions[62 - 63]. However, such works are specific to their blockchain systems, and cannot be directly applied to other blockchains. Traditional non-blocking atomic commit (NC-AC) is also needed to be significantly modified to be compatible with the blockchain system[64]. For the second security issue, the public verifiable randomness sources and countermeasures for active adversaries are introduced. The randomness sources provide the reference for shard formation. Being unpredictable and uniform can minimize the probability of selecting excessive Byzantine nodes in shards[59]. For active adversaries, which corrupt nodes after shard formation, there are also mechanisms to limit their abilities of malicious voting[65].



▲ **Figure 4. Signal shard takeover attack: shard may contain exceeded numbers of Byzantine nodes after committee selection**

3.2.2 DDoS on Memory Pool

A memory pool in a blockchain system is a caching area for receiving, verifying, and ranking incoming transactions before consensus. The memory pool is the first step for processing transactions. Thus its performance will be the bottleneck of TPS. For example, in Bitcoin, the miner first checks the validity of transactions in terms of signatures, UTXOs, formats, etc. Then the transactions will be put in a memory pool waiting to be mined into blocks[37]. The ranking of transactions depends on the mining fee attached to the transactions. High mining fees stimulate miners to mine transactions in a high rank, making them early confirmed. Besides, the relay fees are also required for miners relaying the transactions to each other. Other blockchain systems are designed with similar philosophies. The differences lay in the requirement for fees. In edge blockchains, the fees are omitted and the ranking is decided by the arriving time or other parameters[66 - 68].

Recent studies show that the DDoS attack can significantly affect the memory pool, prohibiting normal transactions from being confirmed[69 - 72]. Attackers first allocate multiple Sybil accounts with enough balances for paying transaction fees and relay fees. Then they initiate a large number of unconfirmed transactions that transfer money to each other to several blockchain nodes in a short time period. When the transaction arrival rate is larger than the confirmation rate of blockchain consensus, there will be a transaction backlog, and the blockchain nodes have to increase the size of memory pools eventually. Although the consensus processes as normal, the actual TPS for normal transactions will be decreased. Attackers try to maximize the number of these transactions in the memory pool but do not want them to be confirmed since it will cost more fees. Therefore, these transactions typically only have relay fees to reduce the attack costs. In edge blockchains, conducting such attacks is more possible than doing this in cryptocurrency. The reasons include that the transactions in edge blockchains are application-specific and may not need to pay money, and the corrupted edge devices can easily generate a large number of transactions.

Existing solutions focus on increasing the costs of launching

such attacks to further prevent them from happening. Researchers set additional constraints to filter the transactions that are likely to be malicious. The constraints consider whether the parents transactions are confirmed previously and therefore pay mining fees[69 - 72], or set the relay fees dynamically increasing when the memory pool size is too large[70]. These solutions only care about cryptocurrency systems, but such mechanisms may not be feasible in edge blockchain networks.

3.2.3 Insecure Computation Offloading

Computation offloading is a unique technique in edge computing. It transfers resource-intensive computational tasks to other nearby devices by dividing and optimizing tasks. In this way, resource-constrained devices reduce the burden and are capable of dealing with complex tasks. Computation offloading is extensively studied and applied in edge computing, and many edge applications essentially rely on it, such as distributed machine learning, video surveillance, and VR/AR[73 - 75]. In edge blockchains, offloading is also utilized for reducing the blockchain consensus costs on mobile devices[76 - 77, 13]. Researchers model the consensus tasks and edge compute services pricing as Stackelberg games to improve the system throughput and optimize the accessibility of the blockchain network.

However, such offloading methods cannot well meet the security requirements of blockchain. Even though the consensus tolerates a certain percentage of Byzantine nodes, malicious edge computing service providers (e.g., corrupted edge servers) are still possible to break the threshold. Specifically, malicious providers can execute other nodes' consensus tasks and act like them simultaneously. This behavior is equivalent to corrupting honest nodes in the blockchain since malicious providers obtain free computation power paid by honest nodes, which is definitely out of the BFT model definition. Consequently, the percentage of Byzantine nodes in blockchain networks will increase and finally become overwhelming.

Secure multiparty computation (SMPC) and outsourced computing can be promising solutions to addressing these issues. SMPC is a cryptographic technique that enables multiple parties to jointly compute tasks without revealing their own private inputs and outputs[78]. With the development advancing, its efficiency is becoming acceptable for edge and IoT devices. Combining the SMPC with blockchain and offloading can prevent malicious computing service providers from manipulating outsourced blockchain tasks[79].

3.3 Blockchain Lightweight Client

Blockchain lightweight client is another critical building block of a blockchain system, especially for developing edge blockchains. It contains transaction generation, query, and verification schemes with blockchain data bootstrapping and synchronization procedures. In practice, a blockchain lightweight client typically does not directly participate in consensus like blockchain full nodes do to save computation, storage, and networking resources. Therefore, a blockchain lightweight client is suitable to be integrated into mobile applications and run on resource-constrained devices in edge networks[80, 12, 81]. Specifically, a lightweight client contains the following functionalities[82]:

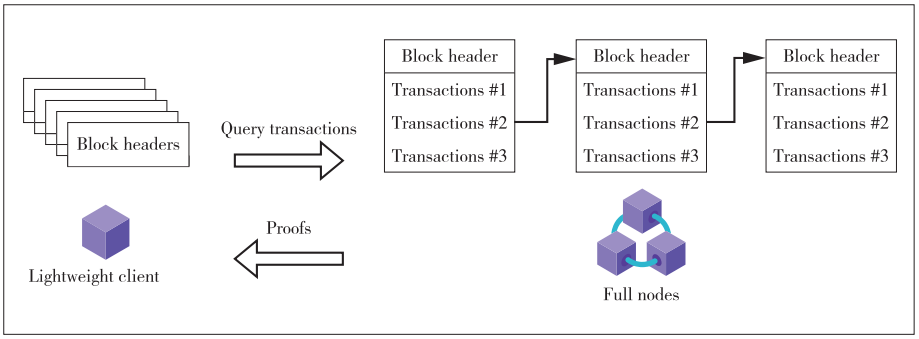
• Bootstrapping and synchronization: Given a blockchain genesis block or file, the client should synchronize all the state metadata from full nodes (e.g., all block headers) with bootstrapping proofs. When the full nodes update their states (e.g., new blocks), the client should also synchronize it and update state metadata with synchronization proofs.

• Transaction generation, query, and verification: Clients should generate valid transactions for full node updating its states. After that, a client can query the existence of submitted transactions confirmed in blockchain states and verify the result proofs.

Bitcoin simplified payment verification (SPV) is believed to be the first implementation of a lightweight client[37]. As shown in Fig. 5, it only stores the block headers of the longest chain locally, which is initially downloaded and periodically synchronized from nearby full nodes. Upon receiving transaction verification requests, lightweight clients retrieve the blocks that contain the transactions with corresponding Merkle branches for verifying their existence.

3.3.1 Key Compromise

Key management refers to the schemes of generating, updating, using, and deleting cryptographic keys. In the blockchain context, the keys are employed for identifying edge nodes, signing transactions, and encrypting data. Due to the decentralized nature, such keys are usually kept by the user sides, and no managers are responsible for them. In well-established blockchain wallets like MetaMask[83], the key files are stored locally with mnemonic phrase encoding and password/biometric authentication protection. Users need to input the correct password or biometric information to unlock the key inside the



▲ **Figure 5. Bitcoin simplified payment verification (SPV): a lightweight blockchain client for Bitcoin, which only stores the block headers to reduce costs**

wallet to sign transactions.

Although many elaborately crafted key management schemes are designed and implemented for high security and usability, the keys are still extremely vulnerable to software bugs, hardware failure, and even simple human errors[84 - 85]. Key compromise is still a significant security issue that remains unsolved. To add insult to injury, these issues are more likely to happen in edge blockchains since edge devices (like IoT devices) are mostly low-end in hardware and software with few sufficient security mechanism. Besides, the devices are also physically accessible and controllable. Attackers can attack the devices through various interfaces existing on edge devices and applications. As a result, the keys managed in edge devices are highly risky of being theft, lost, and broken.

Existing efforts to enhance the security and usability of blockchain key management are twofold. First, from the blockchain side, many schemes are proposed to replace or supplement the transaction verification in blockchains to realize key compromise protection[86 - 89]. The general idea is to allow new operations to claim new keys or recall transactions for users who are theft or lose their keys accidentally. This way serves as remedial measures for unlucky users but creates additional difficulties and lowers the blockchain TPS for normal users. From the device side, advanced cryptography primitives are applied to minimize the risk of key compromise. Group signature, threshold signature, and hierarchical key derivation are used to construct robust key management schemes[90 - 92]. These schemes can provide additional rescue solutions, present informative network typology, and set flexible access control in edge blockchain key management.

3.3.2 Malicious Full Node Attack

The purpose of a malicious full node is to influence light nodes that interact with the blockchain network via a light protocol and inject adversarial blocks. Light clients have poor bandwidth and limited storage capacity. To improve the efficiency of light clients, firstly, they do not store complete ledger information; secondly, they generally verify the validity of the chain within a limited scope. For example, in SPV, light clients validate the chain only through block headers and request Merkle from full nodes on demand to verify that a specific transaction is valid. Incomplete validation makes it possible for malicious full nodes to inject adversary chains into light clients.

Malicious full nodes can create forks in the blockchain. A fork consists of blocks with block headers that satisfy block header validation and adversarial status. Honest full nodes will immediately reject these adversary blocks because they fail in state validation. However, since light clients can only perform header validation, but not state validation, the fork is also a normal chain from the perspective of light clients. If the adversary chain contains more work than the honest chain, according to the longest chain rule, a light client will accept the adversary chain. In addition, a patient adversary willing to wait (days or months) can obtain a high probability of successfully injecting a forged state into a light client. Considering a node, such as an IoT node with a limited battery, is operating in a duty cycle mode and periodically active, the longer the interval between two active states, the higher the adversary probability of successful state injection. Moreover, the adversary also has the probability of having a successful adversarial chain at any random point in time, so it may also successfully convince a light node[93].

Existing solutions focus on building reputation systems and using game-theoretic approaches to secure the light client from malicious full nodes. In reputation systems, miners are ranked by their consensus contribution[94]. Light clients cache the recent blocks from miners with good reputations to securely download blockchain data. Game-theoretic approaches use smart contracts as a trusted arbiter to deal with the client and a set of full nodes[95]. Participants need to deposit some funds on the arbiter contract as collateral. Malicious behaviors like sending fake blocks will be plenty by costing the deposited funds, thus encouraging the full node to provide block data honestly.

4 Future Research Directions

In this section, we point out some specific future research directions that are related to the security of edge blockchains. We envision these directions being significant in future edge blockchains.

4.1 Modular Blockchain Framework

Existing frameworks in edge blockchains only support one or multiple fixed components such as consensus algorithms, databases, and communication protocols. This fact significantly decreases the resistance to supply chain attacks and amplifies the attack revenue. Imagine if some widely used consensus algorithms or other components are suddenly found vulnerable, all the blockchain systems with those components will be risky and hard to be fixed in a short time. This is because the interfaces, data structures, and algorithms among these components are highly coherent. Developers do not have much flexibility to adjust them when security issues occur. Besides, the valuable on-chain assets and data make blockchain systems hard to be readily updated as normal software.

In our previous work, PolyChain proposes a modular blockchain framework, where the main components are fully pluggable and changeable[96]. We divide the blockchain into four components: application component, consensus component, storage component, and network component. This provides much flexibility when facing attacks. In PolyChain, developers can replace vulnerable components with low costs to avoid potential damage. Other works with similar philosophy also emerged recently, and better solutions to blockchain modularization remain to be explored[97 - 98].

4.2 Ordered Blockchain Consensus

Some transactions have inherent relationships and dependencies in certain applications. For example, in Decentralized Finance (DeFi) and Central Bank Digital Currencies (CBDC) [99 – 100], manipulating transaction confirmation orders can launch financial attacks on smart contracts[101]. This is because when users need to submit a batch of transactions to these applications, their exact confirmation order is not guaranteed in most existing consensus algorithms. Miners usually include transactions in blocks according to the attached fees. Many blockchain financial infrastructures are also deployed in edge environments, such as Bitcoin ATMs and cryptocurrency wallets. Therefore, we need to guarantee the security of transaction confirmation orders in edge blockchains.

One easy and safe way is submitting transactions to consensus one by one and waiting for confirmation, but this is inefficient when there are a large number of pending transactions. New efforts on consensus need to provide security guarantees on transaction orders while keeping high efficiency. This is challenging since it basically requires designing extra consensus rounds expressly agreeing on transaction orders.

4.3 Blockchain Secure Live Migration

In edge blockchains, multiple small-size blockchain networks may exist for specific user groups and applications. However, accessing these size-constrained blockchains can be difficult for they are only deployed in a limited number of edge devices with poor network connectivity. Simply scaling the blockchain network by setting up new nodes is a naive solution, but this will occupy other device computing resources and interrupt blockchain consensus, causing further security concerns for the blockchain network, like congestion.

Live migration is a technique that transfers services or processes across computing infrastructures without disrupting normal operations. It has been extensively studied in cloud computing for load balancing, resource management, server consolidation, predictive maintenance, and QoS improvement[102]. Such a technique is also beneficial to edge blockchains. It can reduce the latency of accessing the above-mentioned size-constrained blockchain with low costs and high QoS. Existing migration techniques only focus on container or process architecture, which may not perform well on blockchain since they do not consider the specific architecture of blockchain systems. More effective and secure solutions can be adopted by separately migrating different components of the blockchain system, such as blockchain data and memory pool transactions while keeping consensus running for security[103].

5 Conclusions

Integrating blockchain with edge computing is a valuable landscape in future wireless communication. Many efforts have been made to make blockchain securely run in adversarial environment. However, the features of edge computing bring new security issues, which have not been extensively studied and addressed in previous literature. Many attacks on edge blockchains components are not well understood and prevented. Through this study, we comprehensively review the security of edge blockchains in terms of attacks, countermeasures, and future directions. We envision this survey acting as a security guideline for designing and developing edge blockchains.

References

[1] CAO K Y, LIU Y F, MENG G J, et al. An overview on edge computing research [J]. IEEE access, 8: 85714 – 85728. DOI: 10.1109/ACCESS.2020.2991734
[2] HE Y, WANG Y H, QIU C, et al. Blockchain-based edge computing resource allocation in IoT: a deep reinforcement learning approach [J]. IEEE Internet of Things journal, 2021, 8(4): 2226 – 2237. DOI: 10.1109/JIOT.2020.3035437
[3] LU Y L, HUANG X H, DAI Y Y, et al. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT [J]. IEEE transactions on industrial informatics, 2020, 16(6): 4177 – 4186. DOI: 10.1109/TII.2019.2942190
[4] XU M R, NIYATO D, KANG J W, et al. Wireless edge-empowered metaverse: a learning-based incentive mechanism for virtual reality [C]//IEEE International Conference on Communications. IEEE, 2022: 5220 – 5225. DOI: 10.1109/ICC45855.2022.9838736
[5] SHENG H, WANG S, ZHANG Y, et al. Near-online tracking with co-occurrence constraints in blockchain-based edge computing [J]. IEEE Internet of Things journal, 2021, 8(4): 2193 – 2207. DOI: 10.1109/JIOT.2020.3035415
[6] RAHMAN M A, HOSSAIN M S, LOUKAS G, et al. Blockchain-based mobile edge computing framework for secure therapy applications [J]. IEEE access, 2018, 6: 72469 – 72478
[7] LI X Q, JIANG P, CHEN T, et al. A survey on the security of blockchain systems [J]. Future generation computer systems, 2020, 107: 841 – 853. DOI: 10.1016/j.future.2017.08.020
[8] TAYLOR P J, DARGAHI T, DEHGHANTANHA A, et al. A systematic literature review of blockchain cyber security [J]. Digital communications and networks, 2020, 6(2): 147 – 156. DOI: 10.1016/j.dcan.2019.01.005
[9] ZHANG R, XUE R, LIU L. Security and privacy on blockchain [J]. ACM computing surveys, 2020, 52(3): 1 – 34. DOI: 10.1145/3316481
[10] MONRAT A A, SCHELÉN O, ANDERSSON K. A survey of blockchain from the perspectives of applications, challenges, and opportunities [J]. IEEE access, 7: 117134 – 117151. DOI: 10.1109/ACCESS.2019.2936094
[11] ZHOU Q H, HUANG H W, ZHENG Z B, et al. Solutions to scalability of blockchain: a survey [J]. IEEE access, 8: 16440 – 16455. DOI: 10.1109/ACCESS.020.2967218
[12] YANG R Z, YU F R, SI P B, et al. Integrated blockchain and edge computing systems: a survey, some research issues and challenges [J]. IEEE communications surveys & tutorials, 2019, 21(2): 1508 – 1532. DOI: 10.1109/COMST.2019.2894727
[13] XIONG Z H, ZHANG Y, NIYATO D, et al. When mobile blockchain meets edge computing [J]. IEEE communications magazine, 2018, 56(8): 33 – 39. DOI: 10.1109/MCOM.2018.1701095
[14] MA Z F, WANG X C, JAIN D K, et al. A blockchain-based trusted data management scheme in edge computing [J]. IEEE transactions on industrial informatics, 2020, 16(3): 2013 – 2021. DOI: 10.1109/TII.2019.2933482
[15] KANG J W, YU R, HUANG X M, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks [J]. IEEE Internet of Things journal, 2019, 6(3): 4660 – 4670. DOI: 10.1109/JIOT.2018.2875542
[16] NGUYEN D C, DING M, PHAM Q V, et al. Federated learning meets blockchain in edge computing: opportunities and challenges [J]. IEEE Internet of

Things journal, 2021, 8(16): 12806 – 12825. DOI: 10.1109/jiot.2021.3072611
[17] MAJEED U, HONG C S. FLchain: federated learning via MEC-enabled blockchain network [C]//Proceedings of 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2019: 1 – 4. DOI: 10.23919/apnoms.2019.8892848
[18] KIM W S. Edge computing server deployment technique for cloud VR-based multi-user metaverse content [J]. Journal of Korea multimedia society, 2021: 24(8): 1090 – 1100
[19] DHELIM S, KECHADI T, CHEN L, et al. Edge-enabled metaverse: The convergence of metaverse and mobile edge computing [EB/OL]. (2022-04-13) [2022-09-11]. https://arxiv.org/abs/2205.02764
[20] IBM. IBM blockchain service [EB/OL]. [2022-09-11]. https://www.ibm.com/blockchain
[21] AWS. AWS blockchain-as-a-service [EB/OL]. [2022-09-11]. https://aws.amazon.com/cn/blockchain
[22] ALIBABA. Alibaba blockchain solutions [EB/OL]. [2022-09-11]. https://cn.aliyun.com/solution/blockchain/tbes
[23] ORACLE. Oracle blockchain service [EB/OL]. [2022-09-11]. https://www.oracle.com/hk/blockchain/
[24] WOOD G. Ethereum: a secure decentralised generalised transaction ledger [J]. Computer science, 2014
[25] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains [C]//Proceedings of the Thirteenth EuroSys Conference. ACM, 2018: 1 – 15. DOI: 10.1145/3190508.3190538
[26] AZURE M. Azure blockchain service [EB/OL]. [2022-09-11]. https://learn.microsoft.com/en-us/azure/confidential-ledger/
[27] WANG J, WU L B, CHOO K K R, et al. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure [J]. IEEE transactions on industrial informatics, 2020, 16(3): 1984 – 1992. DOI: 10.1109/TII.2019.2936278
[28] ZHANG X D, LI R, CUI B. A security architecture of VANET based on blockchain and mobile edge computing [C]//Proceedings of 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018: 258 – 259. DOI: 10.1109/HOTICN.2018.8605952
[29] CHENG G J, CHEN Y, DENG S G, et al. A blockchain-based mutual authentication scheme for collaborative edge computing [J]. IEEE transactions on computational social systems, 2022, 9(1): 146 – 158. DOI: 10.1109/TCSS.2021.3056540
[30] BROTSIS S, KOLOKOTRONIS N, LIMNIOTIS K, et al. On the security and privacy of hyperledger fabric: challenges and open issues [J]. IEEE world congress on services (SERVICES), 2020: 197 – 204
[31] DABHOLKAR A, SARASWAT V. Ripping the fabric: attacks and mitigations on hyperledger fabric [C]//International Conference on Applications and Techniques in Information Security. IEEE, 2019: 300 – 311
[32] DOCUMENTATION G. How to run a light node with geth [EB/OL]. [2022-09-11]. https://ethereum.org/en/developers/tutorials/run-light-node-geth/
[33] CASON D, FYNN E, MILOSEVIC N, et al. The design, architecture and performance of the tendermint blockchain network [C]//The 40th International Symposium on Reliable Distributed Systems (SRDS). IEEE, 2021: 23 – 33. DOI: 10.1109/SRDS53918.2021.00012
[34] CUI Z H, XUE F, ZHANG S Q, et al. A hybrid BlockChain-based identity authentication scheme for multi-WSN [J]. IEEE transactions on services computing, 2020, 13(2): 241 – 251. DOI: 10.1109/TSC.2020.2964537
[35] ZHU S, CAI Z, HU H, et al. Zkcrowd: a hybrid blockchain-based crowdsourcing platform [J]. IEEE transactions on industrial informatics, 2019: 16(6): 4196 – 4205
[36] TONG W, DONG X W, SHEN Y L, et al. CHChain: secure and parallel crowdsourcing driven by hybrid blockchain [J]. Future generation computer systems, 2022, 131: 279 – 291. DOI: 10.1016/j.future.2022.01.023
[37] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2022-09-11]. https://nakamotoinstitute.org/bitcoin/
[38] CHAINSAFE. Ethereum javascript API [EB/OL]. [2022-09-11]. https://github.com/ChainSafe/web3.js
[39] REES K. Thousands of solana wallets drained in multimillion-dollar exploit [EB/OL]. [2022-09-16]. https://www.makeuseof.com/solana-wallets-drained-in-attack/
[40] LIU J Q, ZHAO Z H, CUI X, et al. A novel approach for detecting browser-based silent miner [C]//IEEE Third International Conference on Data Science in Cyberspace. IEEE, 2018: 490 – 497. DOI: 10.1109/DSC.2018.00079
[41] RAO V V, MARSHAL R, GOBINATH K. The IoT supply chain attack trends-vulnerabilities and preventive measures [C]//Proceedings of 2021 4th International Conference on Security and Privacy (ISEA-ISAP). IEEE, 2021: 1 – 4. DOI: 10.1109/ISEA-ISAP54304.2021.9689704
[42] FAROOQ M J, ZHU Q Y. IoT supply chain security: overview, challenges, and the road ahead [EB/OL]. [2022-09-16]. https://www.researchgate.net/publication/334658033_IoT_Supply_Chain_Security_Overview_Challenges_and_the_Road_Ahead
[43] ZAHAN N, ZIMMERMANN T, GODEFROID P, et al. What are weak links in the NPM supply chain? [C]//IEEE/ACM 44th International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP). IEEE, 2022: 331 – 340
[44] OPENSSF. Open source security metrics [EB/OL]. [2022-09-16]. https://metrics.openssf.org
[45] OSSF. Security scorecards-security health metrics for open source [EB/OL]. [2022-09-16].https://hacker-gadgets.com/blog/2021/07/10/security-scorecards-security-health-metrics-for-open-source/
[46] SLOWMIST. A blockchain security firm established [EB/OL]. (2018-01-20) [2022-09-16]. https://www.slowmist.com/#services
[47] TANG X, ZHOU K, CHENG J, et al. The vulnerabilities in smart contracts: a survey [C]//International Conference on Artificial Intelligence and Security. ICAIS, 2021: 177 – 190
[48] JIANG B, LIU Y, CHAN W K. ContractFuzzer: fuzzing smart contracts for vulnerability detection [C]//Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering. ACM, 2018: 259 – 269. DOI: 10.1145/3238147.3238177
[49] CAO B, ZHANG Z H, FENG D Q, et al. Performance analysis and comparison of PoW, PoS and DAG based blockchains [J]. Digital communications and networks, 2020, 6(4): 480 – 485. DOI: 10.1016/j.dcan.2019.12.001
[50] CASTRO M, LISKOV B. Practical byzantine fault tolerance [EB/OL]. [2022-09-11]. https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/
[51] YIN M F, MALKHI D, REITER M K, et al. HotStuff: BFT consensus with linearity and responsiveness [C]//Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing. ACM, 2019: 347 – 356. DOI: 0.1145/3293611.3331591
[52] MILLER A, XIA Y, CROMAN K, et al. The honey badger of BFT protocols [C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 31 – 42. DOI: 10.1145/2976749.2978399
[53] SANKAR L S, SINDHU M, SETHUMADHAVAN M. Survey of consensus protocols on blockchain applications [C]//The 4th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2017: 1 – 5. DOI: 10.1109/ICACCS.2017.8014672
[54] NGUYEN G T, KIM K. A survey about consensus algorithms used in blockchain [J]. Journal of Information processing systems, 2018, 14(1): 101 – 128. DOI:10.3745/JIPS.01.0024
[55] FENG L, YANG Z X, GUO S Y, et al. Two-layered blockchain architecture for federated learning over the mobile edge network [J]. IEEE network, 2022, 36(1): 45 – 51. DOI: 10.1109/MNET.011.2000339
[56] ASHERALIEVA A, NIYATO D. Reputation-based coalition formation for secure self-organized and scalable sharding in IoT blockchains with mobile-edge computing [J]. IEEE Internet of Things journal, 2020, 7(12): 11830 – 11850. DOI: 10.1109/JIOT.2020.3002969
[57] YUAN S J, LI J, LIANG J H, et al. Sharding for blockchain based mobile edge computing system: a deep reinforcement learning approach [C]//Proceedings of 2021 IEEE Global Communications Conference. IEEE, 2021: 1 – 6. DOI: 10.1109/GLOBECOM46510.2021.9685883
[58] HONG Z C, GUO S, LI P, et al. Pyramid: A layered sharding blockchain system [C]//IEEE Conference on Computer Communications. IEEE, 2021: 1 – 10. DOI: 10.1109/INFOCOM42981.2021.9488747
[59] WANG G, SHI Z J, NIXON M, et al. SoK: sharding on blockchain [C]//Proceedings of the 1st ACM Conference on Advances in Financial Technologies: ACM, 2019: 41 – 61. DOI: 10.1145/3318041.3355457
[60] SONNINO A, BANO S, AL-BASSAM M, et al. Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers [C]//IEEE Euro-

pean Symposium on Security and Privacy (EuroS&P). IEEE, 2020: 294 – 308. DOI: 10.1109/EuroSP48549.2020.00026
[61] HAN R, YU J, LIN H, et al. On the security and performance of blockchain sharding [EB/OL]. [2022-09-11]. https://www. semanticscholar. org/paper/On-the-Security-and-Performance-of-Blockchain-Han-Yu/e7c5c3811973e26333f766012029d3069657871f
[62] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. OmniLedger: a secure, scale-out, decentralized ledger via sharding [C]//IEEE Symposium on Security and Privacy. IEEE, 2018: 583 – 598. DOI: 10.1109/SP.2018.000-5
[63] ZAMANI M, MOVAHEDI M, RAYKOVA M. RapidChain: scaling blockchain via full sharding [C]//ACM SIGSAC Conference on Computer and Communications Security. CCS, 2018: 931 – 948. DOI: 10.1145/3243734.3243853
[64] GUPTA S, SADOGHI M. Efficient and non-blocking agreement protocols [J]. Distributed and parallel databases, 2020, 38(2): 287 – 333. https://doi. org/10.1007/s10619-019-07267-w
[65] ABRAHAM I, CHAN T H H, DOLEV D, et al. Communication complexity of byzantine agreement, revisited [EB/OL]. [2022-09-11]. https://arxiv. org/abs/1805.03391
[66] GUPTA Y, SHOREY R, KULKARNI D, et al. The applicability of blockchain in the Internet of Things [C]//The 10th International Conference on Communication Systems & Networks (COMSNETS). IEEE, 2018: 561 – 564. DOI: 10.1109/COMSNETS.2018.8328273
[67] SHRESTHA R, BAJRACHARYA R, NAM S Y. Blockchain-based message dissemination in VANET [C]//IEEE 3rd International Conference on Computing, Communication and Security. IEEE, 2018: 161 – 166. DOI: 10.1109/CCCS.2018.8586828
[68] ZHANG P Y, PANG X, KUMAR N, et al. A reliable data-transmission mechanism using blockchain in edge computing scenarios [J]. IEEE Internet of Things journal, 2022, 9(16): 14228 – 14236. DOI: 10.1109/JIOT.2020.3021457
[69] SAAD M, THAI M T, MOHAISEN A. POSTER: deterring DDoS attacks on blockchain-based cryptocurrencies through mempool optimization [C]//Proceedings of the 2018 on Asia Conference on Computer and Communications Security. IEEE, 2018: 809 – 811. DOI: 10.1145/3196494.3201584
[70] LUO S C, SANG Y P, SONG M Y, et al. Preventing DDoS attacks on bitcoin memory pool by the dynamic fee threshold mechanism [C]//Parallel and distributed computing, applications and technologies, 2021: 172 – 184. DOI: 10.1007/978-3-030-69244-5_15
[71] SAAD M, NJILLA L, KAMHOUA C, et al. Mempool optimization for defending against DDoS attacks in PoW-based blockchain systems [C]//IEEE International Conference on Blockchain and Cryptocurrency. IEEE, 2019: 285 – 292. DOI: 10.1109/BLOC.2019.8751476
[72] SAAD M, KIM J, NYANG D, et al. Contra: mechanisms for countering Spam attacks on blockchain's memory pools [J]. Journal of network and computer applications, 2021, 179: 102971. DOI: 10.1016/j.jnca.2020.102971
[73] GUO Y H, ZHAO R, LAI S W, et al. Distributed machine learning for multiuser mobile edge computing systems [J]. IEEE journal of selected topics in signal processing, 2022, 16(3): 460 – 473. DOI: 10.1109/JSTSP.2022.3140660
[74] CHEN J G, LI K L, DENG Q Y, et al. Distributed deep learning model for intelligent video surveillance systems with edge computing [J]. IEEE transactions on industrial informatics, 2019, 99: 1. DOI: 10.1109/TII.2019.2909473
[75] SCHMOLL R S, PANDI S, BRAUN P J, et al. Demonstration of VR/AR offloading to mobile edge cloud for low latency 5G gaming application [C]//The 15th IEEE Annual Consumer Communications & Networking Conference. IEEE, 2018: 1 – 3. DOI: 10.1109/CCNC.2018.8319323
[76] ZUO Y, JIN S, ZHANG S, et al. Blockchain storage and computation offloading for cooperative mobile-edge computing [J]. IEEE Internet of Things Journal, 2021, 8(11): 9084 – 9098
[77] NGUYEN D C, PATHIRANA P N, DING M, et al. Secure computation offloading in blockchain based IoT networks with deep reinforcement learning [J]. Transactions on network science and engineering, 2021, 8(4): 3192 – 3208
[78] ZHAO C, ZHAO S N, ZHAO M H, et al. Secure Multi-Party Computation: Theory, practice and applications [J]. Information sciences, 2019, 476: 357 – 372. DOI: 10.1016/j.ins.2018.10.024
[79] ZHONG H, SANG Y, ZHANG Y, et al. Secure multi-party computation on blockchain: an overview [C]//International Symposium on Parallel Architectures, Algorithms and Programming. Springer, 2019: 452 – 460. DOI: 10.1007/978-981-15-2767-8_40
[80] ASWATHY S U, TYAGI A K, KUMARI S. The future of edge computing with blockchain technology: Possibility of threats, opportunities, and challenges [M]//Recent trends in blockchain for information systems security and privacy. Boca Raton: CRC Press, 2021: 261 – 292. DOI: 10.1201/9781003139737-18
[81] LU Y S, ZHANG J N, QI Y, et al. Accelerating at the edge: a storage-elastic blockchain for latency-sensitive vehicular edge computing [J]. IEEE transactions on intelligent transportation systems, 2022, 23(8): 11862 – 11876. DOI: 10.1109/TITS.2021.3108052
[82] CHATZIGIANNIS P, BALDIMTSI F, CHALKIAS K. Sok: blockchain light clients [C]//International Conference on Financial Cryptography and Data Security Cryptology. Springer, 2022: 615 – 641. DOI: 10.1007/978-3-031-18283-9_31
[83] MetaMask. The crypto wallet for Defi, Web3 Dapps and NFTs [EB/OL]. [2022-09-11]. https://metamask.io/
[84] ESKANDARI S, BARRERA D, STOBERT E, et al. A first look at the usability of bitcoin key management [C]//Proceedings 2015 Workshop on Usable Security. Internet Society, 2015: 55 – 63. DOI: 10.14722/usec.2015.23015
[85] HENDRIX C, LEWIS R. Survey on blockchain privacy challenges [EB/OL]. [2022-09-11]. http://ceur-ws.org/Vol-3031/paper_5.pdf
[86] BLACKSHEAR S, CHALKIAS K, CHATZIGIANNIS P, et al. Reactive key-loss protection in blockchains [C]//International Conference on Financial Cryptography and Data Security. Springer, 2021: 431 – 450. DOI: 10.1007/978-3-662-63958-0_34
[87] O'CONNOR R, PIEKARSKA M. Enhancing bitcoin transactions with covenants [C]//International Conference on Financial Cryptography and Data Security. Springer, 2017: 191 – 198
[88] MÖSER M, EYAL I, GÜN SIRER E. Bitcoin covenants [C]//International Conference on Financial Cryptography and Data Security. Springer, 2016: 126 – 141
[89] BARTOLETTI M, LANDE S, ZUNINO R. Bitcoin covenants unchained [EB/OL]. (2020-06-06)[2022-09-11]. https://arxiv.org/abs/2006.03918
[90] ZHOU T Q, SHEN J, REN Y J, et al. Threshold key management scheme for blockchain-based intelligent transportation systems [J]. Security and communication networks, 2021: 1864514. DOI: 10.1155/2021/1864514
[91] MA M X, SHI G Z, LI F H. Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario [J]. IEEE access, 7: 34045 – 34059. DOI: 10.1109/ACCESS.2019.2904042
[92] ZHANG S J, LEE J H. A group signature and authentication scheme for blockchain-based mobile-edge computing [J]. IEEE Internet of Things journal, 2020, 7(5): 4557 – 4565. DOI: 10.1109/JIOT.2019.2960027
[93] PAAVOLAINEN S, CARR C. Security properties of light clients on the ethereum blockchain [J]. IEEE access, 8: 124339 – 124358. DOI: 10.1109/ACCESS.2020.3006113
[94] LETZ D. Blockquick: super-light client protocol for blockchain validation on constrained devices [EB/OL]. [2022-09-11]. https://eprint.iacr.org/2019/579
[95] YUAN L, TANG Q, WANG G L. Generic superlight client for permissionless blockchains [EB/OL]. [2022-09-11]. https://arxiv.org/abs/2003.06552
[96] JIANG S, CAO J N, ZHU J C, et al. PolyChain: a generic blockchain as a service platform [J]. Blockchain and trustworthy systems, 2021: 459 – 472. DOI: 10.1007/978-981-16-7993-3_36
[97] AMIRI M J, WU C, AGRAWAL D, et al. The bedrock of BFT: a unified platform for BFT protocol design and implementation [EB/OL]. (2022-05-09)[2022-09-11]. https://arxiv.org/abs/2205.04534v1
[98] CELESTIA. The first modular blockchain network [EB/OL]. [2022-09-11]. https://celestia.org/?ref=cypherhunter
[99] WERNER S M, PEREZ D, GUDGEON L, et al. SoK: decentralized finance (defi) [EB/OL]. (2021-01-21)[2022-09-11]. https://arxiv.org/abs/2101.08778v3
[100] SETHAPUT V, INNET S. Blockchain application for central bank digital currencies (CBDC) [C]//The Third International Conference on Blockchain Computing and Applications (BCCA). IEEE, 2021: 3 – 10. DOI: 10.1109/BCCA53669.2021.9657012
[101] KELKAR M, ZHANG F, GOLDFEDER S, et al. Order-fairness for byzantine consensus [C]//Annual International Cryptology Conference. CRYPTO, 2020: 451 – 480. DOI: 10.1007/978-3-030-56877-1_16
[102] REJIBA Z, MASIP-BRUIN X, MARÍN-TORDERA E. A survey on mobility-induced service migration in the fog, edge, and related computing paradigms [J]. ACM computing surveys, 2020, 52(5): 1 – 33. DOI: 10.1145/3326540

[103] BANDARA H D, XU X W, WEBER I. Patterns for blockchain data migration [C]//Proceedings of the European Conference on Pattern Languages of Programs 2020. ACM, 2020: 1 – 19. DOI: 10.1145/3424771.3424796

Biographies

CAO Yinfeng (csyfcao@comp.polyu.edu.hk) received his BS degree in information security from Xidian University (cyberspace security experimental class), China. He is currently a PhD candidate with the Department of Computing, The Hong Kong Polytechnic University, China. His research interests include blockchain systems and cryptography. He received the best paper reward from BlockSys in 2021.

CAO Jiannong is currently the Otto Poon Charitable Foundation Professor in data science and the Chair Professor of distributed and mobile computing in the Department of Computing, The Hong Kong Polytechnic University (PolyU), China. He is also the Dean of Graduate School, the director of Research Institute for Artificial Intelligence of Things (RIAIoT) in PolyU, and the director of the Internet and Mobile Computing Lab (IMCL) . He was the founding director and now the associate director of University's Research Facility in Big Data Analytics (UBDA) in PolyU. He served as the department head from 2011 to 2017. Prof. CAO is a member of Academia Europaea, a fellow of IEEE, a fellow of China Computer Federation (CCF), and an ACM distinguished member. His research interests include distributed systems and blockchain, wireless sensing and networking, big data and machine learning, and mobile cloud and edge computing.

WANG Yuqin is currently a PhD student at the Department of Computing, The Hong Kong Polytechnic University, China. Before that, he received a BE degree from Beijing Forestry University, China in 2021. His research interests include blockchain, edge computing, and wireless algorithm designs.

WANG Kaile received her BE degree in data science and big data technology from the University of International Business and Economics, China in 2021. She is currently a Mphil student at the Department of Computing, Hong Kong Polytechnic University, China. Her research interests include federated learning, data mining, and deep learning.

LIU Xun received her BS degree in computer science from Jilin University, China. She received her MS degree in computer science from the Institute of Information Engineering, Chinese Academy of Sciences. She is currently a PhD student in the Department of Computing, The Hong Kong Polytechnic University, China. Her research interests include cryptography and zero-knowledge proof.

Utility-Improved Key-Value Data Collection with Local Differential Privacy for Mobile Devices

TONG Ze, DENG Bowen, ZHENG Lele, ZHANG Tao

(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

DOI: 10.12142/ZTECOM.202204003

https://kns.cnki.net/kcms/detail/34.1294.TN.20221125.1108.002.html published online November 25, 2022

Manuscript received: 2022-09-09

Abstract: The structure of key-value data is a typical data structure generated by mobile devices. The collection and analysis of the data from mobile devices are critical for service providers to improve service quality. Nevertheless, collecting raw data, which may contain various personal information, would lead to serious personal privacy leaks. Local differential privacy (LDP) has been proposed to protect privacy on the device side so that the server cannot obtain the raw data. However, existing mechanisms assume that all keys are equally sensitive, which cannot produce high-precision statistical results. A utility-improved data collection framework with LDP for key-value formed mobile data is proposed to solve this issue. More specifically, we divide the key-value data into sensitive and non-sensitive parts and only provide an LDP-equivalent privacy guarantee for sensitive keys and all values. We instantiate our framework by using a utility-improved key value-unary encoding (UKV-UE) mechanism based on unary encoding, with which our framework can work effectively for a large key domain. We then validate our mechanism which provides better utility and is suitable for mobile devices by evaluating it in two real datasets. Finally, some possible future research directions are envisioned.

Keywords: key-value data; local differential privacy; mobile devices; privacy-preserving data collection

Citation (IEEE Format): Z. Tong, B. W. Deng, L. L. Zheng, et al., "Utility-improved key-value data collection with local differential privacy for mobile devices," *ZTE Communications*, vol. 20, no. 4, pp. 15 - 21, Dec. 2022. doi: 10.12142/ZTECOM.202204003.

1 Introduction

With the development of mobile communication technologies, service providers are more willing to collect data from mobile devices to enhance the service experience for users. As a classical data structure, key-value data are widespread in practical mobile applications[1-2]. The structure of key-value data is a hybrid data structure, where the key is the identifier of data and the value is the content of data. The following three examples show its potential applications:

1) Mobile devices (such as wearable devices, smartphones, tablets, etc.) generate a large number of data, the majority of which are in a key-value format, i.e., $\langle device\_id, device\_value \rangle$ or $\langle timestamp, device\_value \rangle$. These data could show the usage habits of users on a specific device or during a particular period, which can help data collectors provide a personalized experience for the user. For example, the service center collects $\langle device\_id, sleep\ duration \rangle$ from the user's smart bracelet to remind the user to rest properly at a suitable time[3].

2) Software vendors, such as Android and iOS, collect users' data to enhance the users' experience, i. e. $\langle app\_name, user\ rating \rangle$ or $\langle app\_name, length\ of\ visit \rangle$, in a key-value format, where the key is the name of an APP, and the value is the length of time or a score to access the APP. These data could show the users' experience with a particular application, which can help software vendors study future product improvements. For example, software vendors provide users with personalized recommendations by collecting their specific interest[4].

3) Advertisers are interested in knowing whether the video advertisements they place on mobile devices appeal to potential customers[5]. Therefore, they are willing to collect advertisement ratings from users in the form of key-value, where the key is the ID of the advertisement, and the value is the number of minutes that users watch the advertisement.

However, the key-value data involves a lot of personal information, thus users may be reluctant to upload data from their mobile devices. To address the privacy-preserving data collection issue, some researchers proposed local differential privacy[6] to obfuscate local information in the data collection phase. Because of its decentralization and strict mathematical proof, it has been adopted by mainstream systems such as Ma-

cOS[7] and Windows[8] to collect data. In addition, local differential privacy (LDP) reduces the communication costs of large-scale computing and the frequent interaction with the data center, making it well-suited for mobile devices with limited resources and low computing power.

Recently, there has been extensive research on key-value data collections with LDP. YE et al.[9] first proposed PrivKVM to protect key-value data using synchronized key and value perturbation protocols. It adopted one iteration to obtain frequency estimation and several iterations to achieve an approximately unbiased mean estimation. The result of the last iteration is sent to the next iteration as input. However, it requires all users to be online in all the iterations, which is difficult to achieve in practical scenarios. Moreover, PrivKVM may lead to a high estimation error when the key domain is large. SUN et al.[2] proposed a series of LDP mechanisms based on PrivKVM and introduced conditional analysis for key-value data analysis. However, the mean estimation obtained by SUN et al. is biased. Subsequently, GU et al.[10] proposed a private correlated key-value (PCKV) data collection mechanism, which adopts the padding-and-sampling mechanism to solve the large key domain problem of previous work[9]. Moreover, a budget composition theorem for the relevant perturbation mechanism is further given to enhance the data utility using privacy budget relaxation. However, according to the definition of LDP, we cannot distinguish whether the output key is genuine. Because the virtual values significantly reduce the aggregation accuracy, the aforementioned mean estimation mechanisms perform poorly in the case of a small privacy budget. Therefore, there is a requirement to enhance the utility of key-value data collection under LDP.

Moreover, the mechanisms aforementioned regard all data as equally sensitive and thus provide excessive protection for some data and leave much room for improving data utility. In real-world scenarios, there is quite a lot of non-sensitive data. For example, when the server collects application names and ratings from cell phones, attackers cannot infer users' privacy preferences even if they know that the user logs in WeChat, which is a social APP that has a huge user base. Therefore, using WeChat provides non-sensitive data for users. In contrast, using some minority applications provides sensitive data. Based on this idea, MURAKAMI et al.[11] proposed the concept of utility-optimized LDP (ULDP), which only requires LDP protection for sensitive data to reduce the frequency estimation error. Nevertheless, ULDP is only suitable for frequency estimation, thus the accuracy of data collection under the privacy protection for key-value data needs further enhancements.

To address these issues, we propose a new framework for mobile devices called the utility-improved key value (UKV) data collection with LDP. In UKV, mobile devices take different perturbations based on whether the data are sensitive or not to achieve a balance between privacy and utility. We then introduce an initial implementation of the UKV framework and verify its performance in terms of data utility using public datasets.

The remainder of the paper is organized as follows. The overview and benefits of the UKV framework are introduced in Section 2. Some key challenges are presented in Section 3. In Section 4, we describe a case study of an initial implementation of the UKV framework for mobile devices. The performance of our mechanisms is evaluated in Section 5, and some possible future directions are given in Section 6. Finally, we conclude the paper in Section 7.

2 Overview and Benefits

In this section, we briefly introduce data collection under local differential privacy. Then we describe the UKV framework and its benefits for data protection.

2.1 Data Collection Under Local Differential Privacy

Data collection is an important means of obtaining data from mobile devices. By collecting and analyzing users' data, data collectors can mine users' characteristics (such as living habits and health status) and thus formulate more appropriate development strategies. However, users' data often contains a large amount of personal information. Collecting raw data may lead to serious personal privacy leaks, which not only harms privacy leakers but also brings a series of legal risks and economic losses to data collectors. Therefore, this issue needs to be solved urgently.

Differential privacy[12] provides a feasible solution to the problem of personal privacy leakage due to its characteristic of being plausible and deniable. It provides strictly provable privacy protection without relying on the background knowledge possessed by the attacker. LDP is one of the differential privacy technologies that specifically address the problem of personal privacy leakage during data collection. Unlike central differential privacy, which assumes the existence of a trusted data collector with access to the user's raw data, LDP does not require any qualification on the credibility of the data collector. In particular, LDP requires each user to locally perturb the raw data with a local perturbation mechanism before sending it to the data collector. Therefore, the data security of the users is guaranteed. Because of this unique advantage, LDP has been widely adopted in practice. A successful case is RAPPOR[13] on Google Chrome, which enables Google to collect users' browsing information while protecting user privacy.

A basic LDP mechanism is Generalized Randomized Response (GRR)[14]. The main idea of GRR is to set the output range to be the same as the input range, with a certain probability of providing a "fake" response while maximizing the likelihood of providing a "true" response. Specifically, each user perturbs x to itself with a large probability p, and perturbs x to other data with a small probability q. However, the utility of GRR drops rapidly when the data domain is large. UE[15] solves this problem. UE first encodes the input data as a

one-hot d-dimensional vector with only the bit corresponding to the data set to 1, where d is the size of input domain. Then each bit is perturbed independently. Here, each user retains (only) input 1 with large probability p, and perturbs each 0 to 1 with probability q. Our work is based on the above scheme and achieves secure data collection adapted to mobile devices.

2.2 Overview

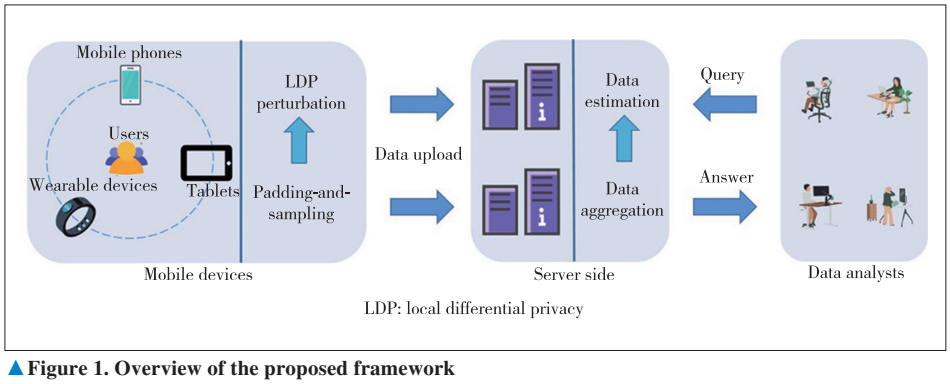
Fig. 1 shows the overview of our framework, which contains three parts: mobile devices, the server side, and data analysts. And, we will describe each part of our framework in detail.

•Mobile devices. Mobile devices are individual users who own personal data. They can not only generate and collect data of users but also perturb the raw data with local differential privacy mechanisms to protect information privacy.

•Server side. The server, which has a large number of computing and storage resources, is responsible for collecting the data sent by mobile devices, and aggregating and estimating the data. Finally, the server releases the data and its corresponding estimations. In this paper, we assume that the server is "semi-honest". Here, "semi-honest" means that the server honestly executes the data collection protocol while potentially leaking the user's historical data to attackers.

•Data analysts. Data analysts are the actual users of the data. The data analyst submits a query request to the server and gets the noise-added results. These analysts may be ordinary users or malicious attackers.

We briefly describe the data flow in a UKV framework to understand the data processing procedure. The raw data are generated by the mobile device and locally perturbed by UKV. Then, the mobile device sends it to the server side. In addition, the key-value data are divided into two categories: sensitive data and non-sensitive data. In the data perturbation phase, UKV divides the privacy budget ε into two parts, namely ε_1 and ε_2, where ε_1 is used for perturbation of key and ε_2 is used for perturbation of value. For sensitive key-value data, the key consumes all privacy budget ε_1; for non-sensitive key-value data, the key does not consume any privacy budget. Furthermore, UKV consumes the privacy budget of ε_2 to perturb the value for two types of key-value data. Finally, the server releases the estimated results to the data analyst.



▲**Figure 1. Overview of the proposed framework**

2.3 Benefits

By applying the UKV framework, users perturb the raw data before sending key-value data to the server. In addition, the UKV framework also provides the following benefits.

• Privacy protection and efficient utility of data. In data collection, each user sends the noise-added data to the server. Then the server aggregates and analyzes the data where the frequency and mean estimation are important data analysis components. UKV can maintain high efficiency with a low privacy budget. As the number of non-sensitive keys increases, the data utility improves rapidly.

• No trusted third party is required. LDP transfers the part that adds noise to the raw data to local devices so that the third-party data collectors cannot get the raw data; thus it avoids the risk of privacy leakage by third parties.

3 Key Challenges

In order to take full advantage of the UKV framework for mobile devices, we still face challenges in the implementation of the proposed framework, which seriously hinders the booming development of related applications.

1) Individuals have different privacy needs for data. The difference between sensitive and non-sensitive data can vary from one user to another (e.g., some people even want to keep the name of the APP that they use and the scores of the movie they give private). Moreover, we concentrate on a situation in which users can easily choose, no matter it is sensitive or not. Nevertheless, there is also a situation in which the user knows nothing about the sensitive data type. For the latter case, the improvement of our UKV framework for data utility is greatly reduced. Therefore, how to divide sensitive data and non-sensitive data is crucial.

2) Association of sensitive data with non-sensitive data. First, we assume that each user sends a key-value data pair and each user's data are irrelevant. This makes sense for most personal data (e.g., application ratings). Yet, for certain types of personal data (e.g., flu status[16]), users may be extremely influenced by other users. Moreover, when users send more than one pair of data, sensitive and non-sensitive data may also be correlated with each other, which means that non-sensitive data release may lead to sensitive data leakage[17]. Therefore, designing a scheme for sending multiple data pairs per user is an important and challenging problem.

3) Lightweight. In practical applications, the communication band-

width cost between the mobile device and the server is proportionate to the domain size of the key. The time complexity of UKV proposed in this paper is $O(d)$. When the key domain is too large, the communication cost increases dramatically, which is unacceptable in many practical applications. Moreover, because of the limited computing resources of mobile devices, they lack the ability to perform complex computing tasks. Thus, designing a lightweight privacy-preserving algorithm for mobile devices is necessary.

4) Selection of parameters. The Padding-and-Sampling protocol is used in the UKV framework, where the padding length l needs to be set in advance. In theory, it should be set based on the data distribution. A small l will reduce the frequency estimation for the key, while a large l will increase the quantity of virtual key-value data, leading to a larger estimation error. However, the best selection of l is not possible because the purpose of UKV is to learn the data distribution. In addition, the choice of privacy budget is essential for balancing privacy and utility. Therefore, it is crucial to choose parameters to achieve near-optimal efficiency.

4 Case Study

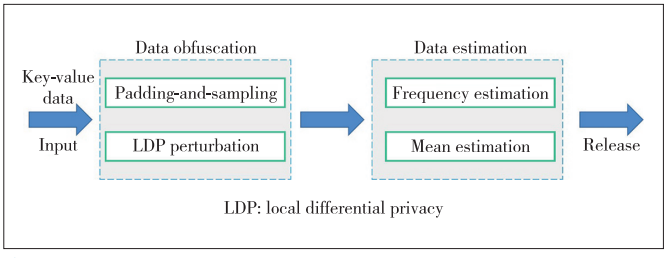
In this section, we provide a case study to introduce the initial implementation of the UKV framework for mobile device data collection.

Fig. 2 shows the implementation of the UKV framework for mobile devices. It consists of two parts:

1) The mobile device perturbs key-value data with LDP to provide provable privacy guarantees.

2) The server estimates data to generate usable data from the collected key-value data for analysis.

The two parts are combined to improve the accuracy of server data analysis while protecting the privacy of key-value data. We then describe the details of the two parts in the following sections.



▲ **Figure 2. Implementation of the utility-improved key value framework**

4.1 Mobile Device

• Padding-and-sampling[18]: Each user samples one datum from possessed key-value data instead of sampling one datum from the domain of all key-value data. In order to make all samplings rate the same, each user first adds different random dummy data to possessed key-value data until he has l key-value data.

• Perturbation: The general overview of the perturbation method includes the key input domain, key output domain, and flip probability. The input domain has sensitive key $k_s \in K_S$ and non-sensitive key $k_n \in K_N$, where K_S and K_N are the sets of sensitive and non-sensitive keys, respectively. In the output domain, $k_r \in K_S \backslash k$ denotes the rest sensitive keys except k, where k may not belong to K_S. When the user inputs k_s to UKV, her output includes k_s with p_{ss} probability and k_r with p_{sr} probability, where the values of p_{ss} and p_{sr} are related to the privacy budget ε_1. When the user inputs k_n, her output includes k_r with the p_{nr} probability and k_n with the p_{nn} probability, where p_{nr} is equal to p_{sr}.

Combining the thought with UE[15], we instantiate a mechanism named UKV-UE under the UKV framework. For the data obtained by sampling, UKV-UE first transforms the input data into a one-dimensional array, e. g., the second data is $\langle id\_2, 0.9\rangle$, which we transform into a vector $\left(\langle 0,0\rangle, \langle 1,1\rangle, \langle 0,0\rangle, \cdots, \langle 0,0\rangle\right)$ with vector length l, and perturbs each bit independently. Each array is divided into two parts: sensitive and non-sensitive bits. Here, we use k to denote the k-th bit of the array and i to denote the rest of the bits of the array. According to the transformation, we know that the k-th bit is $\langle 1, v\rangle$ and the rest bits are $\langle 0, 0\rangle$. For the results of perturbation: 1) when k belongs to sensitive bits, -1 (or 1) indicates the presence of the key, where -1 (or 1) is obtained by a stochastic rounding (SR) mechanism[19] (the SR mechanism is to perturb the value to -1 or 1 with different probabilities depending on the input) and 0 indicates the absence of the key; 2) when k belongs to non-sensitive bits, v' obtained by perturbing v with the hybrid mechanism (HM)[20] indicates the presence of the key (HM output domain is boundedly continuous) and the specified out-of-domain element M indicates the absence of the key.

4.2 Server-Side

Data estimation: The server collects the data uploaded by users. For the sensitive key, the server computes the counts of 1 and -1 that support key k from all the data sent by users, denoted by n_0 and n_1, respectively. Then we could calculate the frequency estimation $\hat{f}_k$ and the corresponding mean estimation $\hat{m}_k$ by

$$\hat{f}_k = \frac{\left(n_0 + n_1\right)/n - p_{ss}}{p_{ss} - p_{sn}},$$

$$\hat{m}_k = \frac{l\left(n_0 - n_1\right)\left(e^{\varepsilon_2}\right)}{n\left(e^{\varepsilon_2} - 1\right)\hat{f}_k p_{ss}}, \tag{1}$$

where n is the number of the users.

For the non-sensitive key, the server computes the number of v that supports key k from all the data sent by users, de-

noted by n_2. Then we could calculate the frequency estimation $\hat{f}_k$ and the corresponding mean estimation $\hat{m}_k$ by

$$\hat{f}_k = \frac{n_2}{n \cdot p_{nn}},$$

$$\hat{m}_k = \frac{\sum_{\langle k,v \rangle \in P} v}{n_2}, \tag{2}$$

where P is the set of perturbed values sent by the users.

In summary, UKV improves the data utility by slackening privacy protection for non-sensitive data.

5 Performance Evaluation

In this section, we evaluate the privacy and utility assurance performance of UKV for data collection in public datasets.

Datasets: In this paper, we use the e-commerce (Ec) dataset[21] and the clothing (Cl) dataset[22] to evaluate the performance of UKV on privacy protection and utility assurance. The Ec dataset includes 23 486 key-value pairs and 1 206 category keys for a total of 23 486 users. The Cl dataset includes 192 544 key-value pairs and 5 850 types of keys, with a total of 105 508 users.

To demonstrate the advantages of the UKV framework, we compare it with the most advanced key-value data collection mechanism PCKV.

Evaluation metrics: We evaluate the frequency and mean estimations by comparing the averaged mean square error (MSE) among non-sensitive keys:

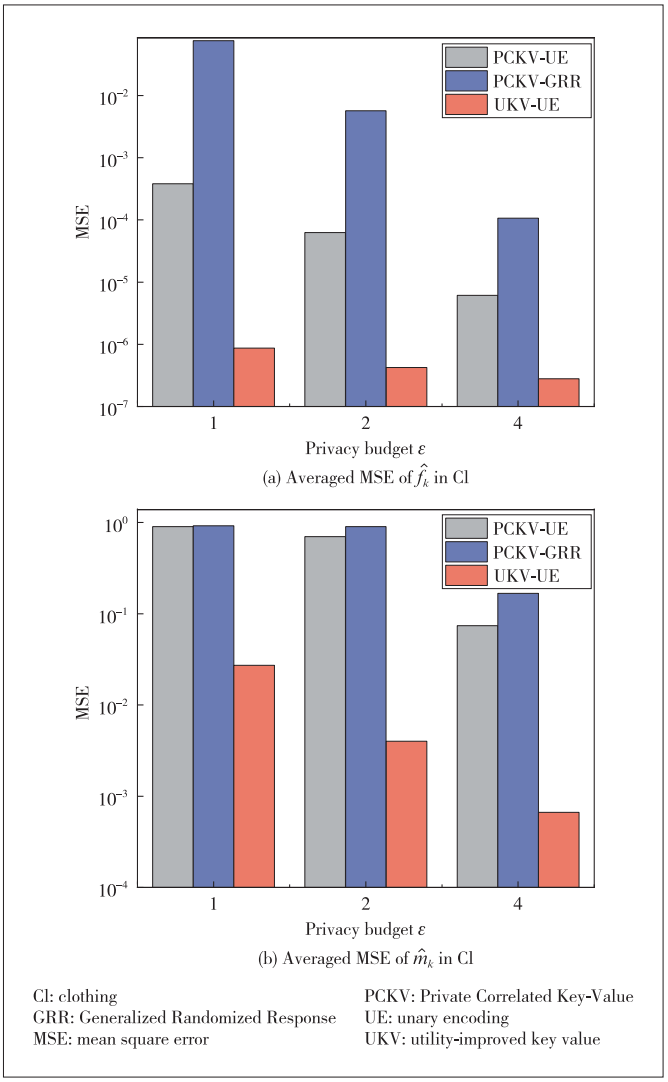
$$\mathrm{MSE}_{\mathrm{freq}} = \frac{1}{|K_N|} \sum_{k \in K_N} \left(\hat{f}_k - f_k \right)^2,$$

$$\mathrm{MSE}_{\mathrm{mean}} = \frac{1}{|K_N|} \sum_{k \in K_N} \left(\hat{m}_k - m_k \right)^2, \tag{3}$$

where K_N is the domain of non-sensitive keys, $\hat{f}_k$ and $\hat{m}_k$ are the frequency and mean estimations of the key-value data, and f_k and m_k are the actual frequency and mean values of the key-value data.

We use the ten most frequent keys as non-sensitive keys, because the frequency of non-sensitive keys is usually higher in practice.

Figs. 3 and 4 show the MSE of non-sensitive keys in two real-world datasets, from which the effect of privacy budget on data utility can be observed. We double the privacy budgets in our experiments. The larger the privacy budget, the lower the mean square error and the higher the data utility. The MSE of the Cl dataset does not change much compared with the results of the Ec dataset because all algorithms benefit from the number of users, which makes up for the effect of the large key domain. As



▲ **Figure. 3. MSE of Cl dataset**

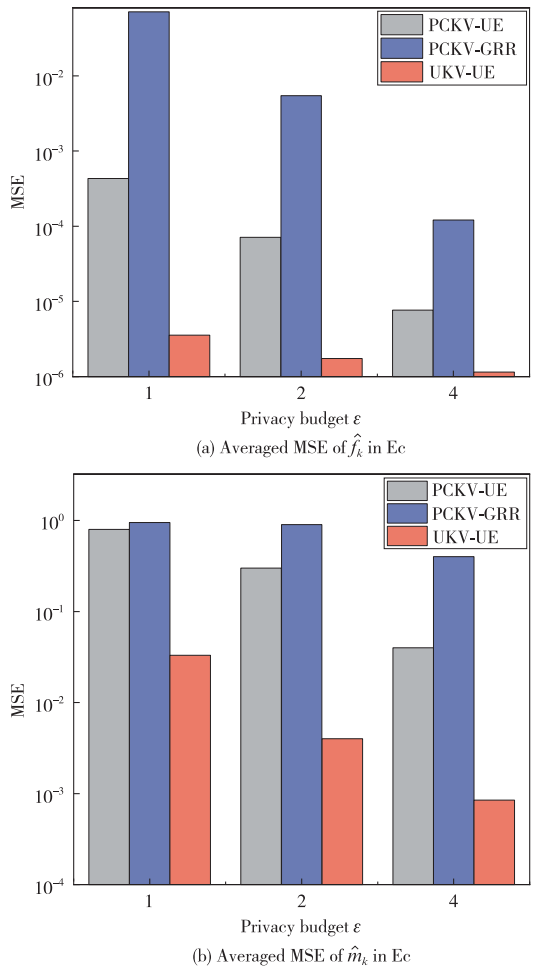
shown in Figs. 3(a) and 4(a), our UKV-UE mechanism performs the best as it does not decrease the privacy budget of frequency estimation while discriminating the key sensitivity in UKV. The theory of dividing the sensitivity to decrease the frequency estimation errors is detailed in Ref. [12].

Similarly, in Figs. 3(b) and 4(b), the UKV-UE mechanism performs well for any privacy budget about the mean estimation. In the case of a small privacy budget, only the UKV-UE achieves higher accuracy.

6 Future Directions

This work, key-value data collection with LDP for mobile devices, still needs further research to advance its development. In this section, we envision some possible future directions.

1) Statistical analysis of key-value data for mobile devices. To the best of our knowledge, the current work is limited to frequency estimation and mean estimation of key-value data. In



▲ **Figure 4. MSE of Ec dataset**

contrast, other applications of key-value data are less explored (e.g., maximum-minimum estimation of key-value data). Therefore, other aggregation statistics of key-value data for mobile devices are a direction worthy of attention.

2) Machine learning on mobile devices. In a distributed machine learning system on mobile devices, the mobile devices collect data and send it to the server. Then, the server divides the subsets of data items according to certain rules and finally distributes the subsets to each device for training. Currently, only a few mobile machine learning frameworks support key-value data formats to submit training data, like searching English words in dictionaries (the dictionary data structure is in key-value format, where the key is the alphabet and the value is their sequence number). Therefore, exploring more training frameworks that support key-value data formats and adding LDP protection to them is quite worthwhile.

3) High-dimensional key-value data in mobile devices. Most of the current major differential privacy protection frameworks are for two-dimensional data sets. However, there are a lot of complex high-dimensional data in mobile devices, and it is necessary to protect them using local differential privacy techniques. Moreover, shifting data protection from two dimensions to multiple dimensions will inevitably bring more challenges, like dimensional disasters. In short, designing a differential privacy protection framework for mobile devices that can be extended to multi-dimensional data protection is an important challenge for data analysis work.

4) Mobile real-time data release. With the need for some particular scenarios (such as a health code and a nucleic acid test), people have an increasing demand for real-time query response and data updates. Real-time data release has high requirements for the stability of data transmission. However, the data transmission stability of mobile devices is doubtful, which may cause frequent dropouts for users. In addition, problems such as repeated data release and dynamic data update significantly increase the risk of privacy leakage in the real-time data release. Therefore, the privacy protection for real-time data release of mobile devices deserves much attention.

5) Preventing poisoning attacks by mobile devices. Poisoning attacks against key-value data aim to reduce data availability by sending carefully crafted data from some fake users to the server while changing the frequency and mean value of the target key chosen by the attacker[23]. For example, an attacker successfully changed a road segment in Google Maps from "clear" to "congested" using 99 mobile phones. Existing defense methods are effective in some cases but ineffective in others. Therefore, researching methods to defend against poisoning attacks from mobile devices is a worthwhile endeavor.

7 Conclusions

We researched the utility improvement of key-value data collection for mobile devices and proposed a novel framework, UKV, which has improved the data utility by providing LDP privacy protection for sensitive key-value data only. We also introduced the main challenges that hindered key-value data collections from maximizing their benefits. Then, we introduced an initial implementation of the UKV framework and validated the excellent utility of our mechanism on two real datasets. Finally, we envisioned some possible future directions to attract more research in this area.

References

[1] ZENG J A, PLALE B. KVLight: A lightweight key-value store for distributed access in cloud [C]//The 16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid). IEEE, 2016: 473 – 482. DOI: 10.1109/CCGrid.2016.55
[2] SUN L, ZHAO J, YE X, et al. Conditional analysis for key-value data with local differential privacy [EB/OL]. (2019-07-11) [2022-09-20]. https://arxiv.org/abs/

1907.05014v1
[3] ANGELINI L, CAON M, CARRINO S, et al. Designing a desirable smart bracelet for older adults [C]//Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication. ACM, 2013: 425 – 434. DOI: 10.1145/2494091.2495974
[4] MENG J K, ZHENG Z B, TAO G H, et al. User-specific rating prediction for mobile applications via weight-based matrix factorization [C]//Proceedings of 2016 IEEE International Conference on Web Services. IEEE, 2016: 728 – 731. DOI: 10.1109/ICWS.2016.104
[5] BALAKRISHNAN S, CHOPRA S, APPLEGATE D, et al. Computational television advertising [C]//Proceedings of 2012 IEEE 12th International Conference on Data Mining. IEEE, 2012: 71 – 80. DOI: 10.1109/ICDM.2012.129
[6] DUCHI J C, JORDAN M I, WAINWRIGHT M J. Local privacy and statistical minimax rates [C]//Proceedings of 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. IEEE, 2013: 429 – 438. DOI: 10.1109/FOCS.2013.53
[7] TANG J, KOROLOVA A, BAI X, et al. Privacy loss in apple's implementation of differential privacy on macOS 10.12. [EB/OL]. [2022-09-20]. https://www.researchgate. net/publication/319622426_Privacy_Loss_in_Apple's_Implementation_of_Differential_Privacy_on_MacOS_1012
[8] DING B, KULKARNI J, YEKHANIN S. Collecting telemetry data privately [C]// Proceedings of the 31st International Conference on Neural Information Processing Systems, IEEE, 2017: 3574 – 3583
[9] YE Q Q, HU H B, MENG X F, et al. PrivKV: key-value data collection with local differential privacy [C]//Proceedings of 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019: 317 – 331. DOI: 10.1109/sp.2019.00018
[10] GU X, LI M, CHENG Y, et al. PCKV: locally differentially private correlated key-value data collection with optimized utility [EB/OL]. (2019-11-28) [2022-09-20]. https://arxiv.org/abs/1911.12834
[11] MURAKAMI T, KAWAMOTO Y. Utility-optimized local differential privacy mechanisms for distribution estimation [C]//Proceedings of the 28th USENIX Conference on Security Symposium. SEC, 2019: 1877 – 1894
[12] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating noise to sensitivity in private data analysis [J]. Theory of cryptography, 2006: 265 – 284. DOI: 10.1007/11681878_14
[13] ERLINGSSON Ú, PIHUR V, KOROLOVA A. RAPPOR: randomized aggregatable privacy-preserving ordinal response [C]//The 2014 ACM SIGSAC Conference on Computer and Communications Security. CCS, 2014: 1054 – 1067. DOI: 10.1145/2660267.2660348
[14] WANG T H, LI N H, JHA S. Locally differentially private heavy hitter identification [J]. IEEE transactions on dependable and secure computing, 2021, 18 (2): 982 – 993. DOI: 10.1109/TDSC.2019.2927695
[15] WANG T H, BLOCKI J, LI N H, et al. Locally differentially private protocols for frequency estimation [C]//The 26th USENIX Conference on Security Symposium. USENIX, 2017: 729 – 745
[16] SONG S, WANG Y Z, CHAUDHURI K. Pufferfish privacy mechanisms for correlated data [C]//Proceedings of the 2017 ACM International Conference on Management of Data. ACM, 2017: 1291 – 1306. DOI: 10.1145/3035918.3064025
[17] NARAYANAN A, SHMATIKOV V. Myths and fallacies of "personally identifiable information" [J]. Communications of the ACM, 2010, 53(6): 24 – 26. DOI: 10.1145/1743546.1743558
[18] WANG T H, LI N H, JHA S. Locally differentially private frequent itemset mining [C]//Proceedings of 2018 IEEE Symposium on Security and Privacy. IEEE, 2018: 127 – 143. DOI: 10.1109/SP.2018.00035
[19] DUCHI J C, JORDAN M I, WAINWRIGHT M J. Minimax optimal procedures for locally private estimation [J]. Journal of the American statistical association, 2018, 113(521): 182 – 201. DOI: 10.1080/01621459.2017.1389735
[20] WANG N, XIAO X K, YANG Y, et al. Collecting and analyzing multidimensional data with local differential privacy [C]//Proceedings of 2019 IEEE 35th International Conference on Data Engineering. IEEE, 2019: 638 – 649. DOI: 10.1109/ICDE.2019.00063
[21] KAGGLE. Ecommerce rating dataset [EB/OL]. [2022-09-20]. https://www.kaggle.com/nicapotato/womens-ecommerce-clothing-reviews
[22] KAGGLE. Clothing fit and rating dataset [EB/OL]. [2022-09-20]. https://www.kaggle.com/rmisra/clothing-fit-dataset-for-size-recommendation
[23] WU Y J, CAO X Y, JIA J Y, et al. Poisoning attacks to local differential privacy protocols for key-value data [EB/OL]. (2021-11-22) [2022-09-20]. https://arxiv.org/abs/2111.11534

Biographies

TONG Ze received his BS degree from Chang'an University, China in 2019, where he is currently pursuing the MS degree with the School of Computer Science and Technology, Xidian University, China. His research interests include differential privacy and network security.

DENG Bowen received his BS degree from Xidian University, China in 2020, where he is currently pursuing the MS degree with the School of Computer Science and Technology, Xidian University. His research interests include differential privacy and social networks.

ZHENG Lele received his BS degree from Xidian University, China in 2018, where he is currently pursuing the PhD degree with the School of Computer Science and Technology, Xidian University. His research interests include differential privacy and the IoT data security.

ZHANG Tao (taozhang@xidian.edu.cn) received his MS and PhD degrees in computer science from Xidian University, China in 2011 and 2015, respectively. He is currently an associate professor with the School of Computer Science and Technology, Xidian University. His research interests include network security and privacy protection.

Key Intrinsic Security Technologies in 6G Networks

LU Haitao[1,2,3], YAN Xincheng[1,3], ZHOU Qiang[1], DAI Jiulong[1,2,3], LI Rui[1,3]

(1. ZTE Corporation, Shenzhen 518057, China;
2. Shenzhen Key Enterprise R&D Institute of Wireless Mobile Technology (ZTE), Shenzhen 518055, China;
3. Shenzhen Key Laboratory of 5G RAN Security Technology Research and Application, Shenzhen 518055, China)

DOI: 10.12142/ZTECOM.202204004

https://kns.cnki.net/kcms/detail/34.1294.TN.20221129.1217.002.html, published online November 29, 2022

Manuscript received: 2022-09-09

Abstract: Intrinsic security is a hot topic in the research of 6G network security. A revolution from the traditional "plugin-based" and "patch-based" network security protection mechanism to a self-sensing, self-adaptive and self-growing network immunity system is a general view of 6G intrinsic security in the industry. Massive connection security, physical-layer security, blockchain, and other 6G candidate intrinsic security technologies are analyzed based on 6G applications, especially hot scenarios and key technologies in the ToB (oriented to business) field.

Keywords: 6G; intrinsic security; ToB application; massive connection; physical-layer security

Citation (IEEE Format): H. T. Lu, X. C. Yan, Q. Zhou, et al., "Key intrinsic security technologies in 6G networks," *ZTE Communications*, vol. 20, no. 4, pp. 22 - 31, Dec. 2022. doi: 10.12142/ZTECOM.202204004.

1 Introduction

The 3rd Generation Partnership Project (3GPP) defines three 5G application scenarios: Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC), and Massive Machine Type Communication (mMTC)[1]. The 3GPP has considered security as a core issue when formulating 5G network standards and proposed the 5G network security architecture in the first 5G standards (3GPP R15)[2], which defines security functions and components in terms of network access security, network domain security, user domain security, application domain security, service-based architecture (SBA) domain security, visibility and configurability. 3GPP R15, frozen in June 2018, mainly delivered the specifications for eMBB and URLLC scenarios. Based on the network security architecture defined by 3GPP R15, we have proposed security solutions to infrastructure, 5G New Radio (NR) air interfaces, core network interfaces and network management interfaces[3 - 4].

The 3GPP R16 standards[5] then improve URLLC features, support industry-level sensitive latency and higher reliability, support Internet of Vehicles (IoV) applications such as Vehicle-to-Everything (V2X), and introduce a variety of 5G NR air interface positioning technologies. These technical features enable 5G to be applied to Internet of Things (IoT) applications such as industries, automobiles, drones, ports and metro systems, laying a foundation for 5G ToB (oriented to business) vertical industry applications. With the emerging 5G use cases, the industry has begun to realize that traditional network security mechanisms are plugin-based and patch-based, which are difficult to adapt to the security challenges faced by the Internet of Everything in the future. Therefore, we need to essentially change the traditional risk defense ideas and explore an intrinsic security solution to various attacks, instead of individual methods to deal with different security problems,

The 3GPP R17 standards[6], finalized in June 2022, further bring more enhanced features to multiple basic technologies, such as further enhanced large-scale multiple-input multiple-output (MIMO), uplink coverage enhancement, terminal energy efficiency improvement, spectrum expansion, and enhancement of integrated access backhauls (IAB) and simple repeaters. In addition, the reduced capability (RedCap) technology, also known as NR-Light is introduced to support IoT terminals with lower complexity, such as sensors, wearable devices and video cameras. Moreover, the issue of intrinsic security has also been discussed more widely in the industry.

The 3GPP R18[7] research project was officially initiated in December 2021, which marks the arrival of the 5G-Advanced era. The subsequent 3GPP R19/R20 will continue in-depth research and improvement of 5G-Advanced technologies. In the

This work is supported by the National Key Research and Development Program of China (6G Network Architecture and Key Technologies) under Grant No. 2020YFB1806704.
Corresponding author: ZHOU Qiang

5G-Advanced era, the air interface protocols will be evolved and enhanced for 5G application scenarios such as mobile broadband, fixed wireless access, industrial IoT, IoV, extended reality (XR), large-scale machine communications, and drone and satellite access. Moreover, related standards for higher frequency bands, such as 52.6 – 71 GHz and terahertz, will be studied and delivered.

It is expected that 3GPP R21/R22/R23 will be carried out in 2026 – 2030 and focus on the research of 6G communication standards that are future communication technology standards we can now envision. 6G communication services will be extended from land to space, to submarine and to underground, achieving space-air-ground-sea integrated communication networks.

This paper provides a review of key security technologies in 5G and security technology enhancement in 5G-Advanced, and then discusses the vision and requirements of 6G intrinsic security systems. The key technologies for 6G intrinsic security are then analyzed, including massive equipment connection security, physical-layer security, blockchain, and AI security technologies.

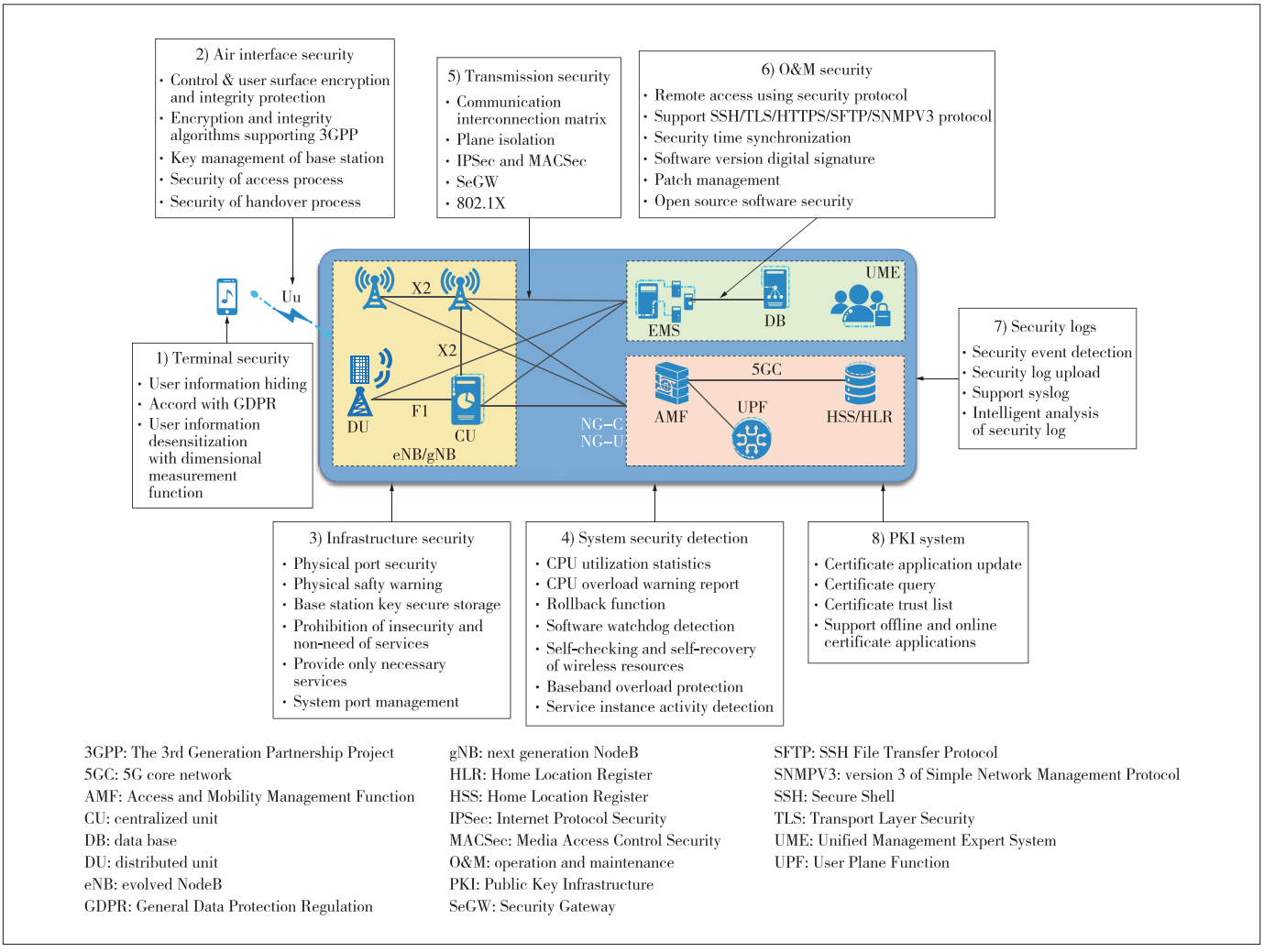
2 Key Security Technologies of 5G and 5G-Advanced

5G NR is a new-generation wireless network based on the New Radio technology. According to the 5G network architecture defined by 3GPP TS33.501[2], the base stations (gNodeB and gNB) are key equipment of the 5G NR system. Therefore, the core focus of security in 5G NR is the external interface of the gNB and the internal interconnection security requirements of the gNB.

Fig. 1 shows the 5G NR security technology architecture.

1) Terminal security is implemented by two-way authentication for user equipment (UE) to access the network. The gNB protects the security of private data through data encryption, transmission channel encryption, permission control, system hardening, and data masking.

2) On the air interface of the access network, control-plane



▲**Figure 1. 5G NR security technology architecture**

and user-plane information protection, including confidentiality and integrity protection, involves security protocols between UE and the gNB.

3) The infrastructure security of the gNB includes physical device security, hardware board design security, storage security, operating system security, disabling insecure services, and avoidance of unsupported hardware and software modules.

4) System security detection protects the normal operation of the gNB, enables quick recovery when the software or hardware is abnormal or faulty, and avoids service interruption of the base station.

5) Transmission security guarantees gNB data transmission by security protocols, involving security for the Xn/X2 interface between gNodeBs and the NG/S1 interface between gNBs and the core network. The transmission network protocol involves the security protocol between the physical layer and the application layer.

6) Basic data configuration, monitoring control, and performance statistics functions are provided for the management system of base station devices. The gNB is connected to the Unified Management Expert System (UME) through the IP network and may be exposed to the public network. Therefore, the gNB is faced with security threats such as illegal intrusion, information disclosure, service interruption and physical damage. Operation and maintenance (O&M) security is protected through account management, rights management, privacy data protection, and transmission security[8].

7) Security logs record security events such as user login and logout, user permission changes for audit, provide effective evidence to prevent personnel or entities from denying executed activities, and collect and store security logs.

8) The PKI system uses asymmetric cryptography algorithms and technologies to implement and provide security services, ensures that base stations use digital certificates to establish Internet Protocol Security (IPSec) security connections with the core network, and provides certificate creation, issuance, and query functions.

As an evolved version of the 5G technology, 5G-Advanced is the evolution of communications technologies, and also a key driving force for new consumption, new businesses and new use cases. It is oriented to business industry applications to facilitate digital transformation of the industries and society. Keeping the existing network capabilities, 5G-Advanced further improves network capabilities, supports large uplink traffic, ultra-low latency, higher reliability, higher availability, higher precision time service and higher precision positioning, and provides communication perception and space-sky-terrestrial integration service guarantee capabilities. Accordingly, 5G-Advanced mainly enhances security technologies in the following aspects:

• High reliability: High reliability enhancement technologies include Packet Data Convergence Protocol (PDCP) duplication, Hybrid Automatic Repeat Request (HARQ) retransmission, intelligent adaptive modulation and coding (AMC) control retransmission, and low-bit-rate Modulation and Coding Scheme (MCS) adjustment. The security technology enhancement involved is PDCP replication security, which ensures that PDCP data and replicated data use the same encryption and integrity protection policy and key, especially the key consistency solution in the cross-site carrier aggregation (CA) scenario and handover scenario.

• High availability: High availability improves availability through device and link redundancy, and ensures that service connections can still be maintained after communication links are disconnected. For example, the Control plane interface of Next Generation (NG-C) link disconnection service holding function of the base station requires continuous services and continuous security. Because security control and management of users are performed in the core network, the gNB also needs to support security control and management of users when the gNB starts link disconnection service holding function.

• 5G accurate timing: The enhanced security of 5G air interface time service mainly refers to the enhanced processing of system information block (SIB) broadcast messages. Because broadcast SIB9 messages can be obtained without access to authentication, the security is poor and 5G air interface time service is vulnerable to attacks from pseudo base stations. Therefore, it is necessary to enhance the security of the terminal procedure, ensure the validity of the SIB9 broadcast message received by the terminal, and re-obtain the time information and use the clock.

• 5G high-precision positioning: The enhanced security of 5G air interface positioning mainly protects positioning data. Data right of access limits must be strictly defined to prevent illegal access and Distribution Denial of Service (DDOS) attacks. The positioning engine for position calculation is the core of high-precision positioning. It is connected to the gNB, UME and service platform, and needs to use different network planes for isolation to ensure network security.

• Data distribution: Local data distribution is an important prerequisite for data security in 5G industrial applications and enterprises to carry out production and operation activities. Data distribution of campus services can be implemented by deploying a dedicated local offloading gateway for campuses or a data processing engine integrated with 5G base stations. Multi-dimensional security isolation measures can be taken to meet the network security requirements of smart and simple campuses.

3 6G Security Vision and Requirements

With the large-scale commercial use of 5G, the industry has started to explore the next-generation mobile communication technology (6G) and carried out research on 6G service requirements, network architecture and enabling technologies[9-11]. The development history of the mobile communication systems from 1G to 5G is a ten-year cycle, so 6G is ex-

pected to be a new-generation mobile communication network oriented to business use in 2030. The 6G era will be an intelligent era in which social services will be balanced and highly advanced, social governance scientific and accurate, and social development green and energy-saving. The 6G network will facilitate in-depth integration of the real physical world and a virtual digital world, building a new world with all things connected and digital twins.

According to the 6G overall vision research report of the IMT-2030 (6G) Promotion Group[12], the 6G network security architecture tends to be distributed and will play a dominant role in the future. It will enable network service capabilities closer to users and transform the traditional centralized security architecture. Brand-new service experiences, such as integrated sensing and communications and holographic communications, will be accompanied with unique user-centered services, which requires a multi-mode and cross-domain security and trustworthiness system. Since traditional "plugin-based" and "patch-based" network security mechanisms will be insufficient for handling potential attacks and security risks on future 6G networks[12], Intrinsic cybersecurity that supports multi-mode trust has been regarded as one of the ten key 6G technologies.

In the early stage of traditional network design, there is no consideration of security factors and service systems and security mechanisms are deployed independently. This will cause several security defects such as passive defense, redundancy of security protection mechanisms and low protection capabilities when new network features, such as trust relationship construction, introduction of a series of new roles and application wide-area transformation, are introduced in future networks such as the industrial Internet and IoT. To avoid such problems, it is necessary to consider the integration design of security technologies and service architectures. Therefore, the construction of intrinsic security models should be explored in the early stage of system design, aiming to implement a complete set of intrinsic security frameworks to enable the intrinsic security attributes of future networks and services and continuously protect users, enterprises, operators and applications[13]. Intrinsic security is a comprehensive capability of a network. This capability consists of a series of security capabilities, which work together to form a self-sensing, self-adaptive and self-growing immune system for 6G netowrks. An intrinsic security system must be built simultaneously during network construction. Besides, it should grow independently during network operation, change with network changes, and improve with the improvement of system services. In this way, the intrinsic security system will continuously ensure the security of networks, services and data.

The IMT-2030(6G) Promotion Group[14] has further clarified that intrinsic security for 6G networks should have the features as follows. First, active immunization, based on trusted technologies, provides active defense functions for network infrastructure and software. Second, elastic autonomy implements dynamic orchestration and elastic deployment of security capabilities to improve network resilience, based on security requirements of users and industrial applications. Third, virtual coexistence is realized by the digital twin technology that is used to unify and evolve the security of physical networks and virtual twins. Fourth, ubiquitous coordination is implemented through intelligent coordination of the end, edge, network and cloud, which can accurately perceive the security situation of the entire network and handle security risks with agility[15].

Intrinsic security should support the development of both networks and vertical industries, from the perspective of its functions. In addition, security itself needs to be secure. Therefore, the requirements for intrinsic security can be divided into three categories: security of business, services of security and security of cybersecurity[16].

Security of business means that intrinsic security should guarantee the security of the underlying layer (network and computing power), capability component layer and application layer, covering such capability components as software and hardware, transmission, operation, big data, and AI, as well as various industry scenarios (such as autonomous driving).

Services of security means that intrinsic security should provide security services related to security capabilities and security management for the application layer, for example, adaptive security for the stop of services and automatic orchestration of security capabilities for the launch of new services.

Security of cybersecurity means that intrinsic security should guarantee its own security. The more exposed surfaces a system has, the greater security risks are likely to occur. Therefore, complying with the rule of simplicity, intrinsic security should be deeply integrated into the network with simplified and higher-performance devices, including software, hardware and ports.

4 Key Technologies of 6G Intrinsic Security

Many innovations and progress have been made in the architecture, applications, technologies, strategies and standardization of 6G networks. However, attackers also become more powerful and intelligent, and can create new forms of security threats. Therefore, intelligent and flexible security mechanisms must be in place to predict, detect, mitigate and prevent security attacks and limit the spread of such vulnerabilities across 6G networks[17].

4.1 Massive Connection Security Technology

In an industrial application scenario, communications technologies will change from human-to-human communications to object-to-object communications, from the downlink-dominant to uplink-dominant, and from the base station-centric to decentralized. A conventional access technology cannot solve the network congestion problems caused by the

access and real-time transmission of massive devices such as an industrial physical network. An innovative Multi-User Shared Access (MUSA) technology proposed by ZTE Corporation can greatly increase the number of connections and system capacity, but reduce latency. The mMTC test shows that MUSA increases the overload rate of connected terminals by 600%, and verifies the massive IoT access performance of equivalent 90 million·MHz^{-1}·h^{-1}·km^{-1}. The access performance of MUSA is increased by 90 times compared with the indicator of 1 million connection/km^2 defined by the International Telecommunications Union (ITU), so the MUSA technology has been a key technology for 5G-Advanced/6G to support massive device connections.

The MUSA technology simplifies the transmission interaction procedure. A large number of terminals can directly initiate transmission without any connection and switch to a deep sleep mode immediately after sending data; the interaction procedure is not required, as shown in Fig. 2. MUSA can save huge overhead of massive user scheduling, thus implementing highly overloaded and spectrum-efficient small-packet transmission and low-cost terminal design, and adapting to the mMTC scenario of 6G applications. However, security is also an important issue that must be considered in the mMTC scenario, that is, how to avoid a complex access authentication process and ensure that a large quantity of accessed terminal devices are trustworthy and legal. Therefore, a lightweight access authentication mechanism is required to implement one-phase access and authentication and ensure user privacy security at the same time.

A common solution is to directly protect the security of the first access message. This method can protect the air interface access messages of a large number of terminals to prevent attackers from eavesdropping and tampering. At the same time, the user ID is encrypted and sent with the message, so that the gNB can authenticate the validity of the terminal and prevent illegal terminals from connecting to the network.

To improve access authentication efficiency, a grouping authentication manner may be used. When a user in a terminal group passes access authentication, all users in the terminal group obtain an access permission by default. If the access permission of a user is cancelled, the access of all users in the group is forbidden.

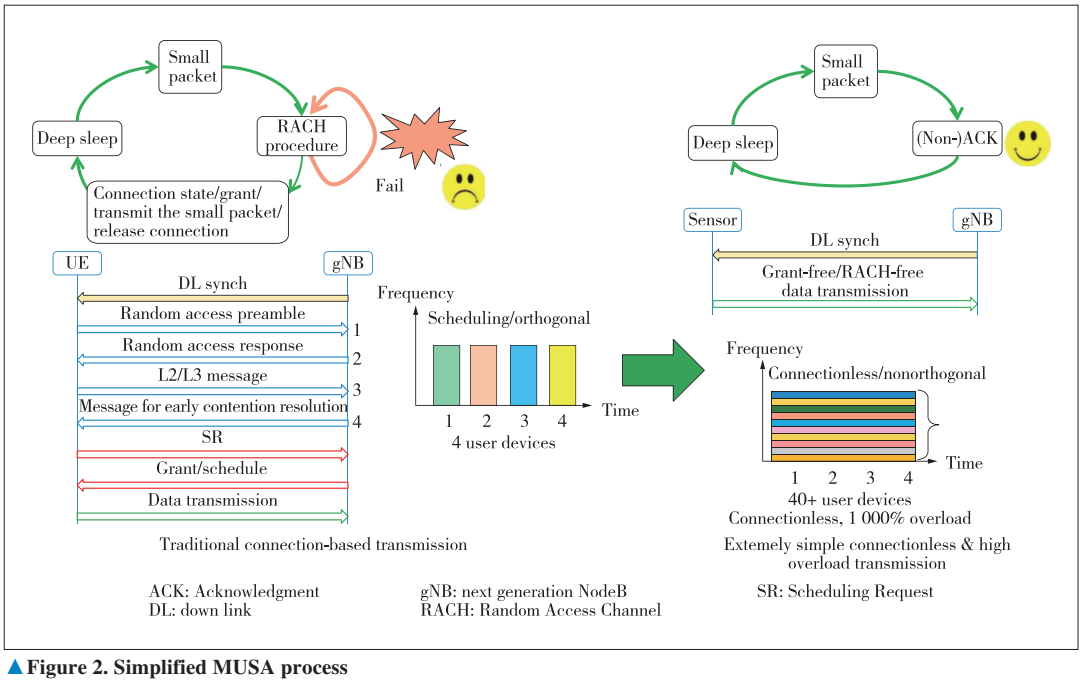
Further, with future development of the physical-layer technology, access may be initiated by using a device fingerprint message and the network may determine validity of the terminal after checking the fingerprint of the terminal device.

4.2 Physical-Layer Security Technology

In 5G communication systems, traditional key-based encryption mechanisms face many challenges. Therefore, the research of intrinsic security of 6G focuses on a self-sensing, self-adaptive and self-growing network immunity system. For implementing physical-layer security, the diversity and time variation of wireless channels and the uniqueness and reciprocity of the wireless channels of both parties of a legal communication are used. Starting from the objective law of radio signal propagation and mining the intrinsic security factors of wireless signals, the difficulty of key distribution and management in encryption technologies can be solved, without relying on the attack capability of eavesdropper. In this way, absolute security in the theoretical sense of information can be achieved. In addition, resource consumption and a delay of physical-layer security are relatively small and can be easily integrated into an existing system. Therefore, the physical-layer security technology is one of the key technologies of 6G intrinsic security.

4.2.1 Self-Adaptive Key Generation on Physical Layer

The existing key generation scheme significantly reduces the entropy rate as the probe rate increases. At a high detection rate, continuous measurement values are highly corre-



▲ **Figure 2. Simplified MUSA process**

lated, and an average amount of information included in each measurement value is reduced, resulting in a relatively low entropy rate, that is, low detection efficiency. The proposed adaptive key generation scheme based on the sliding window policy at the physical layer checks the randomness of the key sequences obtained after quantization in the key generation technology, modifies the bits in the key groups with low randomness, reduces the correlation between the key groups in the sliding window, and finally generates the key sequences with high randomness. Key generation includes three steps: channel detection, quantization, and sliding window detection.

1) Channel detection

Modeling is performed by using a narrowband cluster ray model. It is assumed that a base station is equipped with antennas N_t, a user is equipped with antennas N_r, a channel matrix $\boldsymbol{H}$ includes clusters N_{cl}, and there is a propagation N_{ray} path in each cluster. Therefore, a channel may be represented as:

$$\boldsymbol{H} = \sqrt{\frac{N_t N_r}{N_{cl} N_{ray}}} \sum_{i,l} \alpha_{il} \boldsymbol{a}_r(\theta_{il}) \boldsymbol{a}_t(\phi_{il})^H, \quad (1)$$

where α_{il} is a complex gain of a path of the i-th ray in the l-th cluster, θ_{il} is an angle of arrival (AoA), ϕ_{il} is an angle of departure (AoD) of a corresponding path, and $\boldsymbol{a}(\theta_{il})$ and $\boldsymbol{a}_t(\phi_{il})$ respectively represent array response vectors of the base station and the valid user. Then, after a channel estimation is performed by using a compressive sensing (also known as compressed sensing, CS) technology to obtain a channel path gain parameter, a radio channel key may be generated by using the parameter.

2) Quantization

The quantization process converts the detected channel characteristics into a bit stream, so the quantization policy generates the rate and consistency of the direct shadow key. First, channel estimation is performed, a millimeter wave path gain α is selected as a detection parameter, and then an estimated value α is quantized. A quantization policy obtains an initial bit stream S based on a cumulative distribution function (CDF).

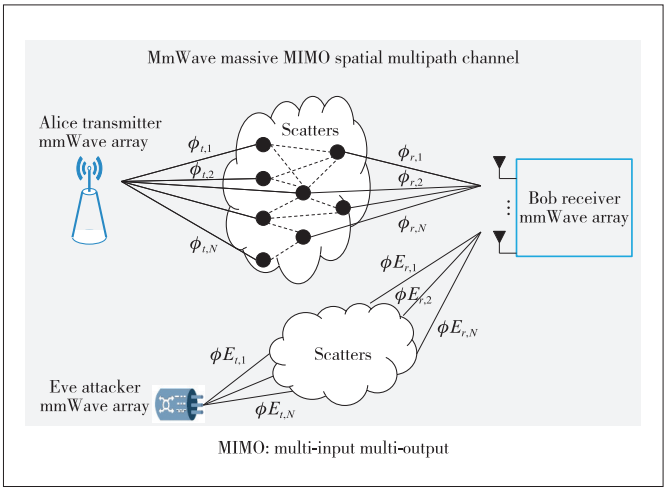
3) Sliding window detection

To ensure a certain key entropy, a sliding window policy is used for adaptive key generation. In a case that a channel measurement value is not random enough, some bits in the sliding window are changed, so that correlation between keys in the window is reduced and a security attribute is improved. The sliding window is specific to a key sequence generated after quantization and is mainly used to check randomness of a key. For the entire key sequence, a sliding window with a fixed length is used to intercept a small segment of initial key and randomness of the key in the window is checked. If the randomness meets a requirement, the key in the window is put into the key pool, the sliding window is moved to the right, and a next small segment of key in the key sequence is intercepted and checked. The window continues to move to the right until the randomness of the entire key sequence is verified.

4.2.2 AI-Based Physical Layer Authentication

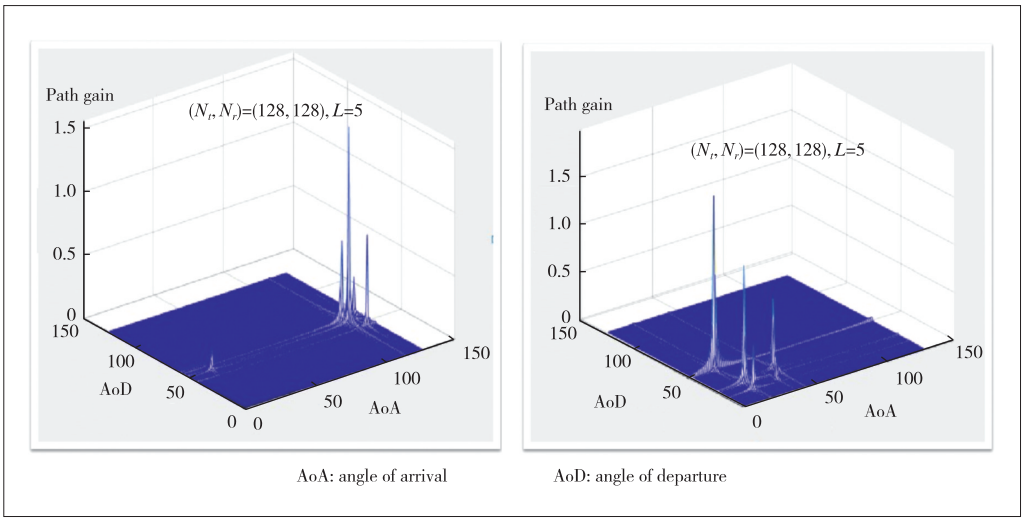
Currently, a channel model inadaptation problem exists in a high-frequency band channel fingerprint-based authentication scheme; eg., most authentication schemes do not have a channel model based on a millimeter wave frequency band, but still use a channel model in a sub-6 GHz system. Therefore, the channel data obtained according to this case cannot truly reflect features such as large bandwidth, severe loss and channel sparsity of a millimeter wave during physical space propagation. The high-frequency communication technology, such as millimeter wave and terahertz, is a key technology of 6G. A physical layer authentication scheme in a high-frequency band channel model needs to be researched, and a machine learning method is used to improve an authentication success rate.

Fig. 3 shows the simulation model of physical layer authentication, it also called the Alice-Bob-Eve model. Alice and Bob are legal receivers. The attacker Eve can initiate eavesdropping and spoofing attacks. Bob is at rest, while Alice and Eve are in the moving state. It is assumed that Bob has established a legal communication with Alice by means of higher layer authentication. In a process of Alice's moving from the beginning to the end, the channel data of the Alice-Bob link are sampled and stored, and the channel data of the Eve-Bob link are sampled and stored in a same manner.



▲ **Figure 3. Simulation model of physical layer authentication**

Because of a high path loss of a non-line-of-sight (NLOS) channel, a millimeter-wave massive MIMO channel presents significant beam domain sparsity and a typical path value in an actual environment is 3 – 5[15]. As the number of antennas increases, the beam domain channels become sparser. Fig. 4



▲ **Figure 4. Virtual channels H_v of two different users**

shows the sparsity of virtual channel paths for two different users, where the number of transmit and receive antennas is N_r = N_t = 128, and that of paths is L_t = 5.

The above physical layer authentication method is based on sparsity of a high frequency channel and machine learning. A semi-supervised learning algorithm is selected, and the data sets obtained, after valid and invalid links are preprocessed, are separately divided, where 75% of the data sets are training data sets and 25% are test data sets. The training data sets are imported to the machine learning classifier to obtain a classification model, the classification model is verified by the test data sets, and an authentication success rate of the model is then obtained.

4.3 Blockchain Technology

A blockchain is a distributed ledger technology based on a cryptography algorithm. The blockchain can be used to build a system that is in a decentralized or multi-centralized manner and cannot be tampered with or forged, and ensures dynamic consistency of a ledger owned by each node. In essence, the blockchain is an Internet shared database, and has features of transparency, security and efficiency. Therefore, the blockchain is applicable to digital transformation of an enterprise affected by low efficiency and to a new business model based on a distributed market. For example, in an IoT application, based on a natural decentralization feature of a ledger, the blockchain is especially efficient in processing a distributed transaction involving multiple parties in the IoT and provides high security for each transaction based on an encryption, confirmation and verification procedure among multiple parties. Blockchain is highly valued in China. It has been included in the 14th Five-Year Plan (2021 – 2025) as one of the emerging digital industries, with a focus on the alliance chain to develop blockchain service platforms and application solutions in the fields of financial technology, supply chain finance and government services. It is foreseeable that the blockchain will be a distributed and secure transaction mode covering tens of millions or even billions of asset units or machines (IoT) in the 6G era and will be a key technology for intrinsic security of 6G networks[18].

With the blockchain technology, trusted data can be stored and shared, and the management information data of terminals, base stations, core networks and operators can be linked up through blockchains to implement trusted storage, anti-tampering and multi-party sharing. For example, measurement data of a base station and a terminal can be stored on a link node and may be used in scenarios such as roaming settlement, data sharing and resource allocation. The mobility information of terminals provided by base stations can be used to support mobility application scenarios in a mobile network. For sake of these benefits, an operator can establish a blockchain server, or multiple operators co-establish and share a blockchain service in a confederation manner. The existing gNodeBs can be split into the centralized unit (CU) and distributed unit (DU) entities. A gNB can contain one CU and multiple DUs. Based on the CU/DU separation architecture, the gNBs can be linked in a blockchain to keep the UE connected to one or more DUs.

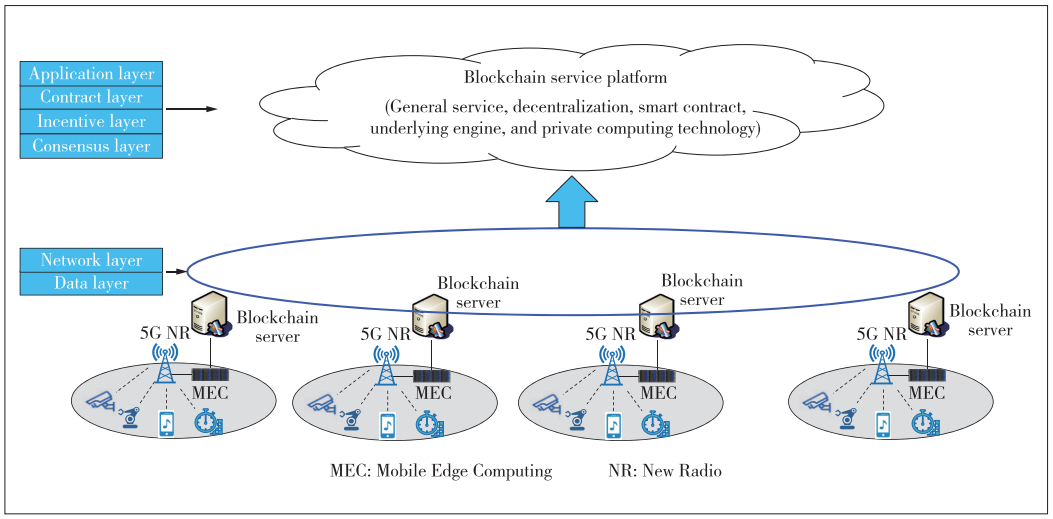
Blockchain can become a 6G intrinsic security technology or be integrated with other 6G technologies to enhance the security of 6G systems, better meeting the ToB application requirements, as shown in Fig. 5.

By enabling 6G security through blockchain, the following security objectives can be achieved:

• User access authentication: Blockchain can provide a flexible and efficient user access control mechanism through access rules and preset logic to implement a blockchain-based 6G network authentication solution.

• Data sharing: Blockchain nodes implement data recording functions and the data can be transmitted point-to-point between these nodes. For specific situations, blockchain nodes can make quick response according to consensus protocols and preset rules.

• Private network slice management: With the blockchain technology, the information such as bandwidth, channel power and data rate can be recorded in each record of a virtualized slice and provided to a user when served. Moreover, such transactions are unchangeably recorded in a shared block and ledger management can also be added into slice management with the concept of a blockchain ledger to implement autono-



▲Figure 5. Enabling 6G security by integration of blockchain

mous and dynamic slice allocation.

• Ensuring data security: The distributed network architecture of blockchain ensures that when one or more nodes are attacked and data stored in 6G network are damaged, other nodes will not be affected.

• Privacy security assurance: Privacy protection in 6G private network can be implemented based on blockchain technologies such as blocking of private data, decentralized storage and information hierarchical smart contract protection.

In the mMTC era, base station-centric mMTC will be transformed into decentralized mMTC to support massive device connections. This is well suited to the decentralized features of blockchain. The features of blockchain technologies such as non-tampering, trace leaving, traceability, collective maintenance, and openness and transparency make it a key candidate solution to intrinsic security in 6G network. Moreover, the deployment forms of blockchain need to be concerned, especially in ToB industrial applications such as IoT networks. For example, the integration deployment of blockchain and Mobile Edge Computing (MEC) modules will ensure the trusted data exchange in a chain. In addition, the on- or off-chain communication mode of blockchain with high reliability and low delay can support efficient and secure communications of large capacity data from multi-type terminals in complex network environment.

4.4 AI Security Technology

A key difference between 5G and 6G is intelligence. AI is one of the hottest topics at present. Almost all fields are exploring the use of AI technologies. The future 6G network architecture will be increasingly huge and heterogeneous, and service types and application scenarios will be increasingly complicated and diversified. It is almost an inevitable choice to make full use of AI technologies to meet such complex requirements. With the in-depth integration of the 6G network with AIs, the 6G intrinsic AI security technology will fully mine and continuously learn multi-dimensional data such as wireless environment, resources, interference, service and user attacks, and security threat information, and provide highly valuable data analysis and decision-making suggestions to significantly improve the efficiency, reliability, real-time, and security of the 6G network, thus implementing a measurable and evolved security intrinsic protection system. Key AI security technologies include active immunization, intelligent management and orchestration, security situational awareness, and trustworthy openness.

1) Active immunization

AI technologies are used to identify and mitigate 6G security problems. Deep reinforcement learning and deep neural networks can be used to detect and prevent intrusions, effectively defending against attacks from pseudo base stations, IP spoofing, DDOS, control plane saturation, and host location hijacking. Predictive analysis using AI can predict attacks before they occur, such as intelligent beamforming techniques based on reinforcement learning (RL) that provide the best beamforming strategy for eavesdropper attacks in 6G THz and visible light communications systems. Edge-based federated learning enables network security in the massive devices and data mechanisms of 6G distributed networks.

2) Intelligent management and orchestration

6G network security shall have an elastic and scalable framework, and the infrastructure shall have the capability of flexibly splitting and combining security services. Through the collaborative intelligent analysis and orchestration mechanism, a flexible and efficient security capability resource pool can be built on demand to implement on-demand customization, dynamic deployment, and elastic scalability of security capabilities, achieving the objectives of active immunization, trust and consensus, and collaborative elasticity.

At the same time, pre-simulation analysis, verification and optimization control are performed for the services and network status in dynamic 6G scenarios to achieve low-cost trial and error of management orchestration, rapid iteration of AI algorithms, optimal AI decision-making and efficient self-generation/self-evolution.

3) Security situation awareness

Different from traditional 5G communication networks, 6G networks will face varied features of different industries in the ToB field. Technical barriers and learning costs of different in-

dustries have derived the demands of collaborative O&M of the peer end, edge, network and cloud. Machine learning and big data analysis technologies will be widely and deeply used in security in smart and endogenous 6G networks. AI technology will enable the 6G network to establish a wide interaction and coordination mechanism among the peer end, edge, network and cloud intelligent subjects, accurately perceive the network security situation and predict potential risks, and then implement self-optimization and evolution through the intelligent consensus decision-making mechanism, which will implement active in-depth security defense and automatic security risk handling[13].

Security situation awareness uses the AI engine to implement continuous online machine learning and iterative update. A network health measurement model is generated by training, which can be applied to real-time devices and network health monitoring. It can quickly identify network risks, device faults and external environment risks that may cause service quality degradation, and provide best handling suggestions to prevent problems from happening. At the same time, long-term monitoring data are used to identify the factors that affect the stable operation of the network, such as equipment, links and environment, in advance, evaluate network health, accurately identify potential risks, predict the fault occurrence time, and give a prompt to users before the fault occurs. The frequency of network faults can be greatly reduced and the high reliability required by enterprise services can be ensured by the active prevention, risk identification in advance, replacement of hardware with hidden risks in time, and guidance of O&M personnel to rectify environmental risks.

4) Trustworthy openness

The openness of various computing power, algorithms and data resources in 5G and other traditional mobile communication systems is not good enough. Most of these resources can only serve the inside of mobile communication systems and their values cannot be expanded. Therefore, the AI resource capabilities in the new 6G system are expected to be fully opened on demand and flexibly invoked and utilized by external third-party applications on demand. Specifically, the opening of data resources includes both the data strongly related to AI (for example, sample training data and model algorithm data) and various types of data of the 6G network (for example, various perception data, control plane data and user plane data). In the process of opening up AI resources and capabilities and realizing shared and utilized values, security trust and privacy protection are important prerequisites. The industry has been studying how to construct a unified open standard of a secure and trusted AI resource capability platform.

5 Conclusions

Before 6G, security technologies are not intrinsic, but the supplement and enhancement of service functions for preventing and eliminating security threats in communication application scenarios. With the emerging of revolutionary 6G technologies, such as terahertz and visible light communications, reconfigurable intelligent surface (RIS), symbiotic sensing and communications, space-sky-terrestrial integration, and digital twins, 6G networks will bring new paradigms with systematical changes. Therefore, a consensus has been reached that 6G network security is no longer traditional "plugin-based" and "patch-based" but intrinsic.

This paper reviews the key security technologies of 5G and 5G-Advanced, analyzes the key technologies of 6G intrinsic security based on 6G applications, and focuses on the massive equipment connection security technologies, physical layer security technologies, blockchain technologies and AI security technologies that are closely related to 6G applications. Although space-sky-terrestrial integration communication security and intrinsic security system architecture are also hot topics of 6G intrinsic security, most related discussions are on concepts and visions. The technical systems and standards of 6G intrinsic security have not yet reached a unified understanding in the industry. Continuing the research and development of application security solutions and security technology evolution of the 5G/5G-Advanced technology, we will continuously pay attention to the disruptive impact caused by 6G intrinsic security, and present our solutions and research results of 6G intrinsic security.

References

[1] WU H Q. Ten reflections on 5G [J]. ZTE Communications, 2020, 18(1): 1 – 4. DOI: 10.12142/ZTECOM.202001001
[2] 3GPP. Security architecture and procedures for 5G system (Release 15): 3GPP TS 33.501 [S]. 2019
[3] LU H T, LI G, GAO X S. Security of 5G network elements and access control [J]. ZTE technology journal, 2019, 25(4): 19 – 24+55. DOI: 10.12142/ZTETJ.201904004
[4] WANG W B, ZHU J G, WANG Q. Evolution requirements and key technologies of 5G core network [J]. ZTE technology journal, 2020, 26(1): 67 – 72. DOI: 10.12142/ZTETJ.202001015
[5] 3GPP. Study on the security of ultra-reliable low-latency communication (URLLC) for the 5G system (5GS) (Release 16): 3GPP TR33.825 [S]. 2019
[6] 3GPP. Enhanced support of industrial IoT in the 5G system (Release 17): 3GPP TR21.917 [S]. 2019
[7] 3GPP. TSGS_94E_Electronic_2021_12 [EB/OL]. [2022-05-01]. https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_94E_Electronic_2021_12
[8] ZTE. ToBeEasy minimalist O&M technical white paper [R]. 2021.
[9] FANG M, DUAN X Y, HU L J. Challenges, innovations and perspectives towards 6G [J]. ZTE technology journal, 2020, 26(3): 61 – 70. DOI: 10.12142/ZTETJ.202003012.
[10] YANG F Y, LIU Y, YANG B. Reflections on 6G networks [J]. ZTE technology journal, 2021, 27(2): 2 – 5. DOI: 10.12142/ZTETJ.202102002.
[11] YAN X C, ZHOU N, JIANG Z H. Trusted communication technologies for future networks [J]. ZTE technology journal, 2021, 27(5): 52 – 59. DOI: 10.12142/ZTETJ.202105011.
[12] IMT-2030 Promotion Group. White paper on overall vision and potential key technologies [R]. 2021
[13] SU L, ZHUANG X J, DU H T, et al. Built-in security framework research for

6G network [J]. SCIENTIA SINICA informationis, 2022, 52(2): 205. doi: 10.1360/SSI-2021-0257
[14] IMT-2030 Promotion Group. 6G network security vision technology research report [R]. 2021
[15] ZTE. White paper on vision of intrinsic cybersecurity beyond 2030 [R]. 2021
[16] TANG J, XU A, JIANG Y, et al. Mmwave MIMO physical layer authentication by using channel sparsity [C]//IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS). IEEE, 2020: 221-224. DOI: 10.1109/ICAIIS49377.2020.9194916
[17] ZHANG C L, FU Y L, LI H, et al. Research on security scenarios and security models for 6G networking [J]. Chinese journal of network and information security, 2021, 7(1): 28 – 45
[18] NIU J H, HUANG H, WANG W B, et al. Analysis of the blockchain technology and its application in 6G networks [J]. Information & communications, 2020, 215: 1673 – 1131

Biographies

LU Haitao received his MS degree from Beijing University of Posts and Telecommunications, China in 1995. He is a senior engineer and got the CISSP in 2019. He is currently a senior system architect with ZTE Corporation and has been engaged in wireless communication technology R&D for a long time. He has led many National Science and Technology Major Projects and National High-Tech R&D Programs ("863" Programs), and has more than 60 patents. He received the Scientific and Technological Innovation Progress Awards of Guangdong Province.

YAN Xincheng received his MS degree from Southeast University, China in 2004. He is a professorate senior engineer and chief system security architect of ZTE Corporation. He has presided over the National Science and Technology Major Project of China in 5G security and has more than 40 patents. He has won several scientific and technological awards and won the titles of "333" third-level talent and high-level talent in Jiangsu Province.

ZHOU Qiang (zhou.qiang@zte.com.cn) received his bachelor's and master's degrees from Nanjing University of Aeronautics and Astronautics, China in 1998 and 2001, respectively. He is a senior engineer and obtains more than ten patents for invention. He has worked with ZTE Corporation since his graduation. He has been engaged in wireless communication research, including 3G, 4G and 5G communication systems. For the last ten years he was the director of R&D department in charge of 5G product development and 6G advanced research.

DAI Jiulong received his bachelor's degree from Hunan University in 2014 and is currently working with ZTE Corporation. He has been committed to wireless protocol stack development and wireless security technology research and planning. His research interests are concentrated in RAN and algorithm security technologies.

LI Rui received his bachelor's degree from Wuhan University, China in 2005 and his master's degree from University of Science and Technology of China in 2008, respectively. He is currently working with ZTE Corporation and his interests and research scope of work focus on 5G RAN and edge cloud native security technologies.

Air-Ground Integrated Low-Energy Federated Learning for Secure 6G Communications

WANG Pengfei[1], SONG Wei[1], SUN Geng[2,3], WEI Zongzheng[1], ZHANG Qiang[1]

(1. School of Computer Science and Technology, Dalian University of Technology, Dalian 116024, China;
2. School of Computer Science and Technology, Jilin University, Changchun 130015, China;
3. Key Laboratory of Symbolic Computing and Knowledge Engineering, Jilin University, Changchun 130015, China)

DOI: 10.12142/ZTECOM.202204005

https://kns.cnki.net/kcms/detail/34.1294.TN.20221205.1627.001.html, published online December 6, 2022

Manuscript received: 2022-09-09

Abstract: Federated learning (FL) is a distributed machine learning approach that could provide secure 6G communications to preserve user privacy. In 6G communications, unmanned aerial vehicles (UAVs) are widely used as FL parameter servers to collect and broadcast related parameters due to the advantages of easy deployment and high flexibility. However, the challenge of limited energy restricts the popularization of UAV-enabled FL applications. An air-ground integrated low-energy federated learning framework is proposed, which minimizes the overall energy consumption of application communication while maintaining the quality of the FL model. Specifically, a hierarchical FL framework is proposed, where base stations (BSs) aggregate model parameters updated from their surrounding users separately and send the aggregated model parameters to the server, thereby reducing the energy consumption of communication. In addition, we optimize the deployment of UAVs through a deep Q-network approach to minimize their energy consumption for transmission as well as movement, thus improving the energy efficiency of the air-ground integrated system. The evaluation results show that our proposed method can reduce the system energy consumption while maintaining the accuracy of the FL model.

Keywords: federated learning; 6G communications; privacy preserving; secure communication

Citation (IEEE Format): P. F. Wang, W. Song, G. Sun, et al., "Air-ground integrated low-energy federated learning for secure 6G communications," *ZTE Communications*, vol. 20, no. 4, pp. 32 - 40, Dec. 2022. doi: 10.12142/ZTECOM.202204005.

1 Introduction

Even though 5G specifications are still being developed, 6G of mobile communications has already attracted great attention from both academia and industry[1]. Compared with 5G communications, 6G[2] will achieve faster speed, higher energy efficiency, wider coverage, etc. However, the wireless channel used for 6G is usually open, which gives wireless users the freedom to communicate but brings insecurity factors at the same time[3]. For example, the communication content can be easily eavesdropped or tampered with[4]. At the same time, data servicers collect large amounts of user information[5], which leads to frequent private data leaks. These factors pose a threat to the data security of 6G users.

Federated learning (FL) is a distributed machine learning framework[6]. In FL, participants train the model with local datasets and upload the obtained model parameters instead of the user privacy data to the parameter server, which aggregates the parameters to obtain the updated global model. With the distributed nature of FL, users can benefit from the global model while keeping the data in their own hands[7-8]. Therefore, utilizing FL at the 6G edge can protect user data, thus making users more willing to participate and fully utilize the value of their local dataset for the training of the global model[9]. In recent years, there have been some studies on integrating FL into wireless communication to improve its privacy and security[10-12], but they still face many realistic problems, e.g., low deployment flexibility in terrestrial communication networks and huge communication costs.

Unmanned aerial vehicles (UAVs) have the advantages of high flexibility and mobility which can give FL more possibilities. Specifically, it can easily provide air-ground integrated

This work was supported in part by the National Key Research and Development Program of China under Grant No. 2021ZD0112400, the NSFC under Grant No. 62202080, the NSFC-Liaoning Province United Foundation under Grant No. U1908214, the CCF-Tencent Open Fund under Grant No. IAGR20210116, the Fundamental Research Funds for the Central Universities under Grant Nos. DUT21TD107 and DUT20RC(3)039, and the Liaoning Revitalization Talents Program under Grant No. XLYC2008017.

line-of-sight communication and effectively improve the transmission range of terahertz signals in 6G networks. As a result, the air-ground integrated network (AGIN) has gradually become the trend for 6G development, aiming to provide users with ubiquitous connectivity and seamless global coverage. In this paper, we consider the organic combination of the air-ground integrated network and FL in the 6G network. We utilize UAVs as parameter servers for FL to collect data from dispersed users, providing wider coverage for users while protecting the private data of 6G users. However, in 6G communications, the framework will face the challenge of limited energy for mobile users as well as for UAVs[13-14]. Specifically, users are reluctant to spend too much energy on the FL process, and the UAV does not have a constant source of energy to support multiple rounds of the FL model transfer and aggregation process. As a result, it may lead to delays in updating the global model. Therefore, to achieve a sustainable FL solution, the issue of energy efficiency in the system has to be considered. Existing solutions that optimize the energy efficiency of air-ground integrated FL[15] generally focus on UAV scheduling optimization and resource allocation, in which mobile devices need to communicate directly with the server, which may increase energy consumption.

In this paper, we propose air-ground integrated low-energy federated learning (AGILFL). Specifically, we use terrestrial base stations (BSs) as message middleware for users and the UAV parameter server to aggregate model parameter updates from their surrounding users separately and send the aggregated model parameters to the server, thus reducing the energy consumption of communication. In addition, deep Q-network (DQN) is adopted to optimize the deployment of UAVs, thus further reducing the overall energy consumption. To implement this procedure, we face the challenge that in some dynamic scenarios, the users' locations are not fixed[16], which would lead to a load on the BS when too many users move within a range of a certain BS. In such a case, users are required to send model parameters directly to the UAV server. To ensure that the 6G communication is always highly reliable, we consider predicting the BS load situation in advance and performing an emergency scheduling for the UAV. Our main contributions are summarized as follows:

1) We propose AGILFL, a framework that integrates AGIN and FL, which is devised to provide low-energy FL for secure 6G communications.

2) We use hierarchical aggregation to reduce the communication consumption efficiency of AGILFL by using BSs as middleware between users and the UAV parameter server significantly. The BS collects and aggregates the updated parameters of users within its coverage area, and sends the aggregated parameters to the UAV server for a second aggregation. With this approach, we can reduce the aggregation workload of the UAV server and the redundant communication between the UAV and users.

3) To ensure the reliability of 6G communication, we consider predicting the BS load situation in advance and urgently dispatching the UAV to cope with extreme situations, e.g., scenarios with a high density of smart devices such as weekend supermarket promotions and concerts, etc.

4) Extensive evaluation experiments are conducted on the MINIST dataset to demonstrate the effectiveness of our proposed method. Experiments have shown that our method can improve the system's overall energy efficiency while maintaining the model's accuracy, which is better than the comparison algorithm.

The remainder of this paper is organized as follows. Section 2 presents the current research work combining FL and wireless networks, with consideration of their energy consumption. Section 3 provides an overview of FL and presents the system model and problem formulation of this paper. DQN and our allocation strategy for the UAV are introduced in Section 4. Section 5 verifies the effectiveness of AGILFL through experiments. Finally, we summarize the contributions and experiments of this paper and present future work in Section 6.

2 Related Work

FL enables a large number of users to train a machine learning (ML) model together in a distributed manner, as a result, it provides a secure and effective training model for ubiquitous 6G intelligence. Recently, studies have explored how FL can be integrated into wireless networks while considering their energy consumption. TRAN et al.[17] proposed a wireless FL model that implemented a trade-off between FL learning time and user energy consumption. HAMER et al.[18] proposed another FL approach to reduce the costs of server-to-client and client-to-server communications by building an ensemble of pretrained base predictors. However, the above studies are limited to terrestrial networks.

ZENG et al.[19] first investigated the possibility of implementing FL on UAVs. They proposed an optimization issue by considering the problem of limited energy of UAVs and designing algorithms to optimize the convergence performance of FL, thus reducing the energy consumption of UAVs in the system. SHIRI et al.[20] proposed an algorithm that combined channel allocation as well as equipment scheduling optimization to reduce the communication among swarms of a large number of UAVs. PHAM et al.[21] proposed a sustainable federal learning framework that used UAVs to provide wireless power to energy-limited FL participants' devices while improving the energy efficiency of UAVs. However, none of the above methods consider integrating UAVs into terrestrial communication networks.

To make full use of UAVs, QU et al.[22] first proposed a conceptual framework of air-ground integrated federated learning (AGIFL) to give FL greater flexibility, thus enhancing the much-needed artificial intelligence in 6G communication networks. JING et al.[23]verified for the first time the feasibility of FL de-

ployment between UAVs and the terrestrial network through a practical platform based on AGIFL. However, none of them solves the problem of the huge energy consumption of the system.

In summary, few extant studies has considered how to reduce the energy consumption of AGIFL. In addition, the above approaches require terminal nodes to communicate directly with the parameter server, which may increase transmission costs. Therefore, in this paper, we propose AGILFL, in which BSs are used as message middleware between users and the UAV parameter server in the FL system. We also use the DQN algorithm to optimize the location of the UAV and minimize the total energy consumption for its movement and transmission, so that AGIFL can effectively reduce the energy consumption of the system.

3 Preliminaries

3.1 Federated Learning

FL is a distributed ML approach that trains shared models in the context of protecting individual privacy. In FL, many participants train the global model in cooperation through a parameter server by aggregating model parameter updates[24]. Participants download the latest global model from the parameter server in each communication round, train the model on their own devices using local datasets, and then upload the updated parameters of the trained model to the server. The server then aggregates (e.g., using FedAvg[6]) the collected updates to get a new global model. In the process, users can benefit from the global model while keeping the data in their own hands.

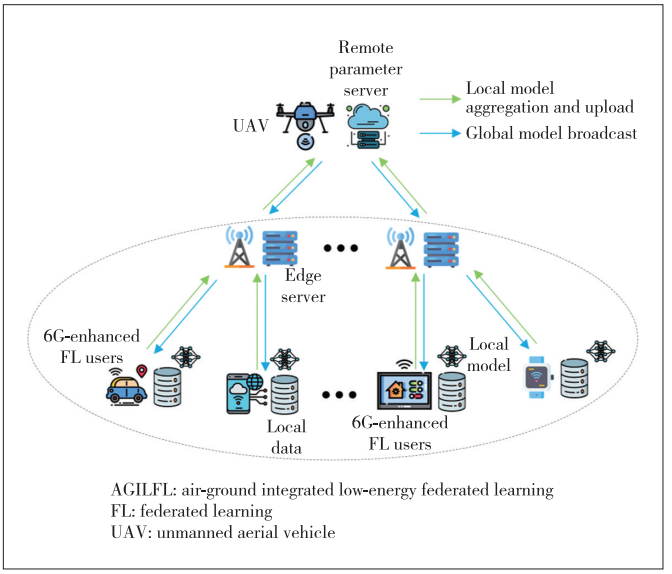
Let $[n]=\{1,\cdots,n\}$ represents the set of participants, the private dataset for each participant i is D_i for $i\in[n]$, and $D=D_1\cup D_2\cup\cdots\cup D_n$ is the complete training dataset. In the t-round of communication rounds, the participant i first downloads the latest global model w_t from the parameter server and then conducts local training. Then, the cumulative computational gradient $w_{t+1}^{(i)}-w_t$ is sent to the parameter server for the global model update, e.g., using FedAvg as in Eq. (1).

$$w_{t+1}=w_t+\frac{1}{n}\sum_{i\in[n]}\left(w_{t+1}^{(i)}-w_t\right). \tag{1}$$

Note that the above process will be repeated until the global model reaches convergence.

3.2 System Model

In this paper, we consider an air-ground integrated 6G communication FL system that can protect the private security of 6G users, as shown in Fig. 1. It consists of a UAV server, m users (e. g., mobile users, Internet of things devices, and the UAV carrying data), and n BSs. These devices are randomly distributed in the air-ground domain. We define the set of users as $U=\{u_1,u_2,\cdots,u_m\}$, the UAV server as V, the n BSs as $B=\{b_1,\cdots,b_n\}$, and the model size of FL training is Ω.



▲Figure 1. Overview of AGILFL's framework

The user u_i is a participant who provides the model in the FL system. The user u_i receives the global model from the BS or the UAV, uses its own data for local training, and sends the trained model to the BS or the UAV. We define that if the user transmits the global model parameters to BS b_j, then $x_{ij}=1$, $y_i=0$; otherwise, the user passes the global model parameters to the UAV, and then $\sum_j x_{ij}=0$, $y_i=1$. The transmission rate[25] from user u_i to UAV V is expressed in Eq. (2).

$$R_i=b_i\log_2\left(1+\frac{g_i p_i}{b_k N_0}\right), \tag{2}$$

where b_i, g_i, p_i, and N_0 represent transmission bandwidth, channel gain, transmission power, and noise power density respectively. In order to ensure that Ω is transmitted within the upload time t_i, constraint $\Omega\leqslant R_i t_i$ needs to be satisfied. In this case, the energy transmitted to BS E_i^{u2b} and the energy transmitted to UAV E_i^{u2v} are expressed in Eq. (3).

$$E_i^{u2b}=E_i^{u2v}=t_i p_i. \tag{3}$$

In this paper, we use BS b_j as the message middleware between users and UAV V in the FL system. The BS set B is responsible for processing the global model parameters sent by surrounding users and then aggregating them. After aggregation, B will send the aggregation results of the global model parameters to UAV V. The transmission rate from BS b_j to UAV V is R_j. We assume that the transmission power of the BS is defined as p_j. Within the upload time t_j, the energy transferred between BS b_j and UAV is defined as E_j^{b2v}, which is the same as the calculation method of energy when the user transfers global model parameters.

When transferring global model parameters, we have the fol-

lowing restrictions. There is path loss during the transmission of global model parameters, that is, with the increase of transmission distance, the power gradually decreases. The corresponding relationship is expressed in Eq. (4).

$$P_r\left(P_s,l_s,l_r\right)=\varsigma\frac{P_s}{d^2\left(l_s,l_r\right)}, \tag{4}$$

where P_s and P_r represent the transmission power of the sender and the receiver respectively, l_s and l_r represent the location of the sender and the receiver respectively, $d(\cdot)$ is the distance function, and ς is the influence factor under different environments. We also limit the minimum received power of all devices to $p_{\min}$.

UAV V acts as the global model manager of the FL system. UAV V is responsible for automatically sending or receiving global model parameters from surrounding users or base stations, aggregating local training models, and updating global model parameters. We assume that UAV V has a fixed height H and moves only in the horizontal direction. Suppose the position of the UAV is $l=(x,y)$ and the position after moving is $l'=(x',y')$. According to Ref. [26], the energy of UAV V movement is expressed in Eq. (5).

$$E_s(l,l')=P_H\frac{d(l,l')}{v_h}, \tag{5}$$

where v_h is the velocity in the horizontal direction and P_H represents the power consumed by the energy of horizontal movement. P_H can be expressed in Eq. (6).

$$P_H=P_p+P_I, \tag{6}$$

where P_p is the energy consumption power to overcome its own skin friction from drag and its calculation formula is shown as follows.

$$P_P=\frac{1}{2}\rho C_D S v_h^3+\frac{\pi}{4}M\rho c_b C_D w^3\beta^4\left(1+3\left(\frac{v_h}{w}\right)^2\right), \tag{7}$$

where C_D is the drag coefficient, c_b is the rotor chord, S is the front area of the UAV, w is the angular velocity, β is the rotor disk radius, and ρ denotes the fluid density of air. P_I is the energy consumed by the wing to redirect air to generate lift to compensate for the weight of the aircraft, and the specific formula is expressed as follows.

$$P_I=G\sqrt{\frac{\lambda-v_h^2}{2}}, \tag{8}$$

where $\lambda=\sqrt{v_h^4+\left(\frac{G}{\pi\rho\beta^2}\right)^2}$ and G is the gravity of the UAV.

3.3 Problem Formulation

Our goal is to optimize the UAV position to minimize the energy consumed by the entire FL system while protecting the private security of 6G users. Because parameter aggregation and global model update are necessary tasks of the FL system, the energy of parameter aggregation and global model update is not considered when the energy is minimized. Aiming to optimize the energy of the AGILFL system, we will focus on the optimization problems as in Eq. (9).

$$\min \sum_{i=1}^{m}\left(\sum_j x_{ij}E_i^{u2b}+y_iE_i^{u2v}\right)+\sum_{j=1}^{n}E_j^{b2v}+E_s(l,l'), \tag{9}$$

$$\text{s.t.}\quad x_i\in\{0,1\},y_i\in\{0,1\}, \tag{9a}$$

$$\sum_j x_{ij}+y_i=1,\forall i, \tag{9b}$$

$$t_iR_i\geqslant\Omega,\forall i, \tag{9c}$$

$$t_jR_j\geqslant\Omega,\forall j, \tag{9d}$$

$$0<l'<l_{\max}, \tag{9e}$$

$$P_r\left(p_i,l_i,l_j\right)\geqslant x_{ij}p_{\min},\forall i,j, \tag{9f}$$

$$P_r\left(p_i,l_i,l'\right)\geqslant y_ip_{\min},\forall i, \tag{9g}$$

$$P_r\left(p_j,l_j,l'\right)\geqslant p_{\min},\forall j, \tag{9h}$$

where x_{ij} represents whether user u_i sends local model parameters to BS b_j, y_i indicates whether user u_i sends local model parameters to UAV V, E_j^{b2v} denotes the energy required for BS b_j to transmit to UAV V, l_i represents the location of user u_i, l_j means the location of BS b_j, l indicates the initial location of UAV V, l' shows the location of UAV V after it moves, and $l_{\max}$ represents the maximum movement range of UAV V.

In the problem, Constraint (9a) limits the range of values of x_i and y_i; Constraint (9b) denotes that the user sends the global model parameters to either the BS or the UAV; Constraints (9c) and (9d) limit the time and rate of transmission parameters to ensure that the model size of FL training Ω is transmitted within upload time t_i or t_j; Constraint (9e) limits the range of movement of the UAV; Constraints (9f), (9g) and (9h) indicate that the power of the signal received by all the devices must be higher than the minimum power.

4 Allocation Strategy of UAV

In this section, we detail the strategy for UAV deployment. The algorithm we propose in this paper consists of two sepa-

rate processes: model training and model application. We first train the model by the DQN algorithm to obtain the output Q-network model. Then we continuously update the environmental state of UAV V and put it into the Q-network to make the optimal action decision for the current state.

4.1 Deep Q-Network

The DQN algorithm is a reinforcement learning method combining deep learning and Q-learning, which has both the powerful feature-aware capability of deep learning and the trial-and-error learning advantage of reinforcement learning. In the DQN algorithm, $Q(s, a)$ represents the value assessment of action a taken by the agent under state s, and the agent selects the action with the highest Q value to perform to obtain a higher reward. In the Q-learning method, the Q-table is used to store the corresponding Q values of the actions in each state. However, the disadvantage of Q-learning is that it takes up a lot of memory space in a more complex state space and the calculation process is also complicated. Compared with traditional Q-learning, DQN can compute the Q-table of the current state in a huge state space as in Eq. (10).

$$Q_\theta(s, a) = Q(s, a), \tag{10}$$

where $Q_\theta(s, a)$ is a neural network with parameter θ, which is called Q-network, and its output result is an estimate of Q.

DQN proposes two improvements to overcome the problems of unstable learning targets and excessive correlation of consecutive samples: 1) experience replay; 2) target Q-network. In this context, the goal of the training process is to minimize the value of the loss function, and the loss function is the mean-square error between the target Q value and the Q value, which is expressed as in Eq. (11).

$$D(\theta_i) = E_{s,a,r,s'}[(Y_i - Q(s, a|\theta_i))^2], \tag{11}$$

where θ_i is the parameter of Q-network; Y_i is the target Q value. The formula is expressed as in Eq. (12).

$$Y_i = \gamma \max_{a'} Q(s', a'|\theta_i') + r, \tag{12}$$

where θ_i' is the parameter of the target Q-network. By fixing the Q value, the stability of the Q value can be guaranteed for a period of training time.

Algorithm 1. DQN model training for the UAV parameter server

Input: Distribution of BSs and users, state space and action space of UAV, learning rate α, and discount rate γ.

Output: Q-network $Q(s, a)$

1. Initialize action space A, state space S, learning rate α, discount rate γ, and replay buffer M.
2. Initialize Q-network parameters θ and target Q-network parameters θ'
3. **for** I in max_epoch **do**
4. Let the users move.
5. Calculate the energy consumption for the new system.
6. Initialize s as the previous state of the UAV parameter server;
7. Decide which action to be taken, using the greedy algorithm
8. Take action a, calculate reward r_t, and calculate the next state s' of the UAV parameter server;
9. Store interaction information (s, a, r_t, s') in experience pool M
10. Random batch sampling of batch samples $(s_i, a_i, r_{sum,i}, s_i')$ from M
11. $Q_i = \begin{cases} r_{\text{sum},i}, & \text{if } s' \text{ is terminal} \\ r_{\text{sum},i} + \gamma \max Q_{\theta'}(s', a') \end{cases}$
12. $\sum_{i=1}^{\text{batch}}(Q_i - Q_\theta(s, a))$ as the loss function
13. Update state s of the UAV parameter server;
14. Update the Q-network $\theta' \leftarrow \theta$;
15. **end for**
16. output Q-network $Q(s, a)$

4.2 Allocation Strategy

We use the DQN algorithm to determine the 3D position of UAV V, thereby minimizing its communication and movement costs. The DQN algorithm predicts the value of the agent's behavior through a deep neural network, thus allowing the agent to obtain a higher return in subsequent decisions. Specifically, in our method, UAV V needs to decide on the appropriate working position based on the large number of distributed BSs around, which is a more complex task scenario. Due to many environmental elements in complex scenes in reinforcement learning, not only will it increase the training cycle and slow down the convergence of the model, but also bring the problem of sparse rewards, which causes the model to work improperly. Aiming to solve the potential sparse reward problem, we propose an energy field model to abstract various parameters in the environment and simplify the UAV state representation, thus speeding up the model convergence and avoiding the sparse reward problem. The energy field is modeled as in Eq. (13).

$$E = \sum_{i=1}^{n} \frac{\varepsilon L_i D_i U_{ri}}{d_i}, \tag{13}$$

where ε is the weight parameter used to control the order of magnitude of energy; d_i is the Euclidean distance between V and b_i; L_i is the load situation of b_i; D_i is the number of data that b_i needs to transmit to V; U_{ri} is the number of users connected to b_i. The formula calculates the energy situation of the UAV's location, and the total energy is the sum of the sub-energy of all BSs. The higher value of E means more users and base station loads near the point and more need for UAV V to serve. This energy field model can guide UAV V to fly to a

more suitable working area and also generate the corresponding decision for the high load situation in the area.

The state space of UAV V is composed of spatial coordinates, current energy consumption power, user coverage, and BS coverage. For the action space of UAV V, we have defined six possible actions: forward, backward, left, right, up, and down. The six actions are denoted as $a_1, a_2, \cdots, a_6$ respectively. If the energy consumption of the transmission of UAV V is higher than the previous energy consumption, UAV V needs to change its location. In this case, the agent must make behavioral decisions based on the state of the environment in which it is located. UAV V takes action a_j based on decisions and transfers to a new state s', while receiving a reward or punishment according to the reward rule to optimize the behavioral decision of the intelligence.

The purpose of this section is to determine suitable UAV locations to reduce the energy loss of the mission and also to perform emergency scheduling for possible regional loads (such as large sporting events, supermarket events, concerts, etc.). Combined with the energy field model proposed above, this paper proposes the reward function as in Eq. (14).

$$r_t = \Delta E + \omega \frac{D_{\text{sum}}}{E^{u2b} + E^{u2v} + E_s(l,l')}, \tag{14}$$

where ΔE is the change in energy at the location of the UAV. When the energy increases, which means that UAV V flies to a more suitable space position, it will be rewarded and the opposite will be punished; ω is the weight parameter that controls the order of magnitude of the reward; D_{sum} is the total amount of data transferred by the system.

Algorithm 2. DQN algorithm for 3D placement of the UAV parameter server

Input: Distribution of BSs and users, Q-network $Q(s, a)$
Output: Optimum position of the UAV parameter server
1. E_{th} is the calculated energy consumption for communication among UAV, users and BSs and UAV movement.
2. **while** the system is running **do**
3. Let the users move.
4. Calculate the energy consumption for the new system.
5. **if** (the energy consumption > E_{th}) **then**
6. **for** step in max_step **do**
7. Initialize s as the previous state of the UAV parameter server;
8. input s into $Q(s, a)$ to get the best decision a_t
9. Take action a_t, calculate the next state s of the UAV parameter server;
10. Update state s of the UAV parameter server;
11. **end for**
12. **else**
13. There is no need to move the UAV parameter server
14. **end if**
15: **end while**

The algorithm we propose in this paper consists of two separate processes: model training and model application. The training is performed in a simulated environment, the specific details are shown in Algorithm 1, where the target Q-network and Q-network are first initialized to predict the Q value of the previous step of the behavior and the current Q value, respectively. In each training epoch, the environmental status of UAV V is first updated, such as pedestrian movement, BS model aggregation, BS load, user model training, system energy consumption, etc. Then current state s of the UAV is determined according to the external state, and is input into the Q-network to get the Q values of all actions. Action a is selected for execution based on the greedy method, UAV state s is changed to s' after the execution of the action, and then reward information r_t is obtained. Then quaternion (s, a, r_t, s') is stored in replay buffer M and batch samples are taken from M to train the Q-network. After that, the Q-network is updated with the target Q-network and finally, the Q-network model is output. Although the process of training UAV V requires some energy, the energy consumption of the proposed DQN method is much smaller and even negligible compared with the traditional greedy scheme[27].

Algorithm 2 shows the process of applying our DQN model, which continuously updates the environment state during the system operation and then calculates the required energy consumption of the system. If the energy consumption is greater than the threshold value, it means that UAV V is required to move, and in this process, UAV V constantly updates its state and inputs the state into the Q-network. UAV V makes action decisions based on the Q-network output and then updates the environment state until the step reaches the max.

5 Experiment and Evaluation

In this section, we evaluate the performance of our proposed algorithm. Firstly, we introduce the default settings, datasets, benchmarks, and metrics in detail. Secondly, we evaluate the utility of AGILFL on the overall energy. Finally, we evaluate the utility of AGILFL on average resource utilization and model accuracy.

5.1 Default Settings

We consider that the FL system is composed of users, BSs, and the UAV. In order to reduce the space for parameter search, we set up 100 users, 5 BSs, and 1 UAV. Each trainable device trains locally using the lenet-5 model. The maximum number of iterations of the global model is set to 200, which is optimized by the mini batch stochastic gradient descent (SGD) optimizer, and the minimum mini batch is 50. During model training, the learning rate is set to 0.03, and the loss function uses cross entropy. The maximum epoch to train the UAV mobile model is set to 200, and the maximum epoch to train the FL model is set to 40.

5.2 Dataset

We use a well-known image classification data set named MINIST, which is composed of 70 000 grayscale pictures of 28 × 28 pixels and each picture corresponds to a number from 0 to 9. In the MINIST dataset, 55 000 pictures are used as the training set, 5 000 pictures as the verification set, and 10 000 pictures as the test set. In our experiment, we evenly place 55 000 pictures among 50 users, and each device contains 1 000 pictures. The parameter UAV places 10 000 pictures as a test set for model training.

5.3 Benchmarks

Firstly, in order to evaluate the advantage of the AGILFL system, we choose the FL system without BSs and the multi-hop transmission (MHT) with BSs as the benchmark. They all have the same number of users. Secondly, in assessing the advantage of AGILFL UAV training, we use DQN training and random movement as benchmarks. Finally, to prove that AGILFL can achieve precision without degradation, we use FL and ML as benchmarks. AGILFL, ML and FL use the same number of data for training, and AGILFL and FL have the same number of users.

5.4 Metrics

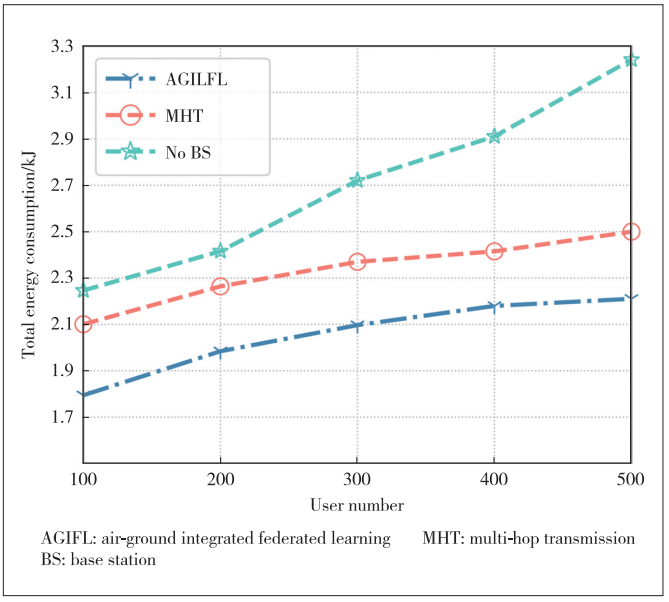
We adopt the total energy consumption as an evaluation metric, that is, the energy consumed by the whole system in energy transmission and UAV movement during each training of FL. In assessing the UAV training performance of AGILFL, we use the reward function during training as a metric. Finally, we also use accuracy as a metric to evaluate the impact on the FL model accuracy.

5.5 Results Analysis

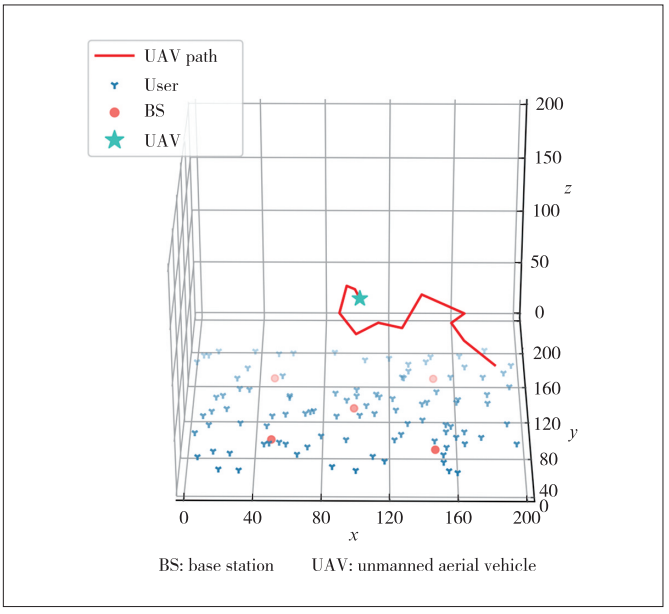
We uniformly generate five BSs in the 200×200×200 air-ground integrated area. To evaluate the impact of user growth on total energy consumption, we randomly generate 100 to 500 users in the region and calculate the total energy consumption. Fig. 2 shows the energy comparison of AGILFL and other benchmarks in the AGIFL system. AGILFL can reduce the total energy consumption by using the BSs as caching devices and by controlling the UAV to find the best position. This experiment shows that AGILFL reduces the overall energy by 11.9% and 18.4% respectively, compared with the other two algorithms.

Our UAV, which is trained to complete the DQN intensive learning network, is placed in the AGIFL system. The UAV starts from a random point and moves in the FL system according to the movement strategy. Fig. 3 shows the trajectory of the UAV in AGILFL. Each step of the UAV's movement maximizes the reward function. Every step the UAV moves, it moves toward the BS and is close to the central BS. We can also see that UAVs will not be far away from users or base stations to avoid wasting energy.

In default settings, we evaluate the performance of the UAV



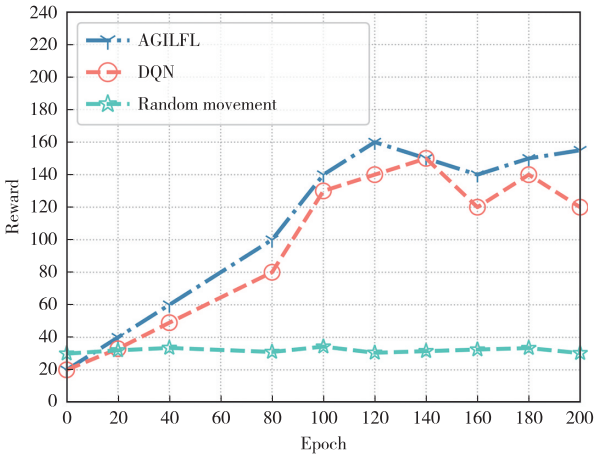
▲Figure 2. Performance of total energy consumption



▲Figure 3. Movement trajectory of UAV

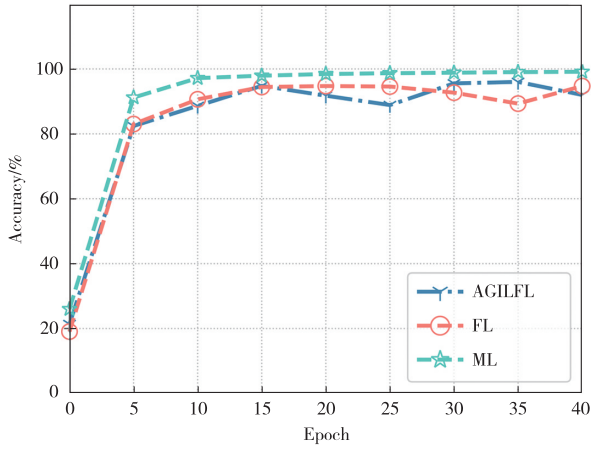
movement strategy. Fig. 4 shows the performance of our optimization algorithm. In the AGIFL system, we use AGILFL, DQN algorithm and random movement respectively to compare their performance in the reward function. AGIFL adopts DQN with an empirical replay algorithm. AGILFL can learn the optimal parameters faster than the DQN algorithm, and experience replay can make the training more stable. Compared with the other two algorithms, AGILFL improves the reward function by 59.5% and 13.5%, respectively.

In default settings, we evaluate the accuracy change of the training model using users' data in different scenarios. Fig. 5 shows the accuracy performance of AGILFL, FL, and ML. AGILFL can reduce total energy consumption without causing



AGILFL: air-ground integrated low-energy federated learning
DQN: deep Q-network

▲Figure 4. Performance of reward



AGILFL: air-ground integrated low-energy federated learning
FL: federated learning
ML: machine learning

▲Figure 5. Performance of accuracy

serious accuracy degradation. Therefore, we propose AGILFL as a friendly, privacy-safe, and low-energy FL framework.

6 Conclusions and Future Work

In this paper, we investigate the problem of how to improve the energy efficiency of AGIFL and propose the AGILFL framework which can guarantee the private security of 6G users. Specifically, in AGILFL, we use a hierarchical aggregation method to improve the energy efficiency of communication by using BSs as middleware between users and the UAV parameter server. At the same time, to ensure that the 6G communication is always in a highly reliable state, we predict the overloaded BSs in advance and make emergency scheduling of the UAV. We use the DQN algorithm to optimize the position of the UAV to minimize the overall energy consumption for UAV movement as well as communication. Finally, through simulation experiments, our proposed method is proven to be real and effective. Compared with the baseline, AGILFL reduces the overall energy by 11.9% and 18.4%, respectively, and improves the reward function by 59.5% and 13.5%, respectively.

The way to reduce the energy consumption of local computing for 6G users in the AGILFL framework is not explored in this paper. In the mechanism we designed, we should also consider a replacement option when the UAV is almost out of power. Our future work will focus on addressing the above issues and exploring the possibility of applying our solutions on a large scale in real-world environments.

References

[1] DANG S P, AMIN O, SHIHADA B, et al. What should 6G Be? [J]. Nature electronics, 2020, 3(1): 20 – 29. DOI: 10.1038/s41928-019-0355-6
[2] GUI G, LIU M, TANG F X, et al. 6G: opening new horizons for integration of comfort, security, and intelligence [J]. IEEE wireless communications, 2020, 27 (5): 126 – 132. DOI: 10.1109/MWC.001.1900516
[3] WANG C G, RAHMAN A. Quantum-enabled 6G wireless networks: opportunities and challenges [J]. IEEE wireless communications, 2022, 29(1): 58 – 69. DOI: 10.1109/MWC.006.00340
[4] WANG M H, ZHU T Q, ZHANG T, et al. Security and privacy in 6G networks: new areas and new challenges [J]. Digital communications and networks, 2020, 6(3): 281 – 291. DOI: 10.1016/j.dcan.2020.07.003
[5] NGUYEN V L, LIN P C, CHENG B C, et al. Security and privacy for 6G: a survey on prospective technologies and challenges [J]. IEEE communications surveys & tutorials, 2021, 23(4): 2384 – 2428. DOI: 10.1109/COMST.2021.3108618
[6] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data [EB/OL]. (2016-02-17)[2022-09-01]. https://arxiv.org/abs/1602.05629v2
[7] YANG Q, LIU Y, CHEN T J, et al. Federated machine learning [J]. ACM transactions on intelligent systems and technology, 2019, 10(2): 1 – 19. DOI: 10.1145/3298981
[8] LI T, SAHU A K, TALWALKAR A, et al. Federated learning: Challenges, methods, and future directions [J]. IEEE signal processing magazine, 2020, 37 (3): 50 – 60. DOI: 10.1109/MSP.2020.2975749
[9] YANG Z H, CHEN M Z, WONG K K, et al. Federated learning for 6G: Applications, challenges, and opportunities [J]. Engineering, 2022, 8: 33 – 41. DOI: 10.1016/j.eng.2021.12.002
[10] LIU Y, PENG J L, KANG J W, et al. A secure federated learning framework for 5G networks [J]. IEEE wireless communications, 2020, 27(4): 24 – 31. DOI: 10.1109/MWC.01.1900525
[11] CHEN M Z, GÜNDÜZ D, HUANG K B, et al. Distributed learning in wireless networks: recent progress and future challenges [J]. IEEE journal on selected areas in communications, 2021, 39(12): 3579 – 3605. DOI: 10.1109/JSAC.2021.3118346
[12] YANG M, WANG X M, QIAN H, et al. An improved federated learning algorithm for privacy preserving in cybertwin-driven 6G system [J]. IEEE transactions on industrial informatics, 2022, 18(10): 6733 – 6742. DOI: 10.1109/TII.2022.3149516
[13] YUAN Z W, TANG H, WANG P F, et al. Human-UAV collaborative task scheduling for 360° video generating in intelligent transportation [C]//The 8th

International Conference on Virtual Reality (ICVR). IEEE, 2022: 407 – 414. DOI: 10.1109/ICVR55215.2022.9847919
[14] WANG P F, YAN Z H, HAN G J, et al. A2E2: Aerial-assisted energy-efficient edge sensing in intelligent public transportation systems [J]. Journal of systems architecture, 2022, 129: 102617. DOI: 10.1016/j.sysarc.2022.102617
[15] JING Y Q, QU Y B, DONG C, et al. Joint UAV location and resource allocation for air-ground integrated federated learning [C]//IEEE Global Communications Conference. IEEE, 2021: 1 – 6. DOI: 10.1109/GLOBECOM46510.2021.9685150
[16] WANG P F, PAN Y Z, LIN C, et al. Graph optimized data offloading for crowd-AI hybrid urban tracking in intelligent transportation systems [J]. IEEE transactions on intelligent transportation systems, 2022: Early Access. DOI: 10.1109/TITS.2022.3141885
[17] TRAN N H, BAO W, ZOMAYA A, et al. Federated learning over wireless networks: optimization model design and analysis [C]//IEEE Conference on Computer Communications. IEEE, 2019: 1387 – 1395. DOI: 10.1109/INFOCOM.2019.8737464
[18] HAMER J, MOHRI M, SURESH A T, et al. FedBoost: communication-efficient algorithms for federated learning [C]//International Conference on Machine Learning. ICML, 2020: 3973 – 3983
[19] ZENG T C, SEMIARI O, MOZAFFARI M, et al. Federated learning in the sky: Joint power allocation and scheduling with UAV swarms [C]//IEEE International Conference on Communications. IEEE, 2020: 1 – 6. DOI: 10.1109/ICC40277.2020.9148776
[20] SHIRI H, PARK J, BENNIS M. Communication-efficient massive UAV online path control: Federated learning meets mean-field game theory [J]. IEEE transactions on communications, 2020, 68(11): 6840 – 6857. DOI: 10.1109/TCOMM.2020.3017281
[21] PHAM Q V, ZENG M, RUBY R, et al. UAV communications for sustainable federated learning [J]. IEEE transactions on vehicular technology, 2021, 70(4): 3944 – 3948. DOI: 10.1109/TVT.2021.3065084
[22] QU Y B, DONG C, ZHENG J C, et al. Empowering edge intelligence by air-ground integrated federated learning [J]. IEEE network, 2021, 35(5): 34 – 41. DOI: 10.1109/MNET.111.2100044
[23] JING Y Q, QU Y B, DONG C, et al. Joint UAV location and resource allocation for air-ground integrated federated learning [C]//IEEE Global Communications Conference. IEEE, 2021: 1 – 6. DOI: 10.1109/GLOBECOM46510.2021.9685150
[24] WANG P F, ZHAO Y A, OBAIDAT M S, et al. Blockchain-enhanced federated learning market with social Internet of Things [J]. IEEE journal on selected areas in communications, 2022, 40(12): 3405 – 3421. DOI: 10.1109/JSAC.2022.3213314
[25] PHAM Q V, LE M, HUYNH-THE T, et al. Energy-efficient federated learning over UAV-enabled wireless powered communications [J]. IEEE transactions on vehicular technology, 2022, 71(5): 4977 – 4990. DOI: 10.1109/TVT.2022.3150004
[26] LU J X, WAN S, CHEN X H, et al. Beyond empirical models: pattern formation driven placement of UAV base stations [J]. IEEE transactions on wireless communications, 2018, 17(6): 3641 – 3655. DOI: 10.1109/TWC.2018.2812167
[27] LIU L S, XIONG K, LU Y, et al. Age-constrained energy minimization in UAV-assisted wireless powered sensor networks: a DQN-based approach [C]//IEEE Conference on Computer Communications Workshops. IEEE, 2021: 1 – 2. DOI: 10.1109/INFOCOMWKSHPS51825.2021.9484487

Biographies

WANG Pengfei (wangpf@dlut.edu.cn) is currently an associate professor with the School of Computer Science and Technology, Dalian University of Technology, China. His current research interests include edge intelligent computing and federated learning.

SONG Wei is currently pursuing her master's degree with the School of Computer Science and Technology, Dalian University of Technology, China. Her current research interests focus on federated learning.

SUN Geng is currently an associate professor with the School of Computer Science and Technology, Jilin University, China. His current research interests include group intelligence and collaborative communications.

WEI Zongzheng is currently pursuing his master's degree with the School of Computer Science and Technology, Dalian University of Technology, China. His current research interests focus on federated learning.

ZHANG Qiang is currently a Changjiang Scholar Professor with the College of Computer Science and Technology, Dalian University of Technology, China. His research interests focus on artificial intelligence.

Physical Layer Security for MmWave Communications: Challenges and Solutions

HE Miao, LI Xiangman, NI Jianbing
(Department of Electrical and Computer Engineering, Queen's University, Kingston, Ontario K7L 3N6, Canada)

DOI: 10.12142/ZTECOM.202204006
https://kns.cnki.net/kcms/detail/34.1294.TN.20221206.1501.001.html, published online December 7, 2022
Manuscript received: 2022-09-11

Abstract: The mmWave communication is a promising technique to enable human commutation and a large number of machine-type communications of massive data from various non-cellphone devices like Internet of Things (IoT) devices, autonomous vehicles and remotely controlled robots. For this reason, information security, in terms of the confidentiality, integrity and availability (CIA), becomes more important in the mmWave communication than ever since. The physical layer security (PLS), which is based on the information theory and focuses on the secrecy capacity of the wiretap channel model, is a cost effective and scalable technique to protect the CIA, compared with the traditional cryptographic techniques. In this paper, the theory foundation of PLS is briefly introduced together with the typical PLS performance metrics secrecy rate and outage probability. Then, the most typical PLS techniques for mmWave are introduced, analyzed and compared, which are classified into three major categories of directional modulation (DM), artificial noise (AN), and directional precoding (DPC). Finally, several mmWave PLS research problems are briefly discussed, including the low-complexity DM weight vector codebook construction, impact of phase shifter (PS) with finite precision on PLS, and DM-based communications for multiple target receivers.

Keywords: mmWave communication; physical layer security; phased array; directional modulation

Citation (IEEE Format): M. He, X. M. Li, and J. B. Ni, "Physical layer security for mmwave communications: challenges and solutions," *ZTE Communications*, vol. 20, no. 4, pp. 41 – 51, Dec. 2022. doi: 10.12142/ZTECOM.202204006.

1 Introduction

The millimeter-wave (mmWave) communication employs high frequencies (30 – 300 GHz) as the carrier frequencies. With the advantage of high carrier frequencies, mmWave communication has much wider available spectrum than that of sub-6 GHz communication. It can provide high data transmission rates with wide spectrum bandwidths[1]. According to the Frequency Range 2 (FR2) defined in the 5G New Radio (NR)[2], the minimum channel spectrum bandwidth defined for FR2 is 50 MHz and the maximum is 400 MHz. With such wide spectrum bandwidths, the mmWave band 5G network can achieve the data transmission rate up to 1.8 Gbit/s[3]. In addition, due to the millimeter-level short wave length of mmWave, the physical dimension of antennas for an mmWave communication device can be greatly reduced. Hundreds to thousands of antenna elements can be integrated as a phased array on the device to enable narrow beamforming[4]. Therefore, mmWave wireless communication is one of the key technologies in 5G NR for 5G mobile networks[5 – 6] that can significantly increase the data transmission rate over small and densely populated areas. It is also expected to be applied in the 6G mobile network, which can support the future growing network applications in the Internet of Things (IoT), the Vehicle-to-everything (V2X), etc.[7 – 8]

Despite the appealing characteristics and applications, the mmWave communications are vulnerable to eavesdropping due to the open nature of the wireless medium[8 – 10]. Eavesdroppers may intercept the communication[10] by residing in the transmitting beam. Such vulnerability threats the confidentiality of some sensitive information, such as financial data, electronic media and medical records. To minimize the risk of sensitive information leakage from mmWave communications, preserving the secrecy is essential in the design and implementation of the mmWave communication system[8, 11].

The traditional cryptography technique is an effective tool to protect the information security. However, traditional cryptography techniques can hardly meet the new requirements of the mmWave communication security. First, traditional cryptography techniques are all based on the mathematical computation complex problem and the secret key. Proper key management is essential to ensure the security. The huge device density and highly dynamic environment make it extremely difficult to design a safe key management protocol for traditional cryptography-based security schemes[12 – 13]. Second, traditional cryptography-based algorithms, especially asymmetric cryptography algorithms, require significant computation resource. Many devices in mmWave communication scenarios,

especially in the 5G network, are IoT devices. For the reason of cost control, these devices are typically built with very limited computational capabilities in terms of the CPU speed, storage size and power supply. Performing the traditional high-computation-cost cryptography algorithm on these resource limited devices may not only deteriorate the individual device life span but also result in poor performance[12, 14]. Lastly, a trusted third party is always required for system initialization and key management in the security scheme based on traditional cryptography. For security reasons, the trusted third party is typically remotely centralized. The dependence on a centralized third party limits the application within a centralized model, which limits the scalability of the mmWave communication, such as the supporting of up to one million devices in per square km[15–16] in 5G networks. And the frequent interactions with the remote party will cause additional delay and increase the system overhead.

Thus, physical layer security (PLS), which is based on the information theory and focuses on the secrecy capacity of the wiretap channel model, gains much attention from academia and industry. While applying to the mmWave communication security, the PLS techniques have significant advantages compared to the traditional cryptography techniques[15, 17]. First, the PLS technique is based on the information theory fundamentals, instead of computational complexity. It greatly reduces the burden on the devices to run the traditional heavy cryptography algorithms[18]. While naturally having good support on lightweight devices with limited computational and power resources, the PLS techniques can still protect the information security in the mmWave communication, even with the existence of powerful computational eavesdroppers[15]. Second, the PLS technique does not rely on the centralized trusted third party for system initialization and key management. The future network with mmWave communications may be with highly dynamic access[17], which means that any device may join or leave the network at any time, especially under mobile scenarios with the Internet of Vehicles (IoV) and unmanned aerial vehicles (UAV). The PLS technique can perform secure data transmission or user authentication directly without the time-consuming system setup. It not only significantly lowers the complexity of system management to lower the implementation cost, but also greatly reduces the latency with lower communication overhead.

In this paper, we first give a brief introduction to the theoretical foundation of PLS together with the typical PLS performance metrics secrecy rate and outage probability. Then, we introduce, analyze and compare the typical PLS techniques for mmWave, which are classified into three major categories of directional modulation (DM), artificial noise (AN), and directional precoding (DPC). Several schemes based on these techniques are discussed in detail to reveal each technique's advantages and constraints in the mmWave environment. Finally, we propose several future mmWave PLS research problems including low-complexity DM weight vector codebook construction, impact of phase shifter (PS) with finite precision on PLS, and DM-based communication for multiple target receivers. The definitions of frequently used acronyms are presented in Table 1.

▼**Table 1. Summary of Acronyms**

Acronym	Definition
ADC	analog-to-digital converter
AN	artificial noise
BS	base station
CE	constant envelope
CJ	cooperative jamming
CSI	channel state information
DAC	digital-to-analog converter
DM	directional modulation
DMC	discrete memoryless channel
DPC	directional precoding
IoT	Internet of Things
IoV	Internet of Vehicles
LOS	line-of-sight
LTE	Long-Term Evolution
MIMO	multiple-input and multiple-output
MISO	multiple-input single-output
OFDM	orthogonal frequency-division multiplexing
OTP	one time pad
PA	power amplifier
PAPR	peak to average power ratio
PLS	physical layer security
PS	phase shifter
QPSK	quadratic phase shift keying
RF	radio frequency
SNR	signal-to-noise ratio
UAV	unmanned aerial vehicle
ULA	uniform linear array

2 Theoretical Background for Physical Layer Security

The theoretical foundation of traditional cryptography is the number theory and abstract algebra. Different from traditional cryptography, the theoretical foundation of the PLS technique is the information theory. By minimizing eavesdroppers' channel capacity with the PLS techniques, information privacy can be preserved at a certain security level. Based on the definition of a channel, the PLS techniques can be classified into two major categories: one is the coding technique aiming at coding channels and the other is the signal processing technique aiming at modulation channels. In this section, we introduce the information theory related concepts in the PLS and review the wiretap channel and several performance evaluation metrics on PLS.

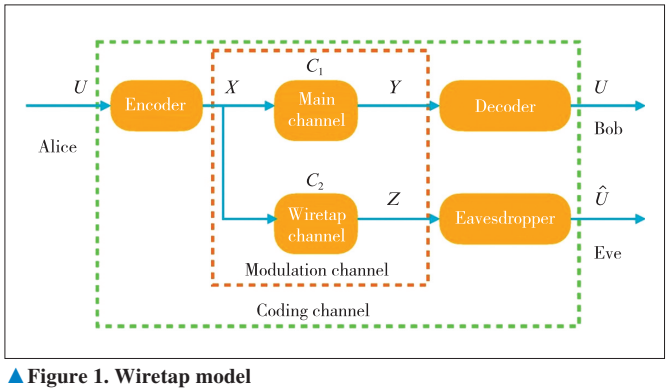
2.1 Perfect Security

Information security has been a topic in human history for thousands of years. The earliest known use of cryptography is found in the wall of a tomb from the Old Kingdom of Egypt circa 1900 BC[18]. Until the 1940s, information security in communications was first mathematically analyzed from the view of information theory by Claude Shannon. The concept of information-theoretically secure communication or "perfect security" was also introduced[19]. Perfect security means that the ciphertext gives absolutely no additional information about the plaintext. Shannon has proved that perfect security can be achieved with the one-time pad (OTP) even against adversaries with infinite computational power. Perfect security aims to protect the confidentiality of the information. While confidentiality is perfectly protected, integrity and availability can also be protected at a certain level.

2.2 Physical Layer Security

To achieve perfect security in communications from the view of information theory, there are extremely strict restrictions on the OTP. The OTP must be the same size as, or longer than, the message to be sent. The OTP must be pre-shared in a secure channel. The OTP can only be used once. These strong restrictions make perfect security only available to be implemented in very limited applications with extremely high costs. In most communications, the required security level does not have to achieve perfect security. On the other hand, the information security techniques should be scalable and affordable for daily use. For these reasons, an acceptable weaker level of information security known as PLS was defined in the wiretap channel model by WYNER in the 1970s[20]. Similar to perfect security, the PLS also focuses on the protection of information confidentiality.

In the wiretap channel model, three parties are defined, as shown in Fig. 1. They are Alice, Bob and Eve. Alice wants to send the message with particular information to Bob as private as possible. Eve eavesdrops the message from Alice to Bob and tries to get the information as much as possible. There are two channels in the model. One is between Alice and Bob (legitimate channel). The other is between Alice and Eve (wiretap channel). Due to the randomness of the physical medium (noise, interference, fading, etc.), differences between these two channels exist. The PLS techniques take advantage of these differences to make the channel from Alice to Bob statistically better than that from Alice to Eve. Thus, the channel capacity between Alice and Bob is higher than the wiretap channel between Alice and Eve. If the data rate from Alice is lower than that of the legitimate channel capacity but higher than the wiretap channel capacity, reliable communication could be achieved in the legitimate channel but not in the wiretap channel. In this way, information confidentiality can be preserved between Alice and Bob.



▲ **Figure 1. Wiretap model**

To measure the secrecy of PLS techniques, several performance metrics have been introduced in information theoretic terms. Among all the metrics, secrecy capacity and outage probably are the most accepted.

2.3 Secrecy Capacity

Secrecy capacity characterizes the maximal rate to meet two requirements in wiretap channels. One requirement is that Bob can reliably get the information in the message sent from Alice through legitimate channels. The other requirement is that Eve cannot get any information in the message sent from Alice through wiretap channel. For discrete memoryless channels (DMC), WYNER first introduced the secrecy capacity for the case of degraded channels[20] as

$$C_s = \sup_{p(X)} \{I(X;Y) - I(X;Y)\}, \tag{1}$$

where X is the input of information source, and Y and Z are the output of legitimate receiver and eavesdropper, respectively. X, Y and Z form a Markov chain $X \to Y \to Z$. The wiretap channel model for PLS in discrete memoryless channels can be extended to models in wireless channels[21]. Gaussian wiretap channel is widely accepted for PLS in wireless channels. It has linear time-invariant multiplicative links with additive white Gaussian noise. Thus, at interval i, the transmitted signal by Alice is X_i, and the received signals by Bob and Eve are $Y_{B,i}$ and $Y_{E,i}$, respectively. They can be expressed as

$$Y_{B,i} = h_B X_i + N_{B,i}, \tag{2}$$

$$Y_{E,i} = h_E X_i + N_{E,i}. \tag{3}$$

Here h_B and h_E are the channel gains for the legitimate channel and wiretap channel, respectively. $N_{B,i}$ and $N_{E,i}$ are the additive Gaussian noises. They are independent of the transmitted signal with zero means and variances σ_B^2 and σ_E^2, respectively. With the average transmit power constraint of P, the secrecy capacity can be expressed as

$$C_s = \frac{1}{2}\log\left(1 + \frac{P|h_B|^2}{\sigma_B^2}\right) - \frac{1}{2}\log\left(1 + \frac{P|h_E|^2}{\sigma_E^2}\right). \quad (4)$$

Note that the secrecy capacity in the Gaussian wiretap channel is equal to the difference between the legitimate channel's Shannon capacity C_M and the eavesdropper channel's Shannon capacity C_E, which can be formed as

$$C_s = C_M - C_E, \quad (5)$$

$$C_M = \frac{1}{2}\log\left(1 + \frac{P|h_B|^2}{\sigma_B^2}\right), \quad (6)$$

$$C_E = \frac{1}{2}\log\left(1 + \frac{P|h_E|^2}{\sigma_E^2}\right). \quad (7)$$

As a result, it can be concluded that secure communication is possible if and only if the legitimate channel is better than the wiretap channel, which is $|h_B^2|/\sigma_B^2 > |h_E^2|/\sigma_E^2$.

2.4 Secrecy Capacity

Another well-accepted PLS performance metric for the Gaussian wiretap channel is the secrecy outage probability introduced by BLOCH et al.[22] The secrecy outage is the event of instantaneous secrecy capacity C_S lower than the target secrecy rate R_S, which is $\{C_S < R_S\}$. The secrecy outage event will trigger the suspending of transmission. Thus, the outage probability is defined as

$$P_{\text{out}}(R_s) = P\{C_S < R_S\}. \quad (8)$$

3 Physical Layer Security Techniques Under MmWave Channel

The mmWave is the spectrum from 30 GHz to 300 GHz. It is receiving lots of interest from academia, industry and government due to the limited available spectrum in sub-6 GHz bands and the advantage of gigabit-per-second data rates in mmWave[6, 23–24]. The hardware constraints, channel model and array size for mmWave are quite different from those for the spectrum below 6 GHz at which the carrier frequencies of most consumer wireless systems operate[4]. First, more analog-to-digital converters with higher resolution are required for mmWave, due to the higher frequency and bandwidth channel. Partitioning the operations into analog and digital domains for signal processing is a possible solution to these hardware constraints. In addition, the propagation environment has a different effect on the channel model because of the smaller wavelength of mmWave signals. Lastly, the array size for mmWave communications could be large, benefitting from the shorter wavelength of the mmWave. This section briefly surveys most recent research work in the PLS topics on DM, AN and DPC.

3.1 Directional Modulation

The DM is a technology that transmits digitally encoded signals to a specific direction while scrambling the other directions' constellations of the same signal at the same time[25]. In this way, confidential communications can be achieved between the transmitter and the designated receiver in the desired spatial direction.

The concept of DM was first introduced to phased arrays by DALY et al.[25] In DALY et al.'s scheme[25], the controlled radio frequency (RF) level analog PSs are added to each antenna of the phased array. By changing the phase weighting through the PSs at the symbol rate, a desired constellation is produced in the intended direction, while deliberately distorting the constellations in other directions. In addition, DALY et al. also implemented the proposed technique with a four-element patch array in Ref. [26]. In the implemented scheme, the genetic algorithm is employed to get the phase shift value of each antenna in order to achieve DM for the quadratic phase shift keying (QPSK) signal. However, DALY et al.'s scheme does not take the characteristics of different channels into account. The calculation of phase values with a genetic algorithm is time-consuming for a large-scale array. Many of the subsequent DM-based PLS schemes[27–31] are investigated for sub-6 GHz channels.

However, DALY et al.'s scheme[25] may be not suitable for the mmWave band system, which has the following characteristics. First, the small carrier wavelength of mmWave makes the implementation of large antenna arrays possible. The high pathloss of the mmWave band signal could be compensated with the high beamforming gain from the large array size[32]. On the other hand, the larger array size increases the complexity of the design for PLS schemes. Second, the larger array size highlights the importance of system structure simplification due to the hardware cost constraint[4]. Specifically, the RF chain cost is the dominant factor in the mmWave system with a large array size[33]. Minimizing the number of RF chains can reduce the hardware cost and power consumption, which are key factors to support massive machine-type communication between resource constraints devices, especially IoT devices. Third, the scattering and multi-paths in the mmWave band are sparse. The propagation channel in the mmWave band, which is highly directional, has large path loss and very few multi-paths[34]. The majority of multipath components is determined by the line-of-sight (LOS) components[35]. Thus, spatial sparsity commonly existing in mmWave channels poses new challenges and opportunities in designing efficient PLS schemes.

By taking advantage of the larger array size of the mmWave system, VALLIAPPAN et al. proposed a low-complexity DM scheme named Antenna Subset Modulation (ASM) [36]. In

VALLIAPPAN's scheme, the array radiation pattern is modulated at the symbol rate to achieve DM. Only a subset of all the array antennas is used for transmission. The antenna subset used for transmission will change with the symbol rate. The subset for each symbol interval is selected from all subsets with the same number of the active antennas at random. As a result, randomness will be added to the constellations in all directions except the intended one.

VALLIAPPAN et al.'s ASM considers and takes the advantages of the large array size characteristic of mmWave system. The design of the constellation in ASM is much simpler. It only requires phase shifts or switching combinations to produce an expected modulation symbol for the user in the target direction. It is quite different from other previous DM techniques such as those in Refs. [26, 37 – 38], which typically run optimization algorithms to obtain the correct set of weights. Because only the inter-antenna phase shift needs to be changed, it opens a new era for the DM application in PLS for the mmWave channel. However, ASM restricts the modulation type to phase modulation only. In addition, many of the antennas remain idle, especially when the RF chain size is much smaller than that of the antenna number. Furthermore, the switching speed must be the same as the data rates, which increases the hardware cost.

Based on VALLIAPPAN et al.'s scheme[38], ALOTAIBI et al. proposed a similar scheme named Switched Phase Array (SPA)[39]. SPA modifies the ASM. In SPA, only one antenna is changed to be off to generate the constellation distortion in undesired directions. Thus, the system complexity is reduced while increasing the active antenna numbers used for transmission with higher gain in the main lobe. In addition, SPA can support both phase modulation and amplitude modulation and cause both phase and amplitude distortion in the undesired direction.

VALLIAPPAN et al.'s ASM[38] and ALOTAIBI et al.'s SPA[39] use the on-off switches to change the beamforming weight vector, which results in the scrambled constellation in the undesired direction. In their schemes, the beamforming weights are all binary. Neither ASM nor SPA takes full advantage of the full value range of beamforming weights to increase the difficulty for eavesdroppers to get the information. In addition, idle antennas exist in both ASM and SPA. The idle antennas neither contribute to the data transmission in the target direction nor generate the interference in the undesired direction. Motivated by the mentioned point, HONG et al. proposed a novel programmable weight phased array (PWPA) scheme[40]. PWPA has a conventional phased-array architecture with a programmable power amplifier used to change the antenna weight element amplitude. Based on the idea of PWPA, HONG et al.[40] proposed an antenna subset transmission scheme with inverted antennas named Inverted Antenna Subset Transmission (IAST) first. In IAST, several antennas are selected to transmit with inverted signals, which is different from the on-off mechanism in ASM and SPA. IAST not only scrambles the constellation but also generates more AN than conventional schemes in the undesired directions.

In recent years, some new DM-based schemes were proposed to address challenges in new scenarios such as Cybertwin and reconfigurable intelligent surface (RIS). HE et al.[41] proposed a low-complexity phased-array PLS scheme for the mmWave communication in Cybertwin-driven V2X scenarios. Similar to the typical DM-based approach, a lightweight swap-based transmitting weight vector is utilized to periodically update the transmitting weight. An efficient algorithm based on the bisection method is also introduced to quickly obtain the initial weight vector at a low computational cost. YE et al.[42] considers that the additionally introduced beam to align to the RIS may cause high sidelobe, which has a significantly negative impact on the discrete optimization in antenna subset selection. To address such a challenge introduced by the RIS, a low sidelobe beamforming approach to enable DM-based PLS in RIS communication networks is proposed, by using a novel cross-entropy iterative method.

3.2 Artificial Noise

For PLS, the security capacity, one of the important performance metrics, is a function of the received signal SNR of legitimate receivers and eavesdroppers in the wireless Gaussian channel. For wireless channels, the received signal power will decrease with the increase of the distance between the transmitter and receiver. For this reason, it is possible that the eavesdropper may be placed in an undesired direction with a much closer distance to the transmitter. Even though the eavesdropper is in the lower order sidelobe of the transmitter beam, the received signal power of the eavesdropper may be still high enough to get an acceptable SNR due to the much smaller power fade of a shorter distance. As a result, the security capacity will be seriously deteriorated in this scenario.

To address this problem, a properly designed AN is added to the transmitted signal in order to degrade the SNR of the received signal by the eavesdropper. The concept of AN was first introduced by GOEL et al.[43] The application of AN in the PLS has been studied in a number of works since then. ASHISH et al. showed that the AN transmission can be secrecy capacity-achieving at high SNR for the multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel, if the eavesdropper's channel knowledge is known by the transmitter[44]. This conclusion indicates that the AN is an effective technique for the PLS under certain conditions. ASHISH et al.'s work lays a solid theoretical foundation for AN-based physical layer security schemes. An optimal power allocation scheme that balanced the message and the AN transmission[45] was then studied for fading MIMO channels by ZHOU et al. Since then, a considerable number of studies have been conducted for AN-based PLS schemes.

However, most of the proposed schemes[43 – 49] focus on the

sub-6 GHz channel. They neither take the hardware and cost constraints of the mmWave system into account, nor make use of the characteristics of the mmWave to additionally enhance the security. ZHAO et al. proposed a scheme named Phase-Only Zero Forcing (PZF) for secret communications[50], by using the AN technique for the mmWave channel. In the proposed scheme, ZHAO et al. fully considered the hardware cost constraints of the massive antenna system for mmWave. Specifically, each RF chain in the array is associated with an analog beamforming vector. All elements' magnitudes must be constants, but they can have arbitrary phases. This constraint comes for two reasons. First, the full digital array with a digital beamforming vector requires each RF chain to be equipped with both the digital-to-analog converter (DAC) and analog-to-digital converter (ADC). Due to the large array size of mmWave systems, which could be tens or even hundreds, the hardware cost of a full digital array system will be extremely high[51 - 52]. Second, the constant magnitude weight has a lower peak-to-average power ratio (PAPR), which means the signal can be amplified with more affordable non-linear power amplifier (PA) with higher efficiency. Compared to expensive linear power PA, the non-linear power PA is more scalable for the mmWave system with a large array size[4, 53].

ZHAO et al.'s main idea is to find a beamforming vector for AN transmitting in the null space of the legitimate receiver's channel. Inspired by ZHAO et al.'s idea, XU et al. proposed a secure massive MIMO communication scheme[54] by taking advantage of the null-space of the user channel, which is constructed by the DACs with lower resolution. By projecting the AN into the null space of the legitimate receiver's channel with proper power allocation between low-resolution or high-resolution DACs, the PLS can be achieved. Specifically, XU et al. derived a closed-form SNR threshold to improve the secrecy rate. The threshold determines the choice between the DACs with low resolution or high resolution. A DAC quantization model is developed to support the analysis of the asymptotic achievable secrecy rate. In addition, XU et al. investigated secure communications over sparse mm-Wave massive MIMO channels. With consideration of the spatial sparsity of a legitimate user's channel, XU et al. proposed a secure communication scheme in Ref. [55]. Through a limited number of RF chains, the information data are precoded onto dominant angle components of the sparse channel. The AN is broadcast to the nondominant angles. Thus, only the eavesdroppers will be interfered with a high probability. With two defined statistical measures of the channel sparsity, XU et al. analytically characterized its impact on the secrecy rate. Analysis shows that a significant improvement in the secrecy rate is achieved, due to the uncertainty introduced by the unknown channel sparsity for the eavesdropper.

ELTAYEB et al. investigated the mmWave PLS in vehicular communication systems and proposed two AN-based schemes[56] for vehicular mmWave communication systems. By utilizing multiple antennas with a single RF chain, the first scheme implements the transmission of symbols to a target direction, while AN is sent in non-receiver directions. The second design uses multiple antennas with a few RF chains to transmit information symbols to a target user, while opportunistically injecting artificial noise in controlled directions. The purpose is to reduce interference in vehicular environments.

JU et al. comprehensively studied the secure transmissions in the mmWave decode-and-forward (DF) relay system[57]. They investigated the optimal parameter design for the DF relay system under the same codeword transmission (SCT) scheme and the different codeword transmission (DCT) schemes. JU et al. derived the closed-form expressions for the secrecy outage probability and connection probability. Then a solution to the secrecy throughput maximization problem was given. Based on this work, JU et al. performed extensive experiments to investigate practical secure transmission problems for mmWave communication systems[58]. They analyzed the vulnerability of existing defenses in practice and found that the existing defenses in Refs. [36] and [56] had vulnerabilities, because they might have impractical hardware requirements or still be vulnerable against multiple colluding eavesdroppers. Finally, JU et al. proposed the artificial noise hopping (ANH) with minimal hardware complexity to effectively enhance the security.

LIN et al. investigated the scenario of a 5G cellular network coexisting with a satellite network in Ref. [59]. By employing a ULA at the base station (BS) and assuming the imperfect angle-of-arrival-based channel state information (CSI) of multiple eavesdroppers (Eves) is known, a constrained optimization problem is formulated. Under the constraints that are the transmit power of BS and the interference threshold of the satellite earth station, the achievable secrecy rate of the cellular user under the worst case can be maximized.

LIN et al. proposed two robust beamforming methods to solve the complex optimization problem, in the case of either coordinated or uncoordinated Eves. They also investigated the secure communication of a cognitive satellite terrestrial network with the software-defined architecture in Ref. [60]. In LIN's scheme, the interference from the terrestrial network can be regarded as a green source to enhance the physical-layer security for the satellite network. With this assumption, a constrained joint optimization problem is formulated to minimize the total transmit power. The optimization satisfies both the terrestrial users' quality-of-service requirement and the satellite users' secrecy rate requirements.

Different from many schemes focusing on protecting the downlink transmission, XU et al.[61] proposed a scheme to protect the uplink transmission for the massive MIMO system with AN-based approaches. By optimizing the power allocation between AN and data symbols, the maximum secrecy rate can be formulated.

3.3 Directional Precoding

The DPC is commonly used in the MIMO system to improve system performance by forming the beam in certain directions, which can concentrate the power in those directions. It can be also used in the PLS to protect the secrecy of the legitimate receiver, by adding additional constraints for the power leaking to the undesired directions. A lot of PLS schemes based on DPC[62 - 67] have been proposed. However, most of them are designed for the sub-6 GHz environment. There is no special consideration for the characteristics of the mmWave environment, especially the large array size and hardware constraints.

To support the PLS under both multiple legitimate receivers and multiple eavesdroppers, HUANG et al. proposed a constant envelope (CE) hybrid precoding scheme (CEP)[68]. A unified CE hybrid precoding framework is introduced for the sub-connected digital and analog hybrid mmWave system to protect communication secrecy. By solving an optimization problem, the qualities of target users' received constellations are guaranteed. It minimizes the power leaked to the possible eavesdroppers. To address the high hardware cost issue with the large array size mmWave system, HUANG et al. applied two measures in the proposed scheme. First, a digital and analog hybrid MIMO architecture with a much reduced number of RF chains is adopted to reduce the high hardware cost and energy consumption of mmWave RF chains. Second, only the CE signal with low PAPR, which can be amplified with high power efficiency but low-cost non-linear PA, is transmitted through the array.

CHEN et al. investigated a novel hybrid beamforming design[62] to jointly optimize the data precoding and the AN power fraction selection in the massive MIMO system. To solve the non-convex secrecy rate maximization problem for hybrid precoder design, CHEN et al. separated the design for analog and digital precoders. The analog precoder was used to maximize corresponding channel gain in the analog data precoder design. In the digital data precoder design, an iterative algorithm was proposed for the optimal design with the removed non-convex codebook constraint.

LI et al. systematically investigated the impact of low-resolution PS on hybrid beamforming under various scenarios[63 - 71]. Specifically, for a wideband mmWave multiple-input and multiple-output orthogonal frequency-division multiplexing (MIMO-OFDM) system, LI et al. introduced a novel hybrid beamforming architecture[63] with varying antenna subarrays and efficient low-resolution PSs. The performance loss due to the employment of practical low-resolution PSs can be mitigated with the multiple-antenna diversity, which comes from the dynamic connection for each RF chain to a non-overlapping antenna subarray with the help of a switch network and PSs. For the architecture of dynamic hybrid beamforming, they jointly designed the hybrid precoder and combiner to maximize the average spectral efficiency. However, they did not consider the impact of low-resolution PSs on PLS.

3.4 Other PLS Schemes

The principle of AN techniques is to send jamming signals to degrade the eavesdropper channel capacity in order to improve the secrecy capacity of the legitimate channel. The jamming signal may be sent from the main transmitter or other friendly users. In this way, the main transmitter can work with other friendly receivers to cooperatively degrade the eavesdropper channel capacity. This technique is called cooperative jamming (CJ), which was first introduced by DONG et al.[72]

HU et al. investigated cooperative secret communications in wireless networks with multiple passive eavesdroppers, without the knowledge of legitimate users' perfect CSI but only eavesdroppers' statistical CSI. The secrecy beamforming with AN and CJ are explored to enhance secrecy[73]. The closed-form secrecy outage probability expression is derived. HU et al. concluded the condition that a positive secrecy rate could be achievable. Finally, a secure transmission with AN and CJ design, which maximizes the secrecy outage probability with a constrained secrecy rate, is proposed.

Motivated by HU's work, SONG et al. proposed an enhanced scheme with weaker CSI assumptions[74]. In SONG et al.'s scheme, only the knowledge of the statistic CSI of illegitimate channels and the imperfect CSI of legitimate channels are known. They derived the optimal power allocation ratio between the information-bearing signal and the AN signal in order to maximize the secrecy rate. Under the statistic CSI of illegitimate channels and the imperfect CSI of legitimate channels, the optimal power allocation, which balances the information bearing signal and the AN signal, is derived to achieve the max secrecy rate.

The mmWave PLS in UAV is another hot topic with significant attention in recent years. LI et al. investigated a secure communication system[75], which considers the smart attack from another UAV besides the legitimate UAVs. LI et al. also considered the practical cases in communications. The first is that the limited number of pilot signals may exist for channel estimation. The second is that the receiver side's channel estimation may be imperfect. To address the problems brought by the imperfect channel estimation and smart attackers who choose different kinds of attacks on the basis of the continuously changing channel environments, LI et al. used the non-cooperative game theory to derive a Q-learning-based power control algorithm, which obtains an adaptive policy for the transmitter. MA et al. investigated the secure mmWave communications assisted by multiple UAV-enabled relays, together with eavesdroppers[76], under the model of randomly distributed eavesdroppers on the ground. With the models of 3D-antenna gain and stochastic geometry, the characteristics of air-to-ground channels are considered for deriving the closed form expressions of secrecy outage probability based opportunistic relay selection. It is demonstrated that the secrecy improves when the relay density increases. For mmWave MIMO-

OFDM systems with dynamic subarray (DS), SUN et al. proposed a machine learning based hybrid precoding scheme[77]. The scheme presents a shared agglomerative hierarchical clustering (shared-AHC) algorithm for DS grouping to improve spectral efficiency (SE) performance.

3.5 Comparison

The techniques for mmWave PLS can be classified into three categories based on their technical patterns: DM, AN and DPC. Their characteristics are summarized in Table 2.

▼**Table 2. Cost and power efficiency comparison of mmWave physical layer security (PLS) techniques**

Category	Hardware Cost	Computation Cost	Power Efficiency
DM	Medium	Depend	High
AN	Low	Medium	Low
DPC	High	High	High

AN: artificial noise
DM: directional modulation
DPC: directional precoding

Specifically, the DM technique depends on the weight vector codebook. It achieves PLS by randomly selecting the vector from the codebook. The computation cost to get the codebook may be either low or high depending on the scheme and codebook size. If the scheme randomly selects the antenna subset just as what the scheme ASM does, there is only a very tiny computation cost. On the other hand, if the sechem, like Polygon, constructs the codebook with an infinite size, the computation cost may be high. The other two techniques are different from the DM technique, which are usually based on optimized weight vector results under certain security constraints. The optimization calculation may be quite complex. However, once getting the results, the weight vector will normally not change at the symbol rate. Thus, high-speed switch is not required as that in DM-based schemes.

A detailed comparison of the typical mmWave PLS schemes is shown in Table 3. Different schemes with different advantages and shortcomings are suitable for different scenarios. The subset array scheme[36] utilizes the characteristic of the large array size of the mmWave system to enable PLS. However, it is only suitable for single path scenarios. The polygon scheme[39] can work under a multiple-path scenario with a different approach. It should be noticed that current DM-based mmWave PLS schemes only support single-target receiver scenarios. It significantly constrains its application in massive machine-type communication scenarios, where multiple target receivers usually exist. To support multiple Bobs, the AN approach is usually adopted, but it comes with the cost of low power efficiency, which may be not friendly to mobile devices. In addition, the AN-based scheme proposed in Ref. [50] requires the CSI on both Bob and Eve. It may be not practical to meet such the condition, since Eve may not be exposed. The DPC-based scheme in Ref. [68] can work for multiple Bobs and multiple Eves at a high cost on both hardware and computational resource.

4 Future Research Problems

In this section, we discuss three future research problems for the PLS-based mmWave environment.

4.1 Low Complexity Directional Modulation Weight Vector Codebook Construction

The DM-based PLS schemes rely on randomly selecting the weight vector from the codebook. The codebook must be constructed before the actual transmission. However, the codebook is highly related to the target receiver's relative direction to the transmitter. Once the relative direction between the transmitter and the target receiver changes, the whole codebook has to be reconstructed. For current DM-based PLS schemes[36, 39, 40, 46], although the hardware cost has been minimized by adopting various techniques such as constant envelope, on-off switch and subarray, the algorithms for codebook construction all still suffer high complexity and high time consumption. This fact makes these schemes hardly adapt to highly dynamic scenarios with frequent and quick relative direction changes, such as vehicle networks and UAV networks, which require the codebook to be reconstructed within a short time. Since mobility is an important feature of the massive machine-type communication scenario, the DM PLS scheme with low complexity codebook construction algorithm is preferred. Motivated by this demand, the research will be conducted on reducing the DM codebook construction algorithm complexity. One of the challenges is how to maintain the PLS while reducing the codebook construction computation cost. Another challenge is how to balance the hardware cost and the codebook construction algorithm complexity.

▼**Table 3. Property comparison of mmWave physical layer security (PLS) schemes**

MmWave PLS Technique	Category	Bob	Eve	Bob Antenna	Eve Antenna	CSI	Propagation
Subset array[36]	DM	Single	Multiple	Single	Single	Bob only	Single path
Polygon[39]	DM	Single	Multiple	Single	Single	Bob only	Multiple path
PZF[50]	AN	Multiple	Single	Single	Multiple	Both	Single path
CEP[68]	DPC	Multiple	Multiple	Single	Single	Both	Single path

AN: artificial noise
CEP: constant envelope (CE) hybrid precoding scheme
CSI: channel state information
DM: directional modulation
DPC: directional precoding
PLS: physical layer security
PZF: Phase-Only Zero Forcing

4.2 Impact of Phase Shifter with Finite Precision on PLS

For the DM-based mmWave PLS schemes, the PS is a critical component to change the weight vector in order to achieve PLS. However, similar to all other hardware, the PS cannot ideally operate as it is expected in the theory. The actual shift phase value may be different from the expected value due to the limited precision of the hardware. It causes a truncation error in the PS. The effect of the truncation error of the PS can hardly be ignored. A dynamic antenna subarray approach in Ref. [63] is introduced to mitigate the performance loss due to the employment of practical low-resolution PSs. However, this approach only focuses on the communication performance enhancement of the target receiver. Its motivation does not come from the view of PLS. The impact of low-resolution PSs on the PLS performance has not been fully investigated. Thus, many opening questions need to be addressed and researched for the impact of finite precision PS on the PLS. How to describe and measure the truncation error in DM-based PLS schemes? Is there any possibility to take advantage of the truncation error to construct new DM-based PLS schemes? These questions pose both opportunities and challenges to the DM-based mmWave PLS schemes.

4.3 Multiple Target Receivers Supported Direction Modulation

Most of the DM-based PLS schemes for mmWave can only support one target receiver, by placing the target receiver in the main lobe. It limits the application to massive machine-type communication scenarios such as IoT device networks, which often require multicast communications to multiple target receivers. The scheme in Ref. [31] provides a multiple target receiver supported DM approach by utilizing the retrodirective array antenna. However, the retrodirective array antenna suffers serious performance degrading under the mmWave band[78]. The hardware cost will also increase dramatically by implementing the retrodirective array antenna with a large array size. The IoT device network with a large number of devices can hardly afford such a high cost. Thus, this approach is not suitable for the massive machine-type communication under mmWave. The approaches in Refs. [79 – 81] provide multi-beam DM solutions to supporting multiple target receivers. However, they do not consider the fact that multiple target receivers may locate in the same direction with different ranges to the transmitter in practical scenarios. Thus, the multi-beam solution cannot fully adapt to the multiple target receiver scenarios. Motivated by the demand on multiple target user support in the massive machine-type communication, the research for multiple target user supported DM will be conducted. The major challenge is how to distinguish different target receivers in both the angular domain and range domain, while protecting their PLS.

5 Conclusions

In this paper, we introduce the concept of PLS together with its importance to the mmWave 5G network, and discuss the typical PLS techniques including DM, AN and DPC. By literature reviewing the PLS schemes based on each PLS technique in detail, we summary the advantages and constraints of the DM, AN and directional precoding technique for the mmWave PLS. Finally, we propose several future research problems on mmWave PLS. Specifically, the multiple target receivers supported DM and the impact of PS with finite precision on PLS have not been fully investigated for the mmWave PLS. The computation cost for DM weight vector codebook construction is still too high to make the DM-based PLS solution adapt to highly dynamic massive machine-type communication scenarios. It is expected to draw more attention and efforts to addressing these interesting open problems in PLS-based mmWave communications.

References

[1] XIAO M, MUMTAZ S, HUANG Y M, et al. Millimeter wave communications for future mobile networks [J]. IEEE journal on selected areas in communications, 2017, 35(9): 1909 – 1935. DOI: 10.1109/JSAC.2017.2719924
[2] 3GPP. NR; User Equipment (UE) radio transmission and reception; Part 2: Range 2 Standalone: 3GPP TS 38.101-2 version 16.3.1 [S]. 2020
[3] DOLCOURT J. We tested 5G speeds across the globe [EB/OL]. [2022-03-31]. https://www. cnet. com/features/we-ran-5g-speed-tests-on-verizon-at-t-ee-and-moreheres-what-we-found
[4] HEATH R W, GONZÁLEZ-PRELCIC N, RANGAN S, et al. An overview of signal processing techniques for millimeter wave MIMO systems [J]. IEEE journal of selected topics in signal processing, 2016, 10(3): 436 – 453. DOI: 10.1109/JSTSP.2016.2523924
[5] BOCCARDI F, HEATH R W, LOZANO A, et al. Five disruptive technology directions for 5G [J]. IEEE communications magazine, 2014, 52(2):74 – 80. DOI: 10.1109/MCOM.2014.6736746
[6] ROH W, SEOL J Y, PARK J, et al. Millimeter-wave beamforming as an enabling technology for 5G cellular communications: theoretical feasibility and prototype results [J]. IEEE communications magazine, 2014, 52(2): 106 – 113. DOI: 10.1109/mcom.2014.6736750
[7] YU Q, REN J, FU Y J, et al. Cybertwin: An origin of next generation network architecture [J]. IEEE wireless communications, 2019, 26(6): 111 – 117. DOI: 10.1109/MWC.001.1900184
[8] YANG N, WANG L F, GERACI G, et al. Safeguarding 5G wireless communication networks using physical layer security [J]. IEEE communications magazine, 2015, 53(4): 20 – 27. DOI: 10.1109/MCOM.2015.7081071
[9] WANG L F, ELKASHLAN M, DUONG T Q, et al. Secure communication in cellular networks: The benefits of millimeter wave mobile broadband [C]//IEEE 15th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). IEEE, 2014: 115 – 119. DOI: 10.1109/SPAWC.2014.6941328
[10] ZHU Y X, WANG L F, WONG K K, et al. Secure communications in millimeter wave ad hoc networks [J]. IEEE transactions on wireless communications, 2017, 16(5): 3205 – 3217. DOI: 10.1109/TWC.2017.2676087
[11] WANG C, WANG H M. Physical layer security in millimeter wave cellular networks [J]. IEEE transactions on wireless communications, 2016, 15(8): 5569 – 5585. DOI: 10.1109/TWC.2016.2562010

[12] MUKHERJEE A, FAKOORIAN S A A, HUANG J, et al. Principles of physical layer security in multiuser wireless networks: a survey [J]. IEEE communications surveys & tutorials, 2014, 16(3): 1550 – 1573. DOI: 10.1109/SURV.2014.012314.00178

[13] ALAM K M, SAINI M, SADDIK A E. Toward social Internet of vehicles: concept, architecture, and applications [J]. IEEE access, 2015, 3: 343 – 357. DOI: 10.1109/ACCESS.2015.2416657

[14] ZENG K. Physical layer key generation in wireless networks: challenges and opportunities [J]. IEEE communications magazine, 2015, 53(6): 33 – 39. DOI: 10.1109/MCOM.2015.7120014

[15] WU Y P, KHISTI A, XIAO C S, et al. A survey of physical layer security techniques for 5G wireless networks and challenges ahead [J]. IEEE journal on selected areas in communications, 2018, 36(4): 679 – 695. DOI: 10.1109/JSAC.2018.2825560

[16] ZHENG T X, WANG H M, YANG Q, et al. Safeguarding decentralized wireless networks using full-duplex jamming receivers [J]. IEEE transactions on wireless communications, 2017, 16(1): 278 – 292. DOI: 10.1109/TWC.2016.2622689

[17] WANG N, WANG P, ALIPOUR-FANID A, et al. Physical-layer security of 5G wireless networks for IoT: challenges and opportunities [J]. IEEE Internet of Things journal, 2019, 6(5): 8169 – 8181. DOI: 10.1109/JIOT.2019.2927379

[18] DAVIES D. A brief history of cryptography [J]. Information security technical report, 1997, 2(2): 14 – 17. DOI: 10.1016/s1363-4127(97)81323-4

[19] SHANNON C E. A mathematical theory of cryptography [J]. Mathematical theory of cryptography, 1945

[20] WYNER A D. The wire-tap channel [J]. The bell system technical journal, 1975, 54(8): 1355 – 1387. DOI: 10.1002/j.1538-7305.1975.tb02040.x

[21] LEUNG-YAN-CHEONG S, HELLMAN M. The Gaussian wire-tap channel [J]. IEEE transactions on information theory, 1978, 24(4): 451 – 456. DOI: 10.1109/TIT.1978.1055917

[22] BLOCH M, BARROS J, RODRIGUES M R D, et al. Wireless information-theoretic security [J]. IEEE transactions on information theory, 2008, 54(6): 2515 – 2534. DOI: 10.1109/TIT.2008.921908

[23] PI Z Y, KHAN F. An introduction to millimeter-wave mobile broadband systems [J]. IEEE communications magazine, 2011, 49(6): 101 – 107. 10.1109/MCOM.2011.5783993

[24] AKDENIZ M R, LIU Y P, SAMIMI M K, et al. Millimeter wave channel modeling and cellular capacity evaluation [J]. IEEE journal on selected areas in communications, 2014, 32(6): 1164 – 1179. DOI: 10.1109/jsac.2014.2328154

[25] DING Y, FUSCO V F. A vector approach for the analysis and synthesis of directional modulation transmitters [J]. IEEE transactions on antennas and propagation, 2014, 62(1): 361 – 370. DOI: 10.1109/TAP.2013.2287001

[26] DALY M P, BERNHARD J T. Directional modulation technique for phased arrays [J]. IEEE transactions on antennas and propagation, 2009, 57(9): 2633 – 2640. DOI: 10.1109/TAP.2009.2027047

[27] DALY M P, DALY E L, BERNHARD J T. Demonstration of directional modulation using a phased array [J]. IEEE transactions on antennas and propagation, 2010, 58(5): 1545 – 1550. DOI: 10.1109/TAP.2010.2044357

[28] DING Y, FUSCO V F. Constraining directional modulation transmitter radiation patterns [J]. IET microwaves, antennas & propagation, 2014, 8(15): 1408 – 1415. DOI: 10.1049/iet-map.2014.0042

[29] DING Y, FUSCO V F. MIMO-inspired synthesis of directional modulation systems [J]. IEEE antennas and wireless propagation letters, 2016, 15: 580 – 584. DOI: 10.1109/LAWP.2015.2459752

[30] DING Y, FUSCO V, CHEPALA A. Circular directional modulation transmitter array [J]. IET microwaves, antennas & propagation, 2017, 11(13): 1909 – 1917. DOI: 10.1049/iet-map.2016.1140

[31] DING Y, FUSCO V. A synthesis-free directional modulation transmitter using retrodirective array [J]. IEEE journal of selected topics in signal processing, 2017, 11(2): 428 – 441. DOI: 10.1109/JSTSP.2016.2605066

[32] CHEN X M, NG D W K, GERSTACKER W H, et al. A survey on multiple-antenna techniques for physical layer security [J]. IEEE communications surveys & tutorials, 2017, 19(2): 1027 – 1053. DOI: 10.1109/COMST.2016.2633387

[33] ZHU J, WANG N, BHARGAVA V K. Per-antenna constant envelope precoding for secure transmission in large-scale MISO systems [C]//IEEE/CIC International Conference on Communications in China (ICCC). IEEE, 2016: 1 – 6. DOI: 10.1109/ICCChina.2015.7448727

[34] LEE G, SUNG Y, KOUNTOURIS M. On the performance of random beamforming in sparse millimeter wave channels [J]. IEEE journal of selected topics in signal processing, 2016, 10(3): 560 – 575. DOI: 10.1109/JSTSP.2016.2524999

[35] XU H, KUKSHYA V, RAPPAPORT T S. Spatial and temporal characteristics of 60-GHz indoor channels [J]. IEEE journal on selected areas in communications, 2006, 20(3): 620 – 630. DOI: 10.1109/49.995521

[36] VALLIAPPAN N, LOZANO A, HEATH R W. Antenna subset modulation for secure millimeter-wave wireless communication [J]. IEEE transactions on communications, 2013, 61(8): 3231 – 3245. DOI: 10.1109/TCOMM.2013.061013.120459

[37] BABAKHANI A, RUTLEDGE D B, HAJIMIRI A. A near-field modulation technique using antenna reflector switching [C]//IEEE International Solid-State Circuits Conference—Digest of Technical Papers. IEEE, 2009: 188 – 189+605. DOI: 10.1109/ISSCC.2008.4523120

[38] MADIHIAN M, DESCLOS L, MARUHASHI K, et al. A high-speed resonance-type FET transceiver switch for millimeter-wave band wireless network [C]//26th European Microwave Conference. IEEE, 2007: 941 – 944. DOI: 10.1109/EUMA.1996.337731

[39] ALOTAIBI N N, HAMDI K A. Switched phased-array transmission architecture for secure millimeter-wave wireless communication [J]. IEEE transactions on communications, 2016, 64(3): 1303 – 1312. DOI: 10.1109/TCOMM.2016.2519403

[40] HONG Y Q, JING X J, GAO H. Programmable weight phased-array transmission for secure millimeter-wave wireless communications [J]. IEEE journal of selected topics in signal processing, 2018, 12(2): 399 – 413. DOI: 10.1109/JSTSP.2018.2822048

[41] HE M, NI J B, HE Y Y, et al. Low-complexity phased-array physical layer security in millimeter-wave communication for cybertwin-driven V2X applications [J]. IEEE transactions on vehicular technology, 2022, 71(5): 4573 – 4583. DOI: 10.1109/TVT.2021.3138702

[42] YE N, ZHUO X R, LI J G, et al. Secure directional modulation in RIS-aided networks: a low-sidelobe hybrid beamforming approach [J]. IEEE wireless communications letters, 2022, 11(8): 1753 – 1757. DOI: 10.1109/LWC.2022.3180931

[43] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise [J]. IEEE transactions on wireless communications, 2008, 7(6): 2180 – 2189. DOI: 10.1109/TWC.2008.060848

[44] KHISTI A, WORNELL G W. Secure transmission with multiple antennas I: the MISOME wiretap channel [J]. IEEE transactions on information theory, 2010, 56(7): 3088 – 3104. DOI: 10.1109/tit.2010.2048445

[45] ZHOU X Y, MCKAY M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation [J]. IEEE transactions on vehicular technology, 2010, 59(8): 3831 – 3842. DOI: 10.1109/TVT.2010.2059057

[46] ZHANG X, MCKAY M R, ZHOU X Y, et al. Artificial-noise-aided secure multi-antenna transmission with limited feedback [J]. IEEE transactions on wireless communications, 2015, 14(5): 2742 – 2754. DOI: 10.1109/TWC.2015.2391261

[47] WANG H M, WANG C, NG D W K. Artificial noise assisted secure transmission under training and feedback [J]. IEEE transactions on signal processing, 2015, 63(23): 6285 – 6298. DOI: 10.1109/TSP.2015.2465301

[48] WU Y P, SCHOBER R, NG D W K, et al. Secure massive MIMO transmission with an active eavesdropper [J]. IEEE transactions on information theory, 2016, 62(7): 3880 – 3900. DOI: 10.1109/TIT.2016.2569118

[49] DO T T, NGO H Q, DUONG T Q, et al. Massive MIMO pilot retransmission strategies for robustification against jamming [J]. IEEE wireless communications letters, 2017, 6(1): 58 – 61. DOI: 10.1109/LWC.2016.2631163

[50] ZHAO W Y, LEE S H, KHISTI A. Phase-only zero forcing for secure communication with multiple antennas [J]. IEEE journal of selected topics in signal processing, 2016, 10(8): 1334 – 1345. DOI: 10.1109/JSTSP.2016.2611483

[51] SOHRABI F, YU W. Hybrid digital and analog beamforming design for large-scale antenna arrays [J]. IEEE journal of selected topics in signal processing, 2016, 10(3): 501 – 513. DOI: 10.1109/JSTSP.2016.2520912

[52] DOAN C H, EMAMI S, SOBEL D A, et al. Design considerations for 60 GHz CMOS radios [J]. IEEE communications magazine, 2004, 42(12): 132 – 140. DOI: 10.1109/MCOM.2004.1367565

[53] RUSEK F, PERSSON D, LAU B K, et al. Scaling up MIMO: opportunities and challenges with very large arrays [J]. IEEE signal processing magazine, 2013, 30(1): 40 – 60. DOI: 10.1109/MSP.2011.2178495
[54] XU J D, XU W, ZHU J, et al. Secure massive MIMO communication with low-resolution DACs [J]. IEEE transactions on communications, 2019, 67(5): 3265 – 3278. DOI: 10.1109/TCOMM.2019.2895023
[55] XU J D, XU W, NG D W K, et al. Secure communication for spatially sparse millimeter-wave massive MIMO channels via hybrid precoding [J]. IEEE transactions on communications, 2020, 68(2): 887 – 901. DOI: 10.1109/TCOMM.2019.2954517
[56] ELTAYEB M E, CHOI J, AL-NAFFOURI T Y, et al. Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems [J]. IEEE transactions on vehicular technology, 2017, 66(9): 8139 – 8151. DOI: 10.1109/TVT.2017.2681965
[57] JU Y, WANG H Y, PEI Q Q, et al. Physical layer security in millimeter wave DF relay systems [J]. IEEE transactions on wireless communications, 2019, 18 (12): 5719 – 5733. DOI: 10.1109/TWC.2019.2938757
[58] JU Y, ZHU Y Z, WANG H M, et al. Artificial noise hopping: a practical secure transmission technique with experimental analysis for millimeter wave systems [J]. IEEE systems journal, 2020, 14(4): 5121 – 5132. DOI: 10.1109/JSYST.2020.2976852
[59] LIN Z, LIN M, WANG J B, et al. Robust secure beamforming for 5G cellular networks coexisting with satellite networks [J]. IEEE journal on selected areas in communications, 2018, 36(4): 932 – 945. DOI: 10.1109/JSAC.2018.2824760
[60] LIN M, LIN Z, ZHU W P, et al. Joint beamforming for secure communication in cognitive satellite terrestrial networks [J]. IEEE journal on selected areas in communications, 2018, 36(5): 1017 – 1029. DOI: 10.1109/JSAC.2018.2832819
[61] XU W Y, LI B, TAO L L, et al. Artificial noise assisted secure transmission for uplink of massive MIMO systems [J]. IEEE transactions on vehicular technology, 2021, 70(7): 6750 – 6762. DOI: 10.1109/TVT.2021.3081803
[62] CHEN W R, CHEN Z, NING B Y, et al. Artificial noise aided hybrid precoding design for secure mmWave MIMO system [C]//Proceedings of 2019 IEEE Global Communications Conference (GLOBECOM). ACM, 2019: 1 – 6. DOI: 10.1109/GLOBECOM38437.2019.9013417
[63] LI H Y, LI M, LIU Q, et al. Dynamic hybrid beamforming with low-resolution PSs for wideband mmWave MIMO-OFDM systems [J]. IEEE journal on selected areas in communications, 2020, 38(9): 2168 – 2181. DOI: 10.1109/JSAC.2020.3000878
[64] TIAN X W, WANG Z H, LI H Y, et al. Secure hybrid beamforming with low-resolution phase shifters in mmWave MIMO systems [C]//Proceedings of 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2020: 1 – 6. DOI: 10.1109/GLOBECOM38437.2019.9013333
[65] LI H Y, LIU R, LI M, et al. FP-based hybrid precoding with dynamic subarrays and low-resolution PSs [C]//11th International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, 2019: 1 – 6. DOI: 10.1109/WCSP.2019.8928111
[66] LI H Y, LIU Q, WANG Z H, et al. Joint antenna selection and analog precoder design with low-resolution phase shifters [J]. IEEE transactions on vehicular technology, 2019, 68(1): 967 – 971. DOI: 10.1109/TVT.2018.2879083
[67] LIU R, LI H Y, GUO Y Q, et al. Hybrid beamformer design with low-resolution phase shifters in MU-MISO SWIPT systems [C]//Proceedings of 2018 10th International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, 2018: 1 – 6. DOI: 10.1109/WCSP.2018.8555694
[68] HUANG Y M, ZHANG J J, XIAO M. Constant envelope hybrid precoding for directional millimeter-wave communications [J]. IEEE journal on selected areas in communications, 2018, 36(4): 845 – 859. DOI: 10.1109/JSAC.2018.2825820
[69] LI H Y, LI M, LIU Q. Hybrid beamforming with dynamic subarrays and low-resolution PSs for mmWave MU-MISO systems [J]. IEEE transactions on communications, 2020, 68(1): 602 – 614. DOI: 10.1109/TCOMM.2019.2950905
[70] WANG Z H, LI M, LI H Y, et al. Hybrid beamforming with one-bit quantized phase shifters in mmWave MIMO systems [C]//Proceedings of 2018 IEEE International Conference on Communications (ICC). IEEE, 2018: 1 – 6. DOI: 10.1109/ICC.2018.8422249
[71] LI H Y, LIU Q, WANG Z H, et al. Transmit antenna selection and analog beamforming with low-resolution phase shifters in mmWave MISO systems [J]. IEEE communications letters, 2018, 22(9): 1878 – 1881. DOI: 10.1109/LCOMM.2018.2852304
[72] DONG L, HAN Z, PETROPULU A P, et al. Improving wireless physical layer security via cooperating relays [J]. IEEE transactions on signal processing, 2010, 58(3): 1875 – 1888. DOI: 10.1109/TSP.2009.2038412
[73] HU L, WEN H, WU B, et al. Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers [J]. IEEE transactions on vehicular technology, 2018, 67(3): 2108 – 2117. DOI: 10.1109/TVT.2017.2744660
[74] SONG H H, WEN H, HU L, et al. Secure cooperative transmission with imperfect channel state information based on BPNN [J]. IEEE transactions on vehicular technology, 2018, 67(11): 10482 – 10491. DOI: 10.1109/TVT.2018.2849364
[75] LI C, XU Y, XIA J J, et al. Protecting secure communication under UAV smart attack with imperfect channel estimation [J]. IEEE access, 2018, 6: 76395 – 76401. DOI: 10.1109/ACCESS.2018.2880979
[76] MA R Q, YANG W W, ZHANG Y, et al. Secure mmWave communication using UAV-enabled relay and cooperative jammer [J]. IEEE access, 2019, 7: 119729 – 119741. DOI: 10.1109/ACCESS.2019.2933231
[77] SUN Y W, GAO Z, WANG H, et al. Machine learning based hybrid precoding for mmWave MIMO-OFDM with dynamic subarray [C]//IEEE Globecom Workshops (GC Wkshps). IEEE, 2019: 1 – 6. DOI: 10.1109/GLOCOMW.2018.8644321
[78] ALI A A M, EL-SHAARAWY H B, AUBERT H. Millimeter-wave substrate integrated waveguide passive van atta reflector array [J]. IEEE transactions on antennas and propagation, 2013, 61(3): 1465 – 1470. DOI: 10.1109/TAP.2012.2228622
[79] DING Y, FUSCO V. Orthogonal vector approach for synthesis of multi-beam directional modulation transmitters [J]. IEEE antennas and wireless propagation letters, 2015, 14: 1330 – 1333. DOI: 10.1109/LAWP.2015.2404818
[80] HONG T, SONG M Z, LIU Y. Dual-beam directional modulation technique for physical-layer secure communication [J]. IEEE antennas and wireless propagation letters, 2011, 10: 1417 – 1420. DOI: 10.1109/LAWP.2011.2178384
[81] SHI H Z, TENNANT A. Simultaneous, multichannel, spatially directive data transmission using direct antenna modulation [J]. IEEE transactions on antennas and propagation, 2014, 62(1): 403 – 410. DOI: 10.1109/TAP.2013.2287284

Biographies

HE Miao received his BE degree from Zhejiang University, China and MASc degree from the University of Waterloo, Canada, respectively. He is currently pursuing his PhD degree with the Department of Electrical and Computer Engineering, Queen's University, Canada. His research interests include signal processing, applied cryptography and information security, with current focus on beamforming using large antenna arrays and physical layer security in millimeter-wave wireless communications.

LI Xiangman received her BE degree from the Department of Electrical and Computer Engineering, Queen's University, Canada. She is currently pursuing the MASc degree with the Department of Electrical and Computer Engineering, Queen's University. Her research interests include machine learning security, secure data trading, and Blockchain Technology.

NI Jianbing (jianbing.ni@queensu.ca) is currently an assistant professor with the Department of Electrical and Computer Engineering and a member of the Ingenuity Labs Research Institute, Queen's University, Canada. He received his PhD degree in electrical and computer engineering from University of Waterloo, Canada in 2018. His research interests are applied cryptography, wireless and mobile network security, edge computing security, machine learning security, and blockchain technology. He received the Best Paper Awards from IEEE MASS 2018, IEEE ICC 2018, IEEE GLOBECOM 2017, EAI SECURECOMM 2016, etc., and the Best Paper Award from *IEEE Transactions on Mobile Computing*. He is serving as the associate editor of *IEEE Systems Journal* and *ACM Distributed Ledger Technologies: Research and Practice*.

Autonomous Network Technology Innovation in Digital and Intelligent Era

DUAN Xiangyang[1,2], KANG Honghui[1,2], ZHANG Jianjian[1]
(1. ZTE Corporation, Shenzhen 518057, China;
2. State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen 518055, China)

DOI: 10.12142/ZTECOM.202204007
https://kns.cnki.net/kcms/detail/34.1294.TN.20221207.1234.001.html, published online December 7, 2022
Manuscript received: 2022-07-22

Abstract: The issues of wireless communication network autonomy, the definition of capability level and the concept of AI-native solution based on the integration of the information communication data technology (ICDT) are first introduced in this paper. A series of innovative technologies proposed by ZTE Corporation, such as an autonomous evolution network and intelligent orchestration network, are then analyzed. These technologies are developed to realize the evolution of wireless networks to Level-4 and Level-5 intelligent networks. It is expected that the future AI-native intelligent network system will be built based on innovative technologies such as digital twins, intent-based networking, and the data plane and intelligent plane. These new technical paradigms will promote the development of intelligent B5G and 6G networks.

Keywords: autonomous network; digtal twin; AI-native

Citation (IEEE Format): X. Y. Duan, H. H. Kang, and J. J. Zhang, "Autonomous network technology innovation in digital and intelligent era," *ZTE Communications*, vol. 20, no. 4, pp. 52 – 61, Dec. 2022. doi: 10.12142/ZTECOM.202204007.

Wireless communication networks are moving from the era of interconnection and cloud to the era of intelligence. The Telecom Management Forum (TMF) has proposed the concept of autonomous networks (AN), which aims to use automation and intelligence technologies to help operators simplify business deployment and enable network capabilities of self-configuration, self-optimization, self-healing and self-evolution. At present, with the emergence of intelligent application scenarios, AN is developing rapidly. The integration of the open network automation platform (ONAP), RAN intelligent controller (RIC) and AN is becoming a hierarchical closed loop and new technologies such as intent-based networks and digital twin networks (DTN) are also being introduced.

1 Concept and Progress of Autonomous Network

1.1 Definition of Autonomous Network

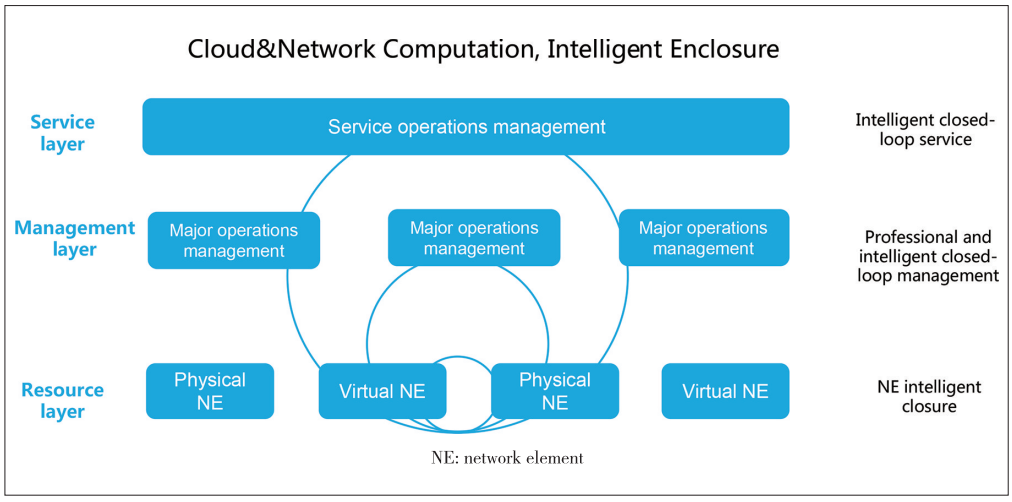
As an industry-recognized systematic method to promote network automation and intelligence, AN can not only help operators "realize network intelligence, enable intelligent services, and promote business intelligence", but also become the intersection of "network technology and digital technology"[1]. AN is expected to be a new driving force for a new round of technological innovation and industrial transformation, to be a new strategic fulcrum for leveraging the upgrading and evolution of the communication industry, to drive network services to open a new era of digitalization, intelligence and greening, and to enable the digitalization transformation of thousands of industries[2]. Fig. 1 shows a typical closed-loop architecture of AN[3].

AN aims to provide vertical industries and consumers with the ultimate experience of Zero-X (zero-wait, zero-contact and zero-fault) through fully automated networks and ICT infrastructure, agile operation, and full-scenario services. By using AI technologies, the AN leaves the complexity to the supplier and minimizes the complexity for the customer. AN helps the operators build and maintain the operation and maintenance (O&M) of Self-X (self-service, self-distribution and self-guarantee), and also enables the departments of network planning and construction, marketing service, and operation and maintenance to achieve the automation and intelligence of production, operation and management.

1.2 Application Scenarios of Autonomous Network

The AN application scenarios in a mobile communication system are divided into two types: intelligent network O&M and intelligent network elements (NE).

In the scenario of intelligent network O&M, AN can implement intelligent improvement of overall network O&M, improving the efficiency of the network and O&M. For example, intelligent energy saving is used to guarantee base station operation and dynamic energy saving. Intelligent MIMO is used to implement accurate scenario identification and ultra-fast op-



▲Figure 1. Closed-loop architecture of autonomous network

timization of antenna weights. Intelligent troubleshooting is used to implement accurate fault location and alarm work order reduction. Intelligent optical access is used to implement weak optical root cause analysis and poor video quality analysis. Intelligent edge technology is used to achieve intelligent coordination at the cloud edge and facilitate vertical industrial applications. Virtualized infrastructure intelligent O&M implements cross-layer management and location of virtualized system O&M problems and makes accurate predictions of cloud system faults. Intelligent slicing implements dynamic scheduling of slice resources and accurate guarantee of end-to-end (E2E) Service-Level Agreement (SLA). Intelligent operation can realize the management and analysis of all data in the whole domain and support the integrated operation of E2E's user perception guarantee and network life cycle.

AN uses AI capabilities to orchestrate network resources intelligently, in order to enable Intelligent NEs. Intelligent orchestration networks with adaptive scenario intentions are built based on user experience, following the capability vision of demand-based orchestration and the basic framework of endogenous intelligence. Through deep coordination between macro-level network orchestration and micro-level user orchestration, intent-driven joint optimization is achieved, which realizes NE-level intelligence.

1.3 Definition of Intelligent AN Model

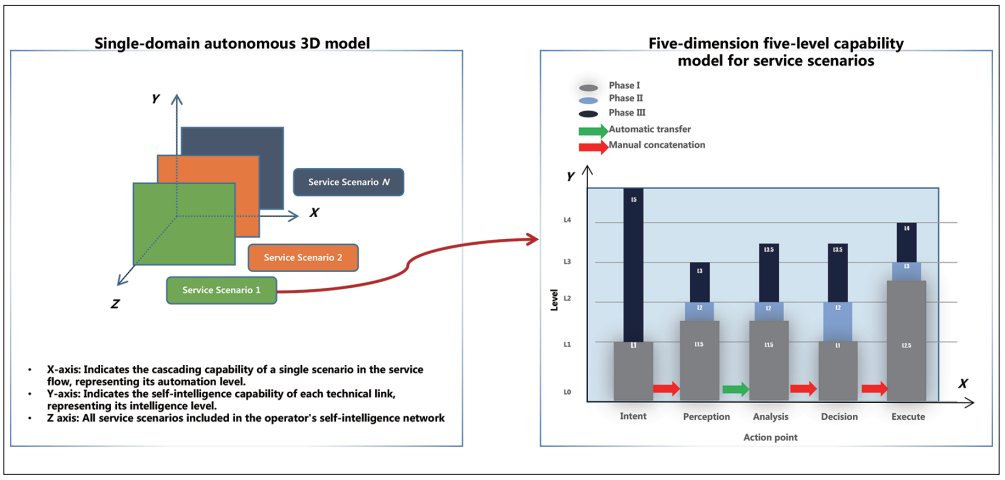
Based on the classification definition of autopilot networks in the industry[3], TMF has constructed a five-level capability classification system for communication network autonomy, and macroscopically defined the classification standard of autopilot networks with L0 – L5 levels. L0 refers to manual intervention with no automation ability, while L5 supports complete intelligence of the network with the ability of self-learning and self-evolution. Besides, L2 enables closed-loop O&M automation of a specific NE in a given external environment based on an AI model. L3 further perceives changes in the real-time environment and implements intention-based closed-loop automatic management in a specific network domain. Based on prediction, L4 realizes closed-loop automatic management driven by customer experience and business quality in a complex cross-domain environment.

In traditional system construction, we usually focus on the real problems that can be solved by a tool or a system, the available systems in different scenarios of network planning, maintenance and operation, and whether this discrete tool can evolve from manual to automatic and intelligent. However, neither a stable workflow nor the organic integration of scenarios, intelligent levels and other factors are considered. As a result, each system has its own way and plays its own role, which finally leads to the chimney effect that is amplified year by year. With the emphasis on single-domain self-governance and intelligent system construction, the existing capability level definition is no longer fully suitable for the continuous development of future industries and competitiveness. Therefore, we comprehensively consider the collaboration between humans and AI from the aspects of intention, perception, analysis, decision-making and execution, and refine the evaluation model of network intelligence capability in scenarios. Fig. 2 shows a reference model architecture defined according to the five-dimension and five-level capability model of business scenarios.

1.4 Standardization Progress of Autonomous Network

With the development of standards and industries, the concept of AN has reached a consensus in academia and industry. The leading operators and suppliers work around the four elements of "target architecture, grading standards, evaluation system and operation practice" to push the AN industry from the incubation period to the promotion period. Industrial and standardization organizations, such as Next Generation Mobile Networks Alliance (NGMN), TMF, ITU, 3GPP, ETSI and China Communications Standards Association (CCSA), have initiated related standardization and research programs and established a cross-organization AN collaboration platform M-SDO to accelerate the implementation of industry standards.

The three key study fields of NGMN in AN are E2E decoupling, green future networks and 6G. The TMF autonomous network project team (ANP) is divided into two lines: business architecture (BA) and technical architecture (TA). TMF has released several standards on multiple hot technologies such as the autonomous network architecture, hierarchy,



▲Figure 2. Reference capability model architecture of autonomous network

intention, closed loop and M-SDO. ITU SG13 focuses on future networks (including IMT-2020), cloud computing and trusted network infrastructure. ITU Focus Group on Autonomous Networks (FG-AN) was established in December 2020 to focus on the pre-research of autonomous network standards. It has released Y.317X series specifications of the requirements, architecture and levels related to the intelligence of autonomous networks. Moreover, the standardization of specific intentions, perceptions and sandboxes is under research. The 3GPP has defined the standards and specifications related to AN from R16. Its working group SA5 undertakes the most projects related to AN, including the standards and specifications of the autonomous network level (ANL), closed-loop control, intent-driven management service (IDMS) and enterprise management data analysis (eMDA). CCSA Network Management and Operation Support Committee (TC7) takes operation management intelligence as the core evolution content. Many meaningful specifications have been released, such as the definition of several functions including 3GPP Network Data Analytics Function (NWDAF) and Management Data Analytics Function (MDAF).

2 Technology Innovation of Autonomous Network

2.1 ZTE uSmartNet

ZTE Corporation has proposed a self-evolving network uSmartnet[4], which adopts the universal AI technology and can be deeply embedded in all levels of the communication network to realize a unified autonomous system. This solution promotes the continuous improvement of network intelligence capabilities by comprehensively introducing AI-enabling technologies into the network infrastructure layer, O&M layer and business operation layer, realizing the network voluntary, simple O&M, and random service.

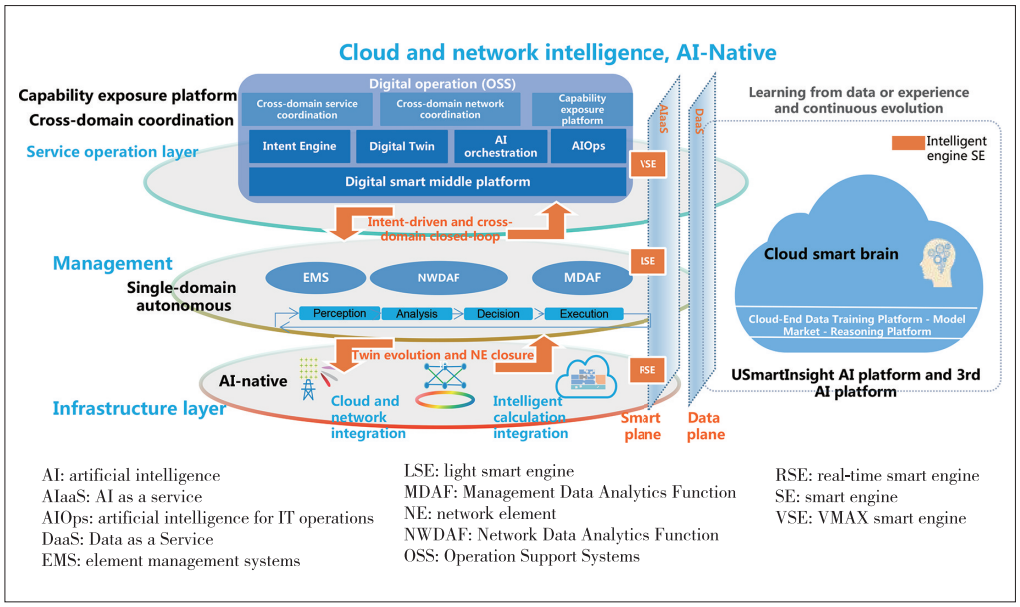
At the network infrastructure layer, AI engines are embedded in NEs to support AI-endogenous infrastructure. At the O&M management layer, single-domain autonomy is achieved through the introduction of an intelligent closed-loop mechanism of perception, analysis, decision making and execution. At the business operation layer, the openness of O&M capabilities and the cross-domain business and network collaboration are realized based on the construction and interconnection of the data middle platform and intelligence middle platform, with the introduction of technical capabilities such as intention engine, digital twins, intelligent orchestration and capability opening.

In terms of technical architecture evolution, Data as a Service (DaaS) and AI as a Service (AIaaS) will be implemented in future networks based on the logic functions of the AI-native data plane and intelligent plane. The cloud smart brain, composed of a cloud-based data lake, AI training platform, model market, and inference platform, provides AI model training and inference capabilities. Fig. 3 shows the technical architecture of the autonomous network uSmartNet.

2.2 Network Cross-Domain Collaboration Technology

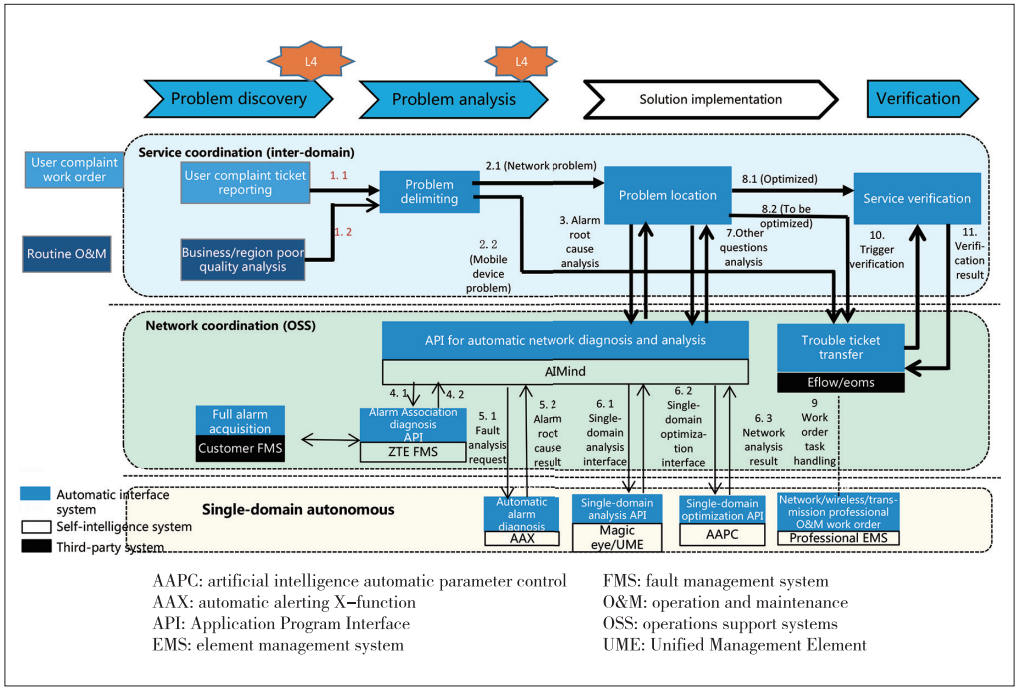
The cross-domain system is located in the upper layer of an O&M management network. The cross-domain collaboration includes cross-domain business collaboration and cross-domain network collaboration. The former mainly focuses on the service indicators oriented to improving user perception and on the guarantee and improvement of end-to-end service experience. The latter is the coordination of the upper-layer operators' quality centers and fault centers at the O&M layer and the underlying single-domain autonomous system, such as the radio access network (RAN), core network (CN) and transmission bearer system. It ensures the closed-loop processing of workflows, O&M and troubleshooting, as well as user experience in closed-loop O&M. Based on capability collaboration, it provides capability openness to operators and third-party customers through a unified capability opening platform and interface and facilitates low-code development services and network capability services.

We take the cross-domain deployment of an automatic quality optimization system based on business awareness as a use case to show cross-domain collaboration (Fig. 4), where the following two typical application scenarios are considered: 1) Troubleshooting of Voice over LTE (VoLTE), evolved packet system (EPS) fallback and Voice over 5G New Radio (VoNR) services, and cross-domain analysis and result verification from E2E terminals to wireless networks, to bearer networks,



AI: artificial intelligence
AIaaS: AI as a service
AIOps: artificial intelligence for IT operations
DaaS: Data as a Service
EMS: element management systems
LSE: light smart engine
MDAF: Management Data Analytics Function
NE: network element
NWDAF: Network Data Analytics Function
OSS: Operation Support Systems
RSE: real-time smart engine
SE: smart engine
VSE: VMAX smart engine

▲ **Figure 3. Technical architecture of ZTE uSmartNet**



AAPC: artificial intelligence automatic parameter control
AAX: automatic alerting X-function
API: Application Program Interface
EMS: element management system
FMS: fault management system
O&M: operation and maintenance
OSS: operations support systems
UME: Unified Management Element

▲ **Figure 4. Cross-domain collaborative deployment framework**

and to core networks; 2) Problem identification of web, video games and cloud virtual reality/augmented reality (VR/AR) services, and E2E network cross-domain analysis and result verification.

Building a complete O&M closed loop through service coordination and O&M systems can implement a loop from problem discovery, problem analysis and fault delimitation to subsequent closed-loop control and verification, as well as a loop from the operations support system (OSS) to the bottom single domain system. This cross-domain collaborative system can greatly improve the efficiency of E2E network O&M and effectiveness of work order flow.

For such cross-domain systems, AN has some new requirements for capability characteristics as follows:

- Enabling interconnection with the complaint work order system and improving complaint scenarios;
- Interfacing with the FMS system and improving the alarm diagnosis ability;
- Enabling interconnection with the network collaboration system to improve the capability of diagnosing and analyzing NEs, users and service problems in the system;
- Connecting professional platform capabilities of such single domains as the core, wireless and transmission to form complete analysis capabilities;
- Enabling interconnection with the work order transfer system of the customer;
- Enabling interconnection with the capability exposure system to implement automatic orchestration of processes.

2.3 Network Intelligent Orchestration Technology

With the gradual scale-up of 5G commercial networks and the fundamental proposition of improving the value and economic benefits of the 5G network, the contradiction between the increasing diversification of 2B+2C (to Business and to Consumer) services and the relatively fixed network resource strategy has become increasingly prominent. Within the limited network resources, we need to provide better services for users and business with more differentiated needs. The transformation from the network-centric resource allocation strategy to a user-centric precise resource service mode is necessary to achieve the best balance between user experience and network efficiency.

Wireless intelligent orchestration is a solution that is based on the computing engine of the IT BBU endogenous intelli-

gence. It conducts multi-dimensional perception and learning of many factors in the network (such as terminal capability and service requirement). In a multi-layer network, user orchestration and network orchestration are the two wheels driving the flexible orchestration of network service capabilities to be realized. The flexible orchestration based on network service capabilities enables the precise empowerment of the network and brings the optimal resolution of user experience and network efficiency.

An intelligent orchestration solution[5] includes user orchestration and network orchestration. The former is to orchestrate the service combination capability of multiple frequency points in the network, with given network service capabilities (fixed spectrum configuration). When the user experience of a service is lower than its experience baseline, an optimal solution will be provided based on the service requirement and terminal capability, which will guide the user to another cell with better service experience. The latter is based on a given traffic distribution situation. If the current network configuration cannot meet user experience requirements, flexible orchestration of network service capabilities will be carried out based on spectrum, carrier, frame structure and beam. In this way, together with traffic trend prediction, self-adaptive network service capability sets based on the current traffic trend can be achieved, thus improving user experience.

Fig. 5 shows the evolution of the intelligent wireless orchestration capability. An intelligent orchestration network is intention-driven instead of experience-driven, aims at meeting differentiated value demands of different development stages and in different scenarios, and achieves accurate matching with the intention customization and orchestration capabilities of network service operation objectives. It changes single-domain orchestration driven by wireless domain experience to cross-domain orchestration based on knowledge plane empowerment, driving the evolution of diversified intelligent service capabilities from user experience to network values. It can also achieve the optimal joint orchestration driven by the intention through the deep coordination between the network orchestration at the macro level and the user orchestration at the micro level. In addition, the integrated orchestration architecture of 2B and 2C and the evolution of the multi-target intelligent resource management capability facilitate the best unity of service differentiation and capability consistency.

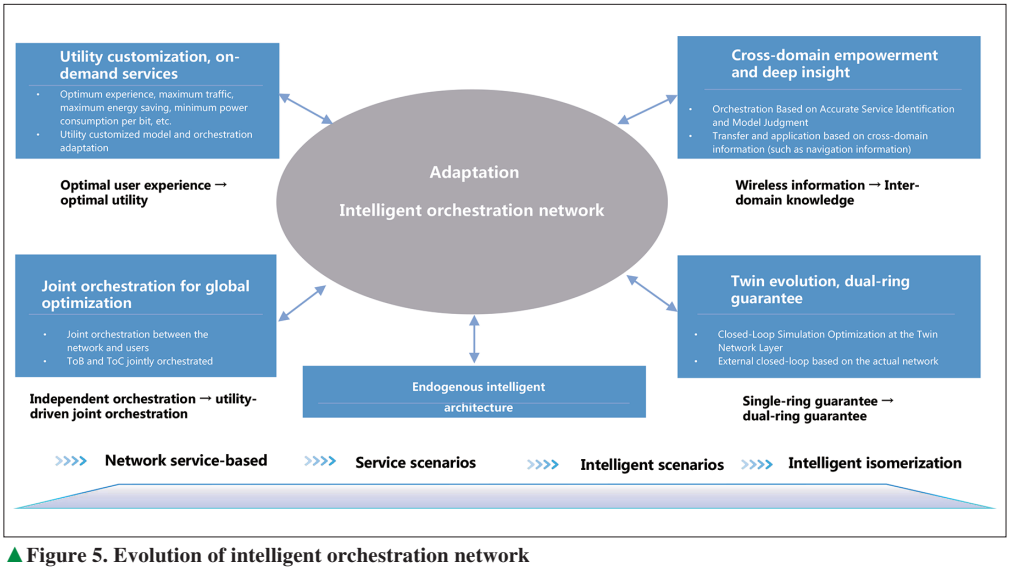
The single-layer closed loop is replaced by a dual-layer closed loop in an intelligent orchestration network. This relies on the high-precision digital modeling and simulation capabilities provided by the digital twin technology to implement efficient search, effect prediction and closed-loop optimization of the virtual network for optimal orchestration solutions in the virtual world. The optimal accurate orchestration capability is also available based on the optimal solutions provided by the digital twin technology and the closed-loop optimization of the physical network.

2.4 AIOps Technology and Algorithm

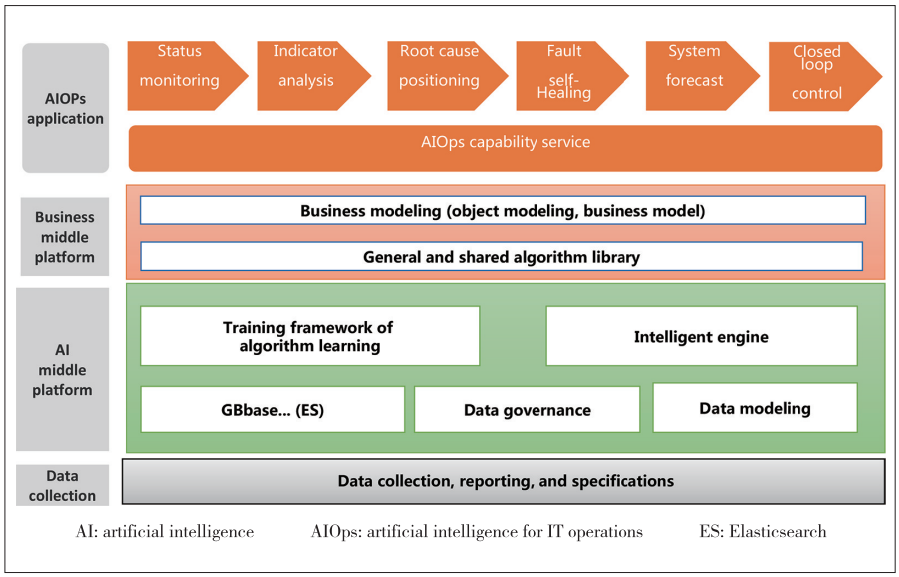
Artificial intelligence for IT operations (AIOps)[6] adopts some generalized AI technologies (rules, knowledge base, machine learning, deep learning, etc.) to implement intelligent operation and maintenance of the network. The application functions of AIOps mainly include status monitoring, index analysis, root cause location, fault self-healing and system prediction of network business operation and maintenance. These will transform the network operation and maintenance from passive to predictable.

The emergence of AIOps transforms the traditional human-machine O&M mode into a human-machine coordination O&M mode. Human-machine coordination uses artificial intelligence technologies such as machine learning (ML) and deep learning (DL) to transfer the algorithms used for network O&M scenarios to O&M tools and facilitates the operation and maintenance through actions such as perception, analysis, decision-making and execution. The AIOps mode gives network O&M management the algorithm and ML ability, makes operation and maintenance intelligent, sublimates data into knowledge, and further promotes the learning ability of machines to form a closed-loop operation and maintenance mode with self-decision-making and self-execution of machines.

AIOps has abundant and diversified use cases and algo-



▲ **Figure 5. Evolution of intelligent orchestration network**



▲Figure 6. AIOps service platform framework

rithms. How to maximize sharing and algorithm optimization is the focus of AIOps. AIOps uses the middle platform to share and reuse components and functions and uses the algorithm library to optimize and generalize algorithms. A unified AIOps platform is composed of the service middle platform, data middle platform and AI middle platform. The service middle platform is responsible for the service capability and capability opening components of the service. The data middle platform is responsible for unified data collection, governance and service provision. The AI middle platform provides the model training and reasoning capabilities of intelligent applications. Fig. 6 shows the service platform framework of the wireless AIOps.

The AIOps-oriented algorithms and application scenarios are as follows:

1) Multi-index association mining: Multi-index association analysis determines whether multiple indexes fluctuate or increase frequently. This algorithm can be used to build fault propagation relationships for fault diagnosis. Common algorithms are Pearson correlation, Spearman correlation and Kendall correlation.

2) Indicator clustering: Multiple key performance indicators (KPIs) are clustered into multiple categories in accordance with the curve similarity. This algorithm can be used for large-scale indicator exception detection. It uses the same exception detection algorithm and parameters in the same indicator type, greatly reducing the training and detection costs. Common algorithms include Density-Based Spatial Clustering of Applications with Noise (DBSCAN), K-medoids and Clustering Algorithm Based on Random Selection (CLARANS).

3) Index and event association mining: The association between events and indicators in text data is automatically mined to establish fault propagation relationships and diagnose faults. Common algorithms are Pearson correlation, J-measure and the two-sample test.

4) KPI trend prediction: By analyzing historical KPI data, KPI trends and predicted values can be determined in the future and then used for abnormal detection, capacity prediction and capacity planning. Common algorithms include the Holt-Winters, time sequence data decomposition and Autoregressive Integrated Moving Average (ARIMA) model.

5) Event and event association mining: Analysis of the association relationship of abnormal events associates the events that occur frequently together in history. This algorithm can be used to build fault propagation relationships for fault diagnosis. Common algorithms include FP-Growth, Apriori and the random forest.

6) Fault propagation relation mining: It combines text data and index data. Based on the above-mentioned algorithms (such as the multi-index association mining, index-event association mining and event-event association mining), the module invocation relation diagram derived from tracing, the auxiliary server-network topology, and the fault propagation relation between components are established. This algorithm is applicable to fault diagnosis.

3 Development Trends of Autonomous Network Technologies

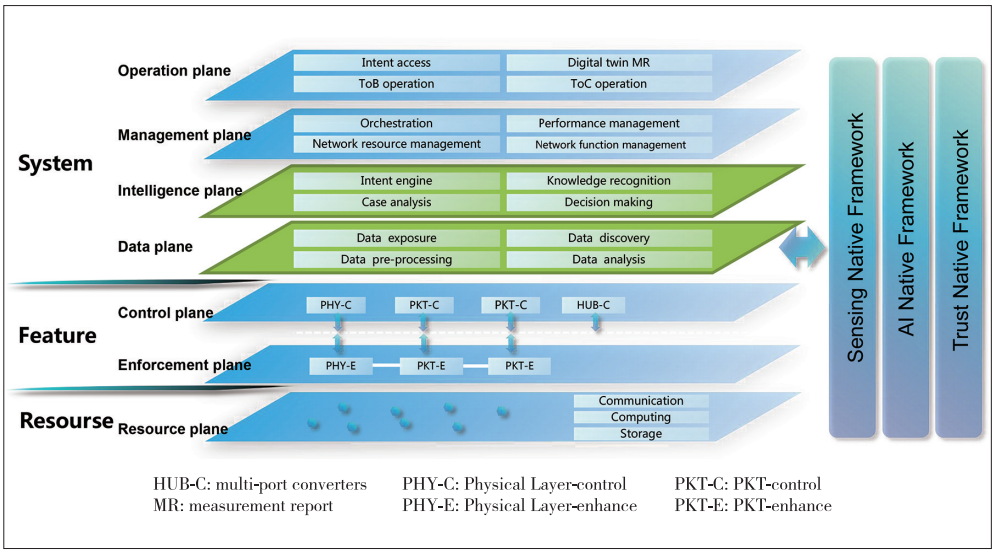
In the future, AN may evolve toward a "multi-service intelligent connection and digital-twin enabled" 6G system[7] and also to the L5-level intelligent capability. The evolution may encounter the problems of current network intelligent plugins and lack of standardization, more application generalization problems of ICDT technologies, and the problems caused by the limitations of the AI technology itself. These problems will be solved with the AI-native technology architecture and more emerging technologies, such as graph neural networks, digital twin networks and self-learning technology, which will direct the technological development trend of autonomous networks.

3.1 AI-Native Architecture

The technological development of AN is presenting a trend of scene intelligence and AI-native system.

Scene intelligence can achieve efficient and precise scenario-based services and continuous evolution through effective, scenario-sensible, policy-flexible and controllable closed-loop intelligence.

AI-native integrated network architecture (Fig. 7) is based on the deep integration of AI computing capabilities and the communication process. It can comprehensively improve the intelligent learning and scenario adaptation capabilities of different levels and support the continuous evolution of personal-



▲Figure 7. Architecture of AI-native network system

ized intelligent service ability. The intelligent plane and data plane are integrated into the network architecture design and implementation of NEs and interfaces, so that future intelligent networks will be self-adaptive, self-learning self-correcting and self-optimizing. The main features of an AI-native system are as follows:

1) It can provide complete AI capabilities in the communication network defined by 3GPP standards, including data, computing power and algorithm capabilities.

2) In terms of communication network architecture, it fully considers the application requirements of the future intelligent plane at the functional and logical levels.

3) In the future, the protocol stack design and interface design have to be changed to adapt to the deployment of AI applications.

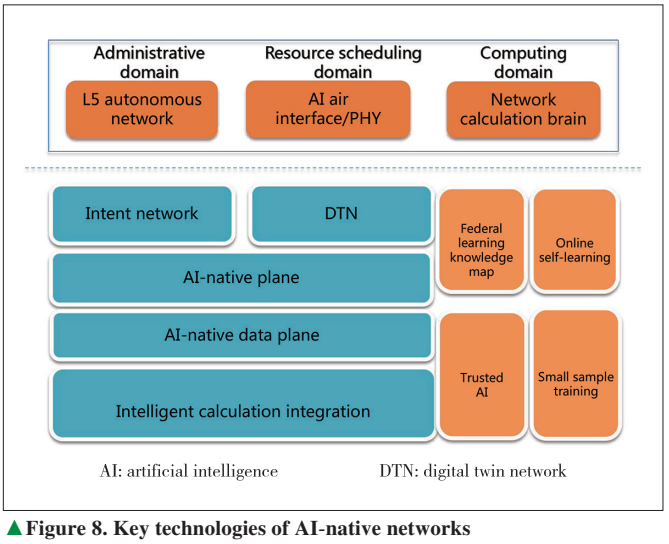
Considering the integration of the AI-native system architecture and the development of AI itself (such as automatic machine learning, trusted AI and model pre-training), the key technology map of AI-native networks in the future B5G system is shown in Fig. 8.

3.2 Intent-Based Network

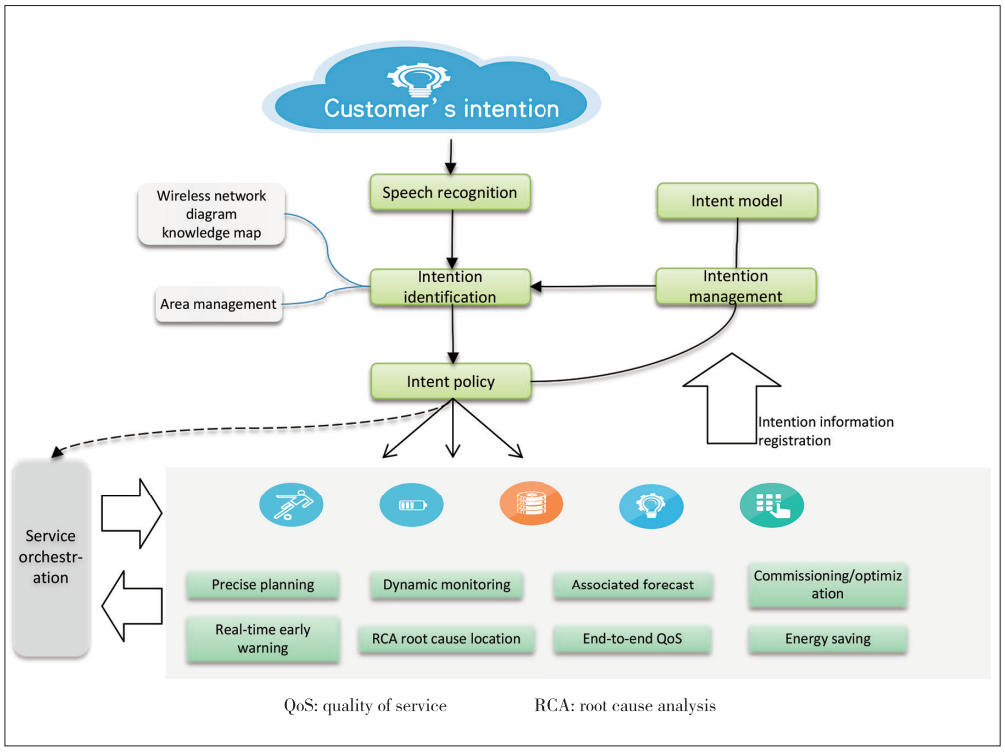
It can be seen from the autonomous classification standards that the L4/L5 high-level autonomy has the following two features: policy self-generation and intention-driven. The former requires that the system automatically generates/updates policies to achieve the operation or maintenance intention without manual intervention or guidance. The latter requires that the system automatically verify and optimize these self-generated policies to avoid system risks. That is to say, the latter requires the system has the capability of processing intention.

An intent-based network[8-10] takes the intention and strategy entered by the operator as guidance. Combined with the self-perception and prediction of environment, network resources and status, it can intelligently translate the demand for the network into network parameter configuration, network function configuration and network architecture configuration, and then realize the deployment and implementation of network function through automated configuration execution and test verification. Network self-configuration based on intelligent endogenesis is characterized by intention transformation ability and dynamic adaptability. Self-configuration can identify the intention of the operator and translate advanced and abstract intention into a clear and quantifiable configuration through intelligent analysis and calculation, so as to provide personalized and adaptive network services and realize the optimization of network performance, user experience and cost.

Fig. 9 shows the construction and processing workflow of an intent engine. In the figure, the intent model formulates the specifications of the intent and its requirements are universal, flexible, with sufficient expression ability, and easy to carry out. The identification of intention includes speech recognition and intent recognition. Specific intentions will be identified in accordance with the texts obtained through speech recognition. Intent recognition needs to know the intentions that the system supports and also a series of label data for each intention (input of supervision learning). The intent policy defines intent implementation that translates received intentions into execution strategies and implements and feeds back the strategies, the intention maintenance that enables real-time



▲Figure 8. Key technologies of AI-native networks



▲ **Figure 9. Intent-based network and intent engine workflow**

perception, prediction and automatic adjustment, and the intent conflict that detects and resolves conflicts.

3.3 Digital Twin Network Technology

With the vision of "ubiquitous intelligence and digital twins" becoming the consensus of the industry, the digital twin technology is playing an important role in the network evolution. A digital twin network (DTN) is a system with physical network entities and virtual digital twins that can perform real-time interactive mapping and interoperation.

DTN[11 - 13] uses the digital twin technology to create virtual mirroring images of the physical network facilities, that is, to build a DTN platform that is consistent with the entity NE, with the physical topology and with real data. It provides the test bed for verifying the correctness of network configuration and the effect of new technologies, which greatly reduces the risk of the existing network and eliminates the possibility of network faults caused by incorrect configuration. DTN is expected to change the working mode of network planning, network establishment, maintenance, optimization and operation in the future and help the network achieve low-cost trial, intelligent decisions and efficient innovation through real-time interaction of the physical network and the twin network.

The relationship between the DNT and the intelligent network is complementary. Fig. 10 shows the collaborative architecture of the twin network and AN. A closed loop is formed between the twin network and the knowledge agent. Before any algorithm application, parameter adjustment and major operations, verification and iteration are carried out in the twin network to ensure a controllable impact and effect on the physical network.

In a digital twin network based on the core data model, simulation model layer and twin management, the data domain collects and stores basic data and is also responsible for data governance; the data model layer mainly processes the model representation of the data layer without the mechanism model; the simulation model layer mainly constructs the service model, such as the channel model, air interface model, network model, terminal model and service model. Building a full-cycle and end-to-end digital twin platform can help implement new technology innovation verification and rapid iteration of intelligent algorithms, and enhance the level of intelligence in collaboration with self-intelligent networks. The digital twin technology will be an important supporting platform technology for intelligent networks in the future. A reference architecture of the digital twin platform is shown in Fig. 11.

4 Exploration and Practice of Autonomous Network Technology

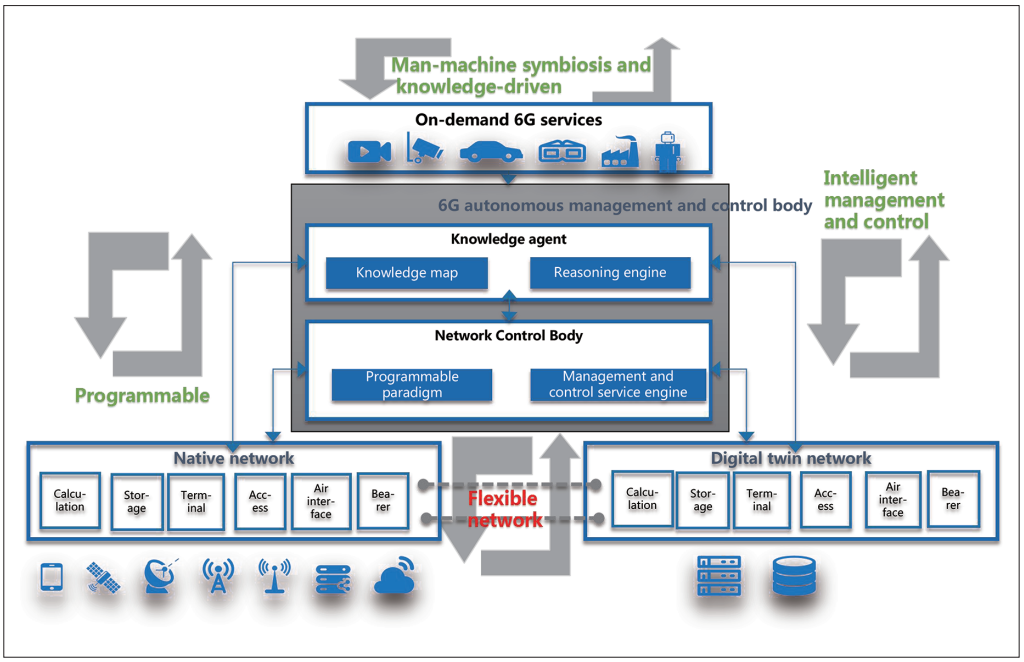
Use cases based on AN have been explored and researched, such as E2E root cause analysis based on closed-loop control, alarm compression based on a knowledge map, user experience assurance based on intention, and network dynamic planning based on digital twins. As follows, we will take the network planning of the Port of Rizhao, Shandong, China as an example to explain the practice of dynamic network planning based on DTN.

1) Characteristics of network planning for the Port

• Container stacking blocks the wireless signal. The stacking height can reach more than 20 m and the wireless signal cannot penetrate the metal box of the container.

• Container stacking dynamically changes. The height of container stacking often changes, the coverage area of wireless signals also changes, and the signal interference level changes constantly.

• The roads are narrow and densely distributed. The roads between the stacks can be up to more than 500 m long and the distance between the two adjacent roads is about 60 m.



▲Figure 10. Autonomous network system based on digital twin network

2) Disadvantages of the existing network planning solution to the Port

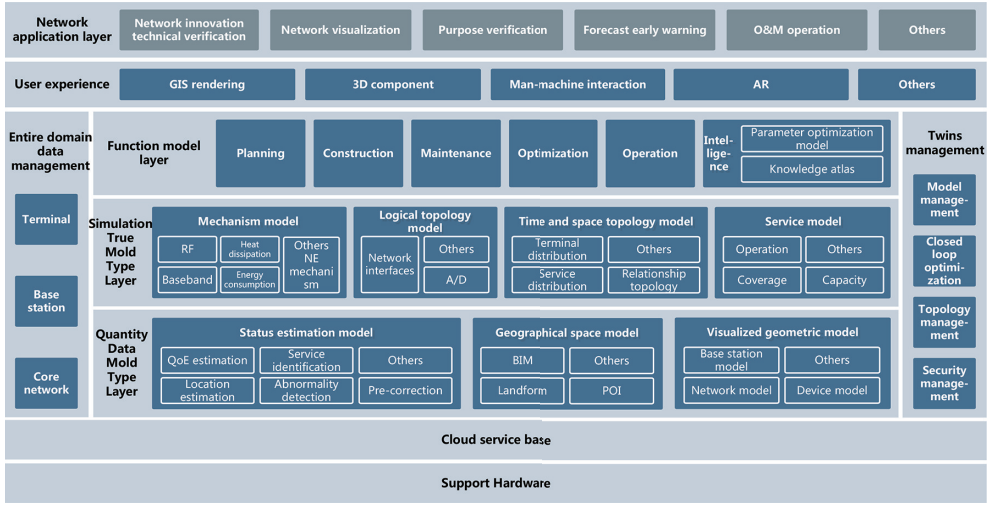
• The existing network planning only supports level network planning based on Reference Signal Receiving Power (RSRP)/Signal and Interference to Noise Ratio (SINR) and cannot match the clear QoS requirements of 2B scenarios.

• The network planning is based on static scenarios. For example, 2B scenarios at the Port of Rizhao may change dynamically, but the static network planning cannot match the scenarios.

• Multiple network optimization is relied on after network construction. For example, after the completion of a 2B scenario by Rizhao Port of Telecom, it usually takes several months of multiple network optimization, or even demolition and reconstruction, which greatly increases the cost.

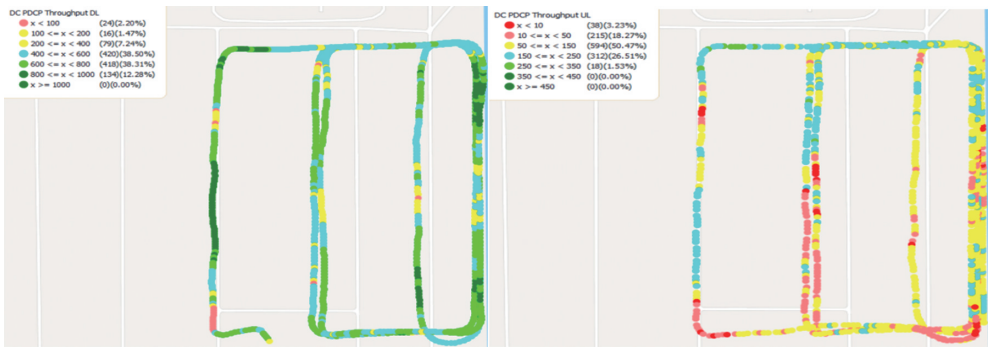
3) Benefits of dynamic planning schemes based on DTN for the Port

We use unmanned aerial vehicles to take photos of the Port of Rizhao first and obtain a digital twin network model of the port through 3D modeling. Through the digital twin network and ray tracing technology, we dynamically plan the network changes of the port. In this way, both the QoS level planning of the network and dynamic changes caused by container changes are supported. It can achieve "free network optimization" and support the design and version parameter planning of high-precision site hardware selection, site location selection, hanging height azimuth and so on, without manual network optimization. Fig. 12 shows the dynamic planning simulation results of this use case.



A/D: analog/digital
AR: augmented reality
BIM: building information modeling
GIS: geographic information system
NE: network element
O&M: operation and maintenance
POI: point of interest
QoE: quality of experience

▲Figure 11. Framework of digital twin network system



DC: dual-connectivity DL: downlink PDCP: Packet Data Convergence Protocol UL: uplink

▲**Figure 12. Dynamic network planning simulation based on digital twin network (DTN)**

5 Conclusions

At present, autonomous networks are booming and various autonomous systems are constantly emerging. Autonomous networks are moving from concept to reality. Looking forward to the future, we need to continuously promote the transformation of an intelligent ecosystem. In terms of standardization, academia and industry are expected to work together to promote the standardization of AI-native systems and also explore the standardization of data and intelligence. 3GPP AI-native endogenous data, algorithms and computing power may be supported. In terms of technological development, the integration of ICDT technology and the introduction of intention engine, digital twins, automatic learning and other technologies will enable the innovation and orderly evolution of intelligent networks in the future for new scenarios of intelligent communications, such as AI-AI (air interface based on AI), large-scale intelligent management and control, communication-sensing-computing integration and semantic communications.

Acknowledgement:

We would like to acknowledge ZTE experts, including RUI Hua, XIE Feng, ZHAN Yong, GU Jun, ZHAO Ding, FAN Xuefeng, GUAN Kai, SHI Xiaobin, DU Yongsheng et al. for their contribution to this paper.

References

[1] TMF. Autonomous networks: empowering digital transformation for the telecoms industry [R]. 2021
[2] FANG M, DUAN X Y, HU L J. Challenges, innovations and perspectives towards 6G [J]. ZTE technology journal, 2020, 26(3): 61 – 70. DOI: 10.12142/ZTETJ.202003012
[3] KANG H H, WANG Q. Autonomous network system architecture and technology development trend [J]. ZTE technologies, 2022, 26(5): 7 – 9
[4] ZTE Corporation. Self-evolving network white paper [R]. 2020
[5] ZHENG L X, GU J. Intelligent orchestration promotes the development of 5G users and improves network value [J]. ZTE technologies, 2021, 25(9): 13 – 15
[6] OSCAR Alliance. Enterprise AIOps intelligent O&M solution white paper [R], 2018
[7] IMT2030(6G) promotion group. 6G network architecture vision and key technologies, white paper [R]. 2021
[8] Future forum. Data-driven and intent-aware intelligent wireless network white paper [R], 2019
[9] ZHOU Y C, YAN S, PENG M G. Intent-driven 6G radio access network [J]. Chinese journal on Internet of Things, 2020, 4(1): 72 – 79
[10] WANG J Y, ZHOU C, ZHANG L, et al. Knowledge-defined intent-based network autonomy [J]. Telecommunications science, 2021, 37(9): 1 – 13
[11] China Mobile Research Institute. Digital twin network (DTN) white paper [R]. 2021
[12] SUN T, ZHOU C, DUAN X D, et al. Digital twin network (DTN): concept, architecture and key technologies [J]. Journal of automation, 2021, 47(3): 569 – 582
[13] CHEN D Y, LU L, SUN T. Multi-protocol cooperative interface for digital twin network [J]. ZTE technology journal, 2022, 28(1): 29 – 33. DOI: 10.12142/ZTETJ.202201008

Biographies

DUAN Xiangyang is Vice President of ZTE Corporation. His main research field is wireless communication technology. He has successively presided over and participated in more than three fund projects, and published over 20 papers.

KANG Honghui (kang.honghui@zte.com.cn) is the chief architect of ZTE Corporation. His research interest is wireless network intelligence. He has published five patents on wireless network intelligence technology and 6G network AI architecture and application.

ZHANG Jianjian is a senior project manager of ZTE Corporation, with a research focus on wireless network management automation and intelligent network O&M technology.

Broadband Sequential Load-Modulated Balanced Amplifier Using Coupler-PA Co-Design Approach

RAN Xiongbo, DAI Zhijiang, ZHONG Kang,
PANG Jingzhou, LI Mingyu
(School of Microelectronics and Communication Engineering, Chongqing University, Chongqing 400044, China)

DOI: 10.12142/ZTECOM.202204008
https://kns.cnki.net/kcms/detail/34.1294.TN.20221111.1327.002.html, published online November 14, 2022
Manuscript received: 2022-06-20

Abstract: The basic theory of the sequential load-modulated balanced amplifier (SLMBA) is introduced and the working principle of its active load modulation is analyzed in this paper. In order to further improve the performance of the SLMBA, a co-designed method of the coupler and power amplifier (PA) is proposed, which is different from the traditional design of couplers. According to the back-off point and saturation point of the SLMBA, this coupler-PA co-design approach can make the working state of the coupler and three-way PA closer to the actual situation, which improves the overall performance of the SLMBA. The maximum output power ratio of the control PA and the balance PA is then determined by the preset output power back-off (OBO) of 10 dB, and the phase compensation line is determined by the trace of the load modulation impedance of the balanced PA. In order to verify the proposed method, an SLMBA operating at 1.5–2.7 GHz (57% relative bandwidth) is designed. The layout simulation results show that its saturated output powers achieve 40.7–43.7 dBm and the small signal gains are 9.7–12.4 dB. Besides, the drain efficiencies at the saturated point and 10 dB OBO point are 52.7%–73.7% and 44.9%–59.2% respectively.

Keywords: SLMBA; broadband; coupler; co-design

Citation (IEEE Format): X. B. Ran, Z. J. Dai, K. Zhong, et al., "Broadband sequential load-modulated balanced amplifier using coupler-PA co-design approach," *ZTE Communications*, vol. 20, no. 4, pp. 62–68, Dec. 2022. doi: 10.12142/ZTECOM.202204008.

1 Introduction

With the advent of the 5G era, modern communication systems often using particularly complex modulation methods result in an increasingly larger peak-to-average power ratio (PAPR), which requires the power amplifier (PA) to keep high efficiency at the output power back-off (OBO) region. Load modulation PAs, as one of the architectures that can efficiently amplify high PAPR signals, have become a research hotspot in recent years.

With the emergence of a large number of new application scenarios, such as portable small base stations and smart wearable devices, the battery capacity determines the output power. Compared with the limited 6 dB OBO of a traditional Doherty PA[1-5], a larger range of OBO is required in these new scenarios. Active load modulation balanced power amplifiers (LMBA), as a new load modulation PA architecture, have great advantages in terms of high efficiency at large OBO and broadband design. They also have great potential in the construction of 5G base stations.

In 2016, SHEPPHARD et al. from Cardiff University, UK proposed a new dual-input PA architecture—LMBA[6]. Two directional couplers are used as the input and output networks of the two PAs respectively and the control signal is injected into the balanced PA through the isolated port of the output coupler. LMBA can modulate the load impedance of the balanced amplifier by changing the amplitude and phase of the external control signal to realize high efficiency at OBO. In 2017, PEDNEKAR et al.[7] from the University of Colorado, USA proposed a single-input LMBA architecture based on the traditional LMBA architecture. The output signal of a peaking PA is directly injected into the isolation port of the output coupler as a control signal to realize load modulation of the balanced PA and an octave LMBA which worked at 1.8–3.8 GHz is designed. The maximum output power is 44 dBm and added efficiencies at the 6 dB OBO are 29%–45%. In order to meet the application scenarios of wireless base stations, QUAGLIA et al.[8] of Cardiff University, UK proposed an LMBA architecture using the pre-matching technology and compared the bandwidth and linearity of the proposed structure with the

This work was supported in part by the National Natural Science Foundation of China under Grant Nos. 62001061, 62171068 and 62171065, and in part by ZTE Industry-University-Institute Cooperation Funds under Grant No. HC-CN-20210520005.
Corresponding author: DAI Zhijiang

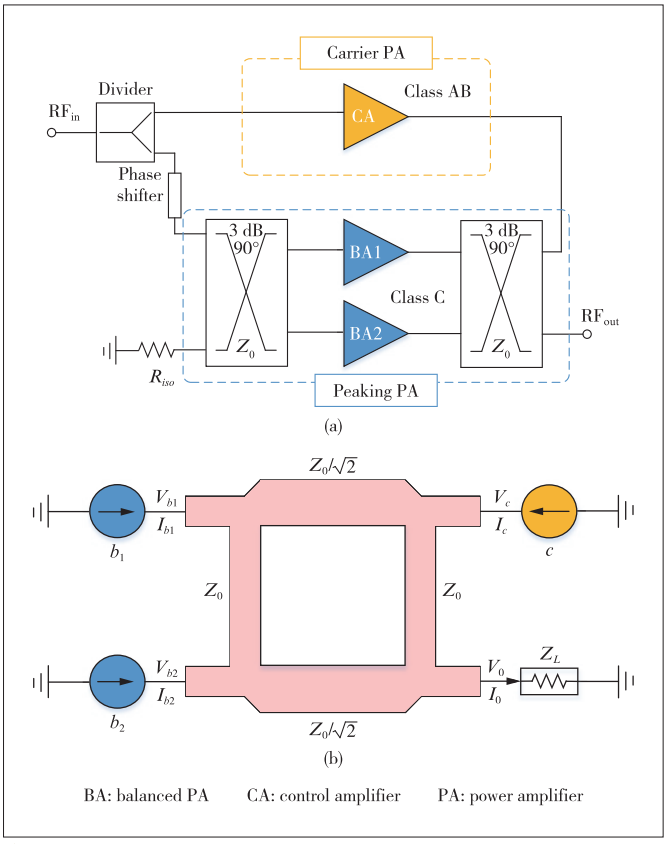
Doherty PA in 2018. An LMBA working in 1.7 – 2.5 GHz was designed for communication base stations. In 2020, PANG et al.[9] of University College Dublin, Ireland and CAYO et al.[10] of University of Central Florida, USA proposed a new LMBA architecture called Sequential LMBA (SLMBA). The control PA would work in class AB as the carrier PA and the balanced PA would work in class C as a peak PA. Compared with the traditional LMBA, this architecture can achieve a larger range of OBO and higher efficiency in the OBO region. In 2020, PANG et al.[11] also proposed an LMBA that worked in a continuous working mode and realized a continuous output matching network by controlling the phase difference of each PA branch. In 2021, CAO et al.[12] proposed an asymmetric SLMBA architecture, in which the balanced PA was composed of two PAs with different maximum power so that the impedance of the isolated termination of the output coupler was no longer constant. This meant that the control PA also had a load modulation progress and the overdriving of SLMBA was solved. An ALMBA with 0.55 – 2.2 GHz (relative bandwidth of 120%) was designed and the measured efficiencies at 10 dB OBO were 39% – 64%.

Since the first LMBA architecture was proposed in 2016, researchers have conducted a lot of research on it. However, the research generally focuses on application scenarios and architectural innovations and there are few targeted designs for its couplers. In this paper, we will study the co-design of the coupler and PAs for improving the overall performance of SLMBA.

2 Introduction and Theoretical Derivation of SLMBA

The architecture of SLMBA is shown in Fig. 1(a). In this architecture, a class AB amplifier is used as a carrier amplifier, while a balanced PA (BA) is biased in class C as a peaking amplifier. The carrier amplifier is connected to the isolated port of the 90° directional coupler as a control amplifier (CA), while the peaking amplifiers are connected to the through port and the coupling port, respectively. When the phase difference of two peaking amplifiers is 90°, they will become a balanced pair of amplifiers. In the low power region, when the output power is below the power of the predetermined OBO point, the peaking amplifiers are turned off and the output power is only provided by the carrier PA; when the output power is higher than the power of the predetermined OBO point, the two peaking PAs are turned on and the carrier amplifier reaches power saturation. With the further increase of input power, due to the saturation state of the carrier PA, the additional power increase is mainly provided by the peaking PAs.

As shown in Fig. 1(a), SLMBA consists of a CA and a pair of BAs. The BAs are biased in class C, in which two symmetrical PAs are connected at the input and output of two orthogonal directional couplers and the phase difference of two paths is 90°. A PA working in class AB is used as a CA, and its output signal is injected into the isolated port of the output coupler as a control signal of the SLMBA. The three-way PAs can be regarded as three current sources, which act on the output coupler as an excitation source. The current sources b_1 and b_2 are two symmetrical balanced PAs and the current source c is CA. Fig. 1(b) shows the load modulation schematic with an ideal coupler. The normalized $\boldsymbol{S}$ parameter matrix of the coupler can be directly obtained, as shown in Eq. (1).



▲ **Figure 1. (a) Sequential load-modulated balanced amplifier (SLMBA) architecture and (b) active load modulation model of SLMBA**

$$\boldsymbol{S} = \frac{-1}{\sqrt{2}}\begin{bmatrix} 0 & j & 1 & 0 \\ j & 0 & 0 & 1 \\ 1 & 0 & 0 & j \\ 0 & 1 & j & 0 \end{bmatrix}. \tag{1}$$

We set the characteristic impedance of the coupler to Z_0. According to the conversion relationship of the two-port network, the impedance matrix can be obtained as Eq. (2).

$$\boldsymbol{Z} = Z_0\begin{bmatrix} 0 & -\sqrt{2}\,j & 0 & j \\ -\sqrt{2}\,j & 0 & j & 0 \\ 0 & j & 0 & -\sqrt{2}\,j \\ j & 0 & -\sqrt{2}\,j & 0 \end{bmatrix}. \tag{2}$$

According to Eq. (2), the expression of the load impedance of the balanced PA can be deduced as Eq. (3).

$$Z_{b_1} = \frac{V_{b_1}}{I_{b_1}} = Z_0\left(1 - \sqrt{2}\,\frac{I_c e^{j\left(\frac{\pi}{2} - \Delta\theta_c\right)}}{I_{b_1}}\right) = Z_0\left(1 - \sqrt{2}\,\frac{e^{j\left(\frac{\pi}{2} - \Delta\theta_c\right)}}{\alpha}\right). \tag{3}$$

It can be seen from Eq. (3) that the load impedance of the BAs is only related to the characteristic impedance Z_0 of the coupler, the current ratio (α), and the phase difference between CA and BAs ($\Delta\theta_C$). Fig. 2(a) shows the impedance traces of the BAs and the CA with different phase differences and different output power levels under the OBO of 10 dB. As shown in Fig. 2(a), the load impedance of the CA remains constant and is not affected by the output current and output power of the BAs; the load impedances of the BAs are infinite when they are not turned on. However, the values of their load impedance gradually decrease with the increasing output power. It can be seen that the trajectories of Z_{BA} decrease along the real axis of the Smith chart and finally reach saturation with the increase of output power. Therefore, the theoretical optimal modulation phase difference of SLMBA is −90°. In the design, the phase difference of the two PAs is usually set to −90°.

The power and efficiency of SLMBA are derived below. When the phase difference is fixed as $\Delta\theta_C = -90°$, the output power of the CA and BAs can be deduced as:

$$P_c = \frac{1}{2}\mathrm{Re}\left[V_c I_c^*\right] = \frac{1}{2}Z_0 I_c^2,$$
$$P_b = 2*\frac{1}{2}\mathrm{Re}\left[V_{b_1} I_{b_1}^*\right] = Z_0 I_c^2\left[\alpha^2 - \sqrt{2}\,\alpha\cos\left(\Delta\theta_c - \frac{\pi}{2}\right)\right]. \tag{4}$$

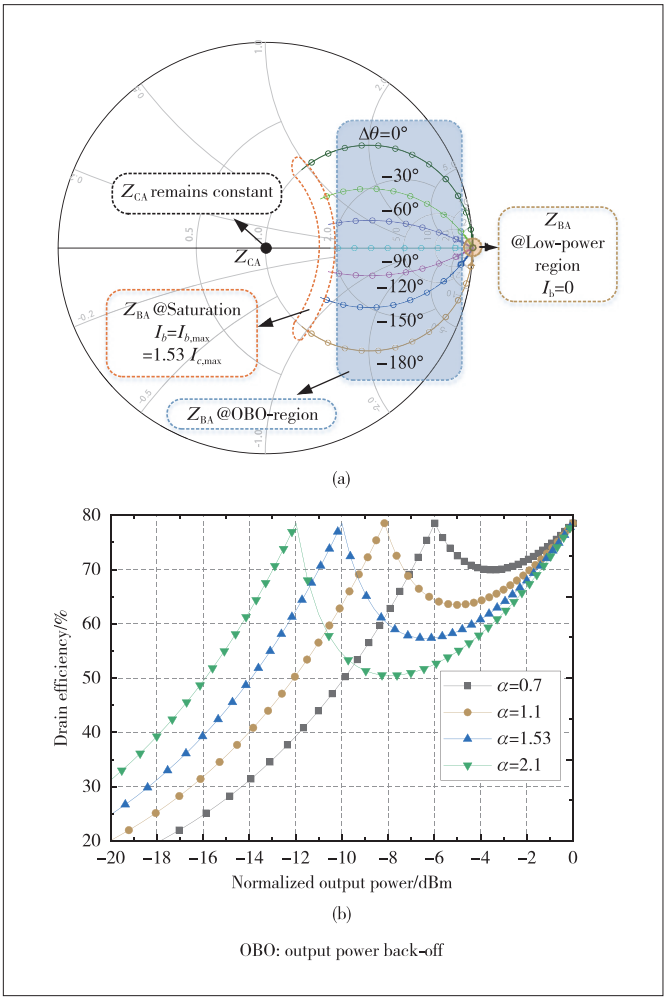
From Eq. (4), the relationship between the output power of SLMBA and the output power of the three PAs can be obtained:

$$P_{\text{out}} = \frac{1}{2}\mathrm{Re}\left[V_0 I_0^*\right] = P_c + P_b. \tag{5}$$

It can be seen from Eq. (5) that the output power of the SLMBA is equal to the sum of the output power of the CA and BAs. Therefore, the efficiency of SLMBA can be expressed as:

$$\eta_{\text{SLMBA}} = \frac{P_c + P_b}{P_{c,\text{DC}} + P_{b,\text{DC}}}. \tag{6}$$

After the value of OBO is determined, the current ratio α is also determined. For instance, if the value of OBO is 10 dB, α is 1.53. Fig. 2(b) shows the drain efficiency curves of SLMBA at different current ratios.



▲ **Figure 2. (a) Load impedance traces of sequential load-modulated balanced amplifier (SLMBA) (OBO=10 dB) and (b) drain efficiency curves of SLMBA at different values of α**

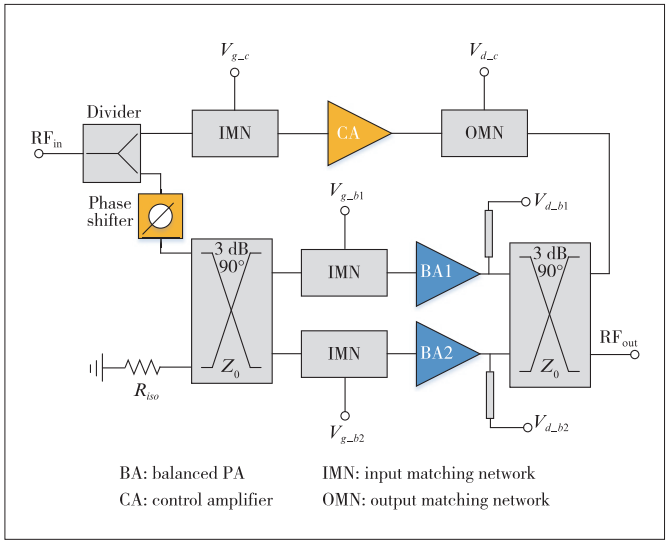
3 Design of Broadband SLMBA

Fig. 3 shows the schematic diagram of the broadband SLMBA architecture. The CA works in class AB as the carrier PA. The maximum output power of the BAs is equal, and the BAs work in class C as the peak PA. The output coupler is directly used as the output network of the BAs to avoid SLMBA's bandwidth being limited by additional output-matching networks.

According to the working principle of SLMBA described in the previous section, amplitude modulation consists of two basic parts: 1) determining the current or power ratio between the BAs and the CA and 2) controlling CA to work in a saturation state and BAs to turn on simultaneously in the power back-off region.

The maximum output power of CA depends on the saturation output power of SLMBA and the OBO level. The relationship between the saturation output power of SLMBA and the preset OBO can be described as:

$$P_{\text{CA,SAT}} = \frac{P_{\text{Total,SAT}}}{\text{OBO}}, \tag{7}$$



▲ **Figure 3. Architecture of broadband sequential load-modulated balanced amplifier (SLMBA)**

where $P_{\text{Total, SAT}}$ represents the saturation output power of SLMBA, which is the sum of the output power of CA and BAs:

$$P_{\text{Total, SAT}} = P_{\text{BA, SAT}} + P_{\text{CA, SAT}}. \tag{8}$$

In the actual design process, the preset range of OBO can be realized by selecting BAs and CA transistors with appropriate output power. The CA of this design adopts CGH40010F provided by Wolfspeed and the standard drain voltage is 28 V. However, the drain voltage of the CA is stepped down to 12 V to expand the range of OBO. This can extend the OBO range to 10 dB. The selection of the output power of the BAs is shown in Eq. (9).

$$P_{\text{BA,SAT}} = (\text{OBO} - 1)P_{\text{CA,SAT}}. \tag{9}$$

Therefore, we chose CGH40010F with a standard output power of 10 W and a drain voltage of 28 V as BAs to achieve OBO=10 dB. Then the gate voltage is controlled to make BAs work in class C and turn on at the preset OBO point. Since the CA is in power saturation in the entire range of OBO, the total output power of the SLMBA depends largely on the output power of the BAs.

According to the theory of SLMBA deduced above, the load impedance of CA in the whole process of SLMBA remains unchanged with infinite isolation of the ideal coupler:

$$Z_{\text{C}} = Z_0 = 50\ \Omega. \tag{10}$$

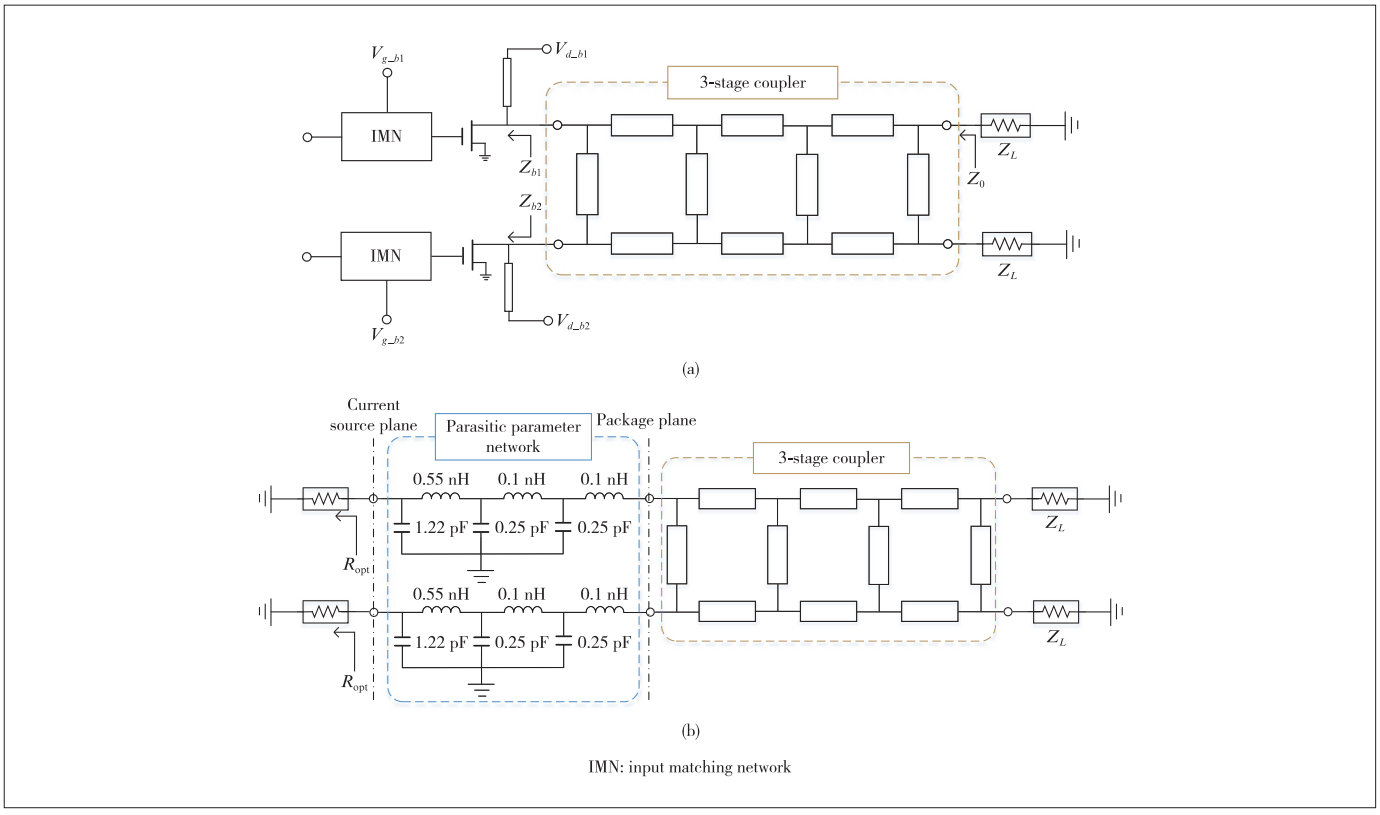
The main bandwidth limitation of a Doherty PA is brought by the inverter network of 90°of the carrier PA. For an SLMBA, the load of the output network of the carrier PA remains unchanged. Therefore, the SLMBA has the potential to extend broadband. Since the load of CA remains unchanged during the whole working process of SLMBA, its design can be directly performed as an independent single PA, which can greatly reduce the design difficulty.

For BAs, the expression of the load impedance is shown in Eq. (3) after they are turned on. It can be seen that the performance depends greatly on the parameters of the coupler, so the design of the coupler is very important for SLMBA. However, in the actual design, the isolation degree of the isolated termination of the coupler will not be ideal, which will cause the output impedance of the isolated termination to fluctuate. So it will seriously reduce the efficiency at the OBO level of the SLMBA. Meanwhile, the load impedances of the coupler's input ports are influenced by the active BAs instead of any fixed passive load impedance, which also shows that the independent design method of the coupler does not conform to the actual working state of SLMBA.

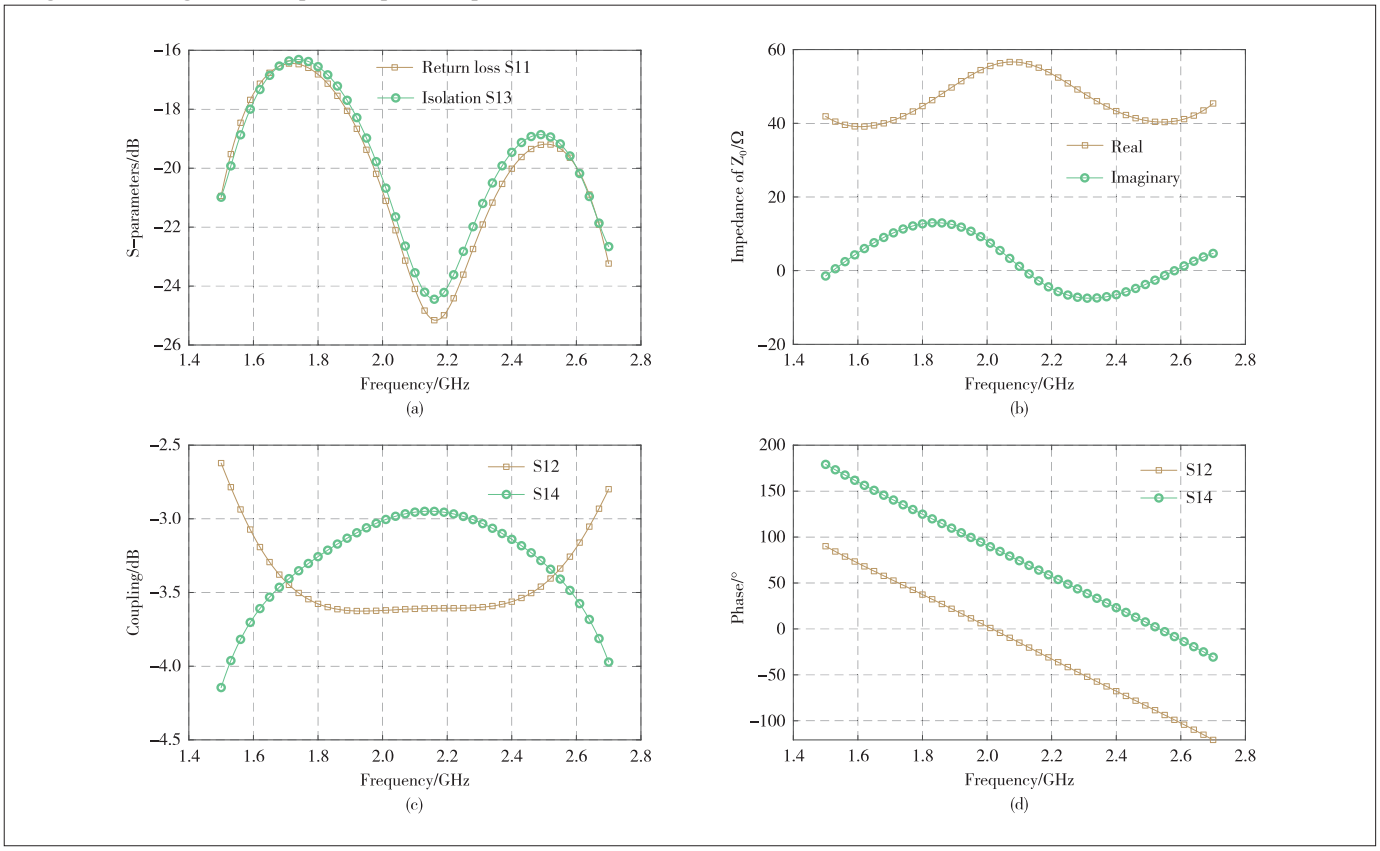
Therefore, based on the above two aspects, a method for co-design of the coupler and PAs is proposed in this paper. In the proposed method, the OBO and saturation states of SLMBA are designed respectively. The schematic diagram of the proposed SLMBA is shown in Fig. 4. In the design of the OBO state, two BAs are directly used as the load condition of the input port of the coupler. On this basis, the output impedance of the isolated termination of the coupler is made constant to reduce the load fluctuation of the control PA for improving the efficiency at the OBO of SLMBA. For the design of the saturated state, the optimal impedance of the transistor R_{opt} and the transistor package parameter network are regarded as the load conditions of the input port of the coupler. On this basis, the parameters such as isolation and coupling of the coupler are designed. The advantage of the proposed co-design approach (Fig. 4) makes the operations of the coupler and three PAs closer to the actual situation, which can improve the overall performance of SLMBA. The simulation results of the designed 3-stage coupler are shown in Fig. 5.

Then, the phase modulation should be designed. It can be known that the impedance modulation of BAs will have different traces under different phase differences between the CA and BAs. That is to say, the phase difference between the two branches will affect the efficiency of the range of OBO in the whole operating frequencies, so it is significant to control the phase modulation.

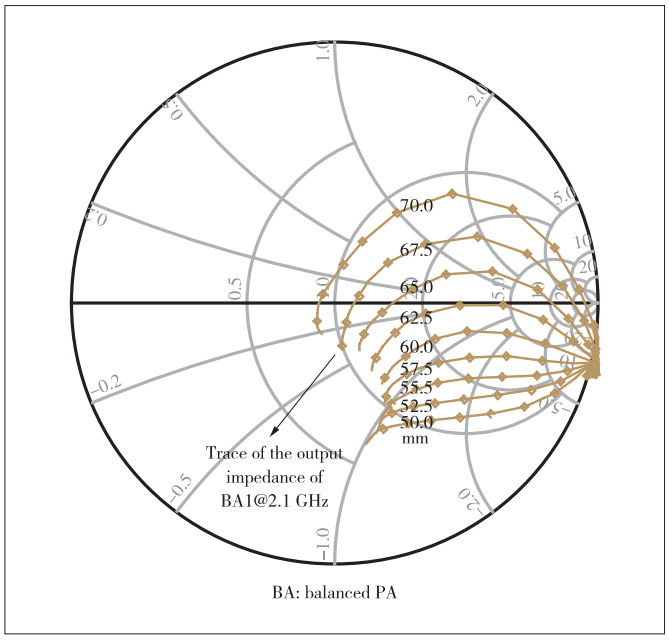
Fig. 6 shows the impedance modulation traces of BA under the different phase compensation lines at the center frequency of 2.1 GHz. According to the load line of classical class B PAs[12], a purely resistive impedance trace is optimal for its power and efficiency. It can be seen that the impedance trajectory of BA is the closest to the real axis (pure resistance) when the input phase compensation line is 62.5 mm. According to Ref. [13], the slope of the phase compensation required by SLMBA with frequency is basically the same as the microstrip line. Therefore, the SLMBA phase can be greatly compensated in the entire operating frequencies when the input phase compensation line of BA is connected to the 62.5 mm



▲ **Figure 4. Co-design of the coupler and power amplifier (PA): (a) back-off state; (b) saturation state**



▲ **Figure 5. Simulation results of the 3-way coupler**



▲ **Figure 6. Impedance traces of BA1 under different phase compensations**

transmission line.

By debugging the layout of SLMBA, the length of the phase compensation line is set to 60 mm. The printed circuit board (PCB) structure of SLMBA designed by using the proposed co-design method of coupler-PA is shown in Fig. 7. The simulation results are shown in Fig. 8. The designed SLMBA with 1.5 – 2.7 GHz (relative bandwidth 57%) has saturated output powers of 40.7 – 43.7 dBm with saturated drain efficiencies of 52.7% – 73.7%, the small signal gain is 9.7 – 12.4 dB, and the efficiencies are 44.9% – 59.2% at 10 dB OBO level.

4 Conclusions

Different from the traditional coupler design method, a co-design approach is proposed for the design of the output coupler and matching network of SLMBA, which improves the performance of SLMBA at the back-off and saturation states. An SLMBA operating at 1.5 – 2.7 GHz (57% relative bandwidth) is then designed. The layout simulation results show that its saturated output power reaches 40.7 – 43.7 dBm, the small signal gain is 9.7 – 12.4 dB, saturated drain efficiency is 52.7% – 73.7%, and 10 dB output power back-off efficiency is 44.9% – 59.2%.

References

[1] PANG J, HE S, HUANG C, et al. A post-matching doherty power amplifier employing low-order impedance inverters for broadband applications [J]. IEEE transactions on microwave theory and techniques, 2015, 63(12): 4061 – 4071. DOI: 10.1109/TMTT.2015.2495201

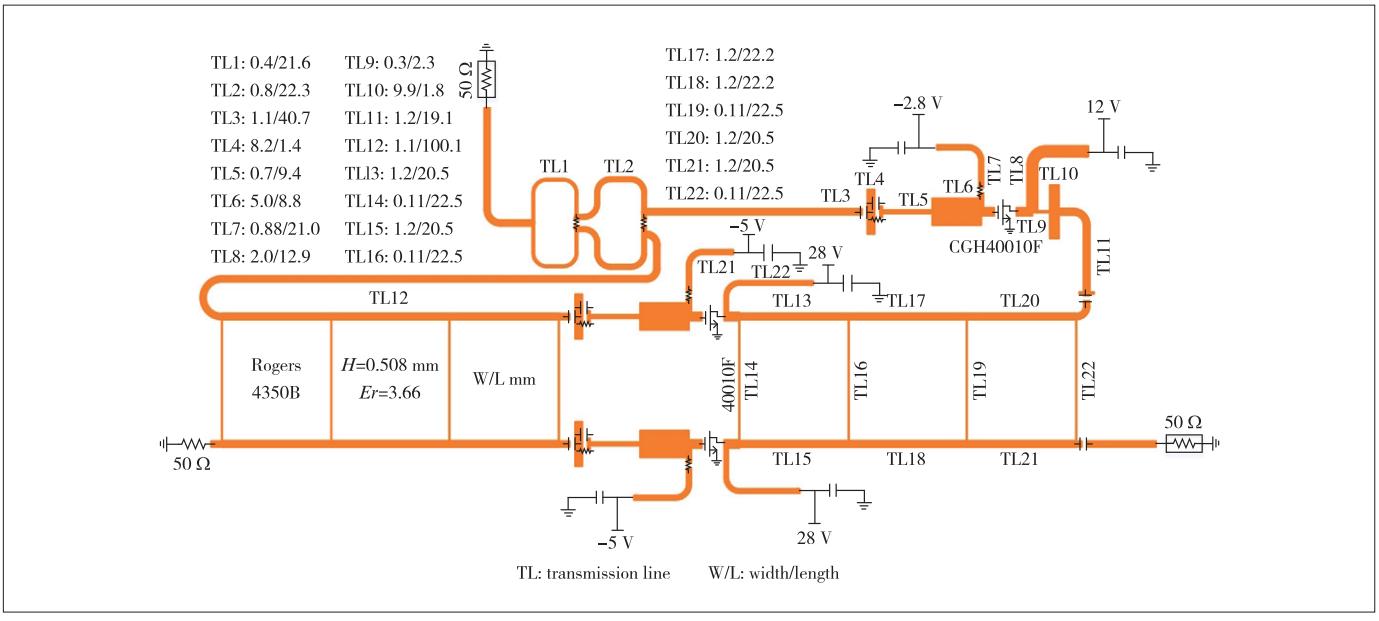
[2] KANG H, LEE H, LEE W, et al. Octave bandwidth doherty power amplifier using multiple resonance circuit for the peaking amplifier [J]. IEEE transactions on circuits and systems I: regular papers, 2019, 66(2): 583 – 593. DOI: 10.1109/TCSI.2018.2869905

[3] MOON J, KIM J, KIM J, et al. Efficiency enhancement of doherty amplifier through mitigation of the knee voltage effect [J]. IEEE transactions on microwave theory and techniques, 2011, 59(1): 143 – 152. DOI: 10.1109/TMTT.2010.2091207

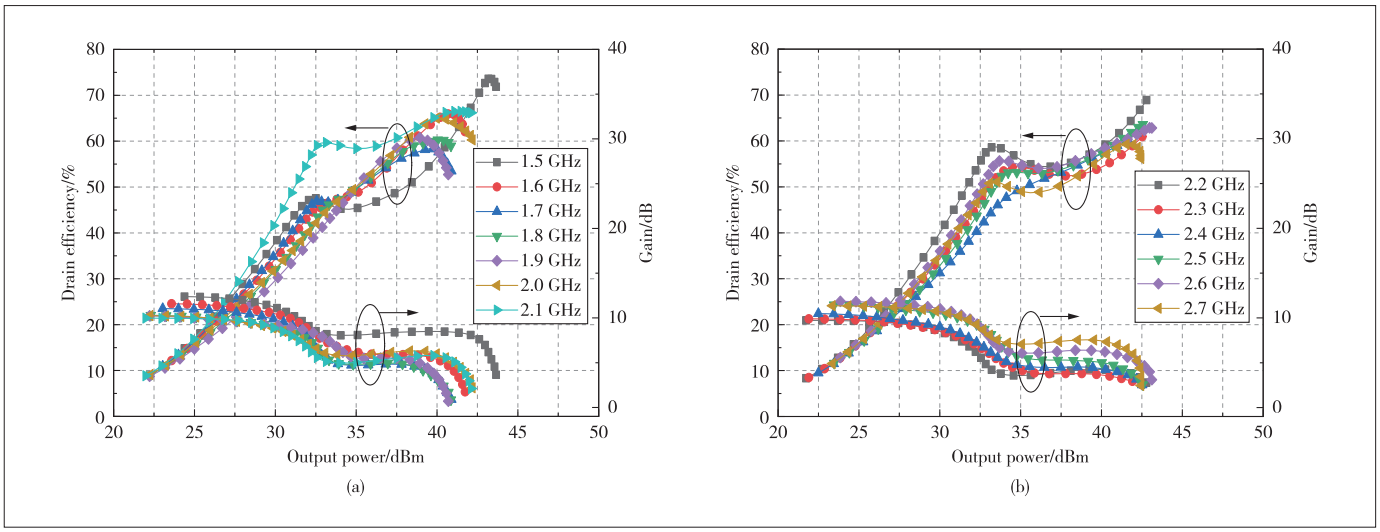
[4] COLANTONIO P, GIANNINI F, GIOFRE R, et al. Increasing doherty amplifier average efficiency exploiting device knee voltage behavior [J]. IEEE transactions on microwave theory and techniques, 2011, 59(9): 2295 – 2305. DOI: 10.1109/TMTT.2011.2160278

[5] FANG X-H, LIU H-Y, CHENG K-K M, et al. Two-way doherty power amplifier efficiency enhancement by incorporating transistors' nonlinear phase distortion [J]. IEEE microwave and wireless components letters, 2018, 28(2): 168 – 170. DOI: 10.1109/LMWC.2017.2783845

[6] SHEPPHARD D J, POWELL J, CRIPPS S C. An efficient broadband reconfigurable power amplifier using active load modulation [J]. IEEE microwave and wireless components letters, 2016, 26(6): 443 – 445. DOI: 10.1109/LMWC.2016.2559503



▲ **Figure 7. Printed circuit board (PCB) structure of the designed sequential load-modulated balanced amplifier (SLMBA)**



▲ **Figure 8. Simulation results of the sequential load-modulated balanced amplifier (SLMBA)**

[7] PEDNEKAR P H, BERRY E, BARTON T W. RF-input load modulated balanced amplifier with octave bandwidth [J]. IEEE transactions on microwave theory and techniques, 2017, 65(12): 5181 – 5191. DOI: 10.1109/TMTT.2017.2748123
[8] QUAGLIA R, CRIPPS S. A load modulated balanced amplifier for telecom applications [J]. IEEE transactions on microwave theory and techniques, 2018, 66 (3): 1328 – 1338. DOI: 10.1109/TMTT.2017.2766066
[9] PANG J, LI Y, LI M, et al. Analysis and design of highly efficient wideband RF-input sequential load modulated balanced power amplifier [J]. IEEE transactions on microwave theory and techniques, 2020, 68(5): 1741 – 1753. DOI: 10.1109/TMTT.2019.2963868
[10] CAO Y, CHEN K. Pseudo-doherty load-modulated balanced amplifier with wide bandwidth and extended power back-off range [J]. IEEE transactions on microwave theory and techniques, 2020, 68(7): 3172 – 3183. DOI: 10.1109/TMTT.2020.2983925
[11] PANG J, CHU C, LI Y, et al. Broadband RF-input continuous-mode load-modulated balanced power amplifier with input phase adjustment [J]. IEEE transactions on microwave theory and techniques, 2020, 68(10): 4466 – 4478. DOI: 10.1109/TMTT.2020.3012141
[12] Y. CAO Y, LYU H, CHEN K. Asymmetrical load modulated balanced amplifier with continuum of modulation ratio and dual-octave bandwidth [J]. IEEE transactions on microwave theory and techniques, 2021, 69(1): 682 – 696. DOI: 10.1109/TMTT.2020.3014616
[13] CAO Y, CHEN K. Pseudo-doherty load-modulated balanced amplifier with wide bandwidth and extended power back-off range [J]. IEEE transactions on microwave theory and techniques, 2020, 68(7): 3172 – 3183. DOI: 10.1109/TMTT.2020.2983925

Biographies

RAN Xiongbo received his BSc degree in electronic engineering from the Hangzhou Dianzi University, China in 2019, and MSc degree in electronic engineering from the School of Microelectronics and Communication Engineering, Chongqing University, China in 2022. His research interests include microwave and millimeter-wave devices and circuits, and wideband high-efficiency power amplifier design.

DAI Zhijiang (daizj_ok@126.com) received his BS and PhD degrees in electrical engineering from University of Electronic Science and Technology of Chinain in 2011 and 2017, respectively. From 2017 to 2018, he was a research engineer with Huawei Technologies, where he focused on the study of MIMO wireless communication systems. He is currently a lecturer with the School of Microelectronics and Communication Engineering, Chongqing University, China. His research interests lie in the area of automatic matching techniques of PA, wideband and linear RF PA design, MMIC circuits, and wireless communication systems.

ZHONG Kang received his BS degree in electronic information engineering from Guizhou University, China in 2021. He is currently pursuing his MS degree at the School of Microelectronics and Communication Engineering, Chongqing University, China. His current research interests include broadband high-efficiency power amplifiers and load modulated power amplifiers.

PANG Jingzhou received his BS degree in electrical engineering and PhD degree in circuits and systems from University of Electronic Science and Technology of China in 2010 and 2016, respectively. From December 2016 to July 2018, he was with Huawei Technologies Company Ltd., Chengdu, where he was an engineer in charge of the research and development of 5G high-efficiency power amplifiers and transmitters. From July 2018 to August 2020, he was with the RF and Microwave Research Group, University College Dublin, Ireland, where he was a research fellow in charge of the research of novel broadband transmitter architectures and RF/microwave/millimeter-wave monolithic microwave integrated circuit (MMIC) power amplifiers. He is currently an associate professor with the School of Microelectronics and Communication Engineering, Chongqing University, China. His research interests include broadband high-efficiency power amplifier systems, bandwidth extension techniques for high-efficiency transmitters, and MMIC power amplifier design for RF/microwave and millimeter-wave applications. Dr. PANG was a recipient of the EDGE Marie Sklodowska-Curie Individual Fellowship and the Third Place Award of the High Efficiency Power Amplifier Student Design Competition at the IEEE Microwave Theory and Techniques Society (IEEE MTT-S) International Microwave Symposium (IMS) in 2013.

LI Mingyu received his PhD degree in electronic engineering from University of Electronic Science and Technology of China, in 2009. From 2012 to 2013, he was a research fellow with The University of Kitakyushu, Kitakyushu, Japan. He is currently an associate professor with the School of Microelectronics and Communication Engineering, Chongqing University, China. His current research interests include RF/microwave transceiver design, statistical and adaptive signal processing for wireless communications, and behavioral modeling and linearization for RF power amplifiers.

Distributed Multi-Cell Multi-User MISO Downlink Beamforming via Deep Reinforcement Learning

JIA Haonan[1], HE Zhenqing[1], TAN Wanlong[1], RUI Hua[2,3], LIN Wei[2,3]

(1. National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China;
2. ZTE Corporation, Shenzhen 518057, China;
3. State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen 518055, China)

DOI: 10.12142/ZTECOM.202204009

https: //kns.cnki.net/kcms/detail/34.1294.TN.20221124.0844.002.html, published online November 25, 2022

Manuscript received: 2022-02-24

Abstract: The sum rate maximization beamforming problem for a multi-cell multi-user multiple-input single-output interference channel (MISO-IC) system is considered. Conventionally, the centralized and distributed beamforming solutions to the MISO-IC system have high computational complexity and bear a heavy burden of channel state information exchange between base stations (BSs), which becomes even much worse in a large-scale antenna system. To address this, we propose a distributed deep reinforcement learning (DRL) based approach with limited information exchange. Specifically, the original beamforming problem is decomposed of the problems of beam direction design and power allocation and the costs of information exchange between BSs are significantly reduced. In particular, each BS is provided with an independent deep deterministic policy gradient network that can learn to choose the beam direction scheme and simultaneously allocate power to users. Simulation results illustrate that the proposed DRL-based approach has comparable sum rate performance with much less information exchange over the conventional distributed beamforming solutions.

Keywords: deep reinforcement learning; downlink beamforming; multiple-input single-output interference channel

Citation (IEEE Format): H. N. Jia, Z. Q. He, W. L. Tan, et al., "Distributed multi-cell multi-user miso downlink beamforming via deep reinforcement learning," *ZTE Communications*, vol. 20, no. 4, pp. 69 - 77, Dec. 2022. doi: 10.12142/ZTECOM.202204009.

1 Introduction

To meet the increasing wireless communication traffic demand, the frequency reuse factor of cellular systems is expected to be slackened as one, which indicates that all the cells operate in the same frequency band. However, the small frequency reuse factor brings an inter-cell interference problem, heavily degrading the achievable sum rate performance of the wireless system. Therefore, inter-cell interference should be managed carefully. A multi-cell multiple-input single-output (MISO) downlink beamforming technique with cooperation among the base stations (BSs) is introduced as a promising solution. The typical zero-forcing beamforming[1] works in a highly coordinated scenario where each piece of user equipment (UE) is served by all the BSs, which needs all the transmit data and channel state information (CSI) to be shared among the BSs. Nevertheless, it is impractical due to the heavy data-sharing burden[2]. A centralized solution[3] collects the global CSI and jointly design beamforming vectors based on fractional programming (FP). Although it can achieve near-optimal performance, it has high computational complexity and leads to unavoidable delays when collecting CSI and sending beamforming vectors, thereby making it impossible to be applied in a dynamic channel environment.

Many distributed schemes are proposed to reduce the computational cost of centralized solutions. In particular, an achievable rate region of the multi-cell MISO Gaussian interference channel (MISO-IC) system is analyzed in Ref. [4], which proves that the well-designed distributed schemes can reach the Pareto boundary. To reduce information sharing among BSs, a data-sharing-based distributed scheme is proposed in Ref. [5]. A fully distributed scheme with no CSI or data sharing is discussed in Ref. [6], which works well at a high signal-to-interference-plus-noise-ratio (SINR). However, these works assume that the BSs are capable of obtaining the instantaneous downlink CSI of the UE in other cells without

This work is supported by the joint research project with ZTE Corporation under Grant No. HC-CN-2020120002.

CSI sharing, which is also infeasible in a practical system.

Deep reinforcement learning (DRL) has shown great potential in decision-making problems. By converting the multi-cell downlink beamforming problem into a decision-making problem, several distributed approaches based on DRL are developed[7-8]. Particularly, a multi-agent deep Q-learning based approach is introduced in Ref. [7], in which each BS learns to make the decisions of beam direction and power for each UE based on the local CSI and the exchanged information among the BSs. However, because of the curse of dimensionality[9], the Q-learning based approach in Ref. [7] is almost impossible to be applied in the cases where there are multiple user devices in the same cell or the BSs are equipped with large-scale antennas, since the discrete action space expands exponentially with the number of user devices and antennas.

In this paper, we develop a distributed-training distributed-execution (DTDE) multi-agent deep deterministic policy gradient (MADDPG) based algorithm to maximize the instantaneous sum rate of the multicell multi-user MISO-IC system under the power constraint for each BS. Thanks to the features of DDPG, the policy network gives continuous value directly, which significantly reduces the dimension of actions. Our main contributions are summarized as follows:

1) A new distributed MADDPG-based scheme is proposed, capable of solving the instantaneous sum rate maximization problem when cells have multiple user devices and BSs are equipped with large-scale antennas. By decomposing the original beamforming problem into the beam direction design and power allocation problems, each BS as an agent can learn to choose beam direction and power allocation based on the wireless environment.

2) A new limited information exchange protocol is proposed for the distributed BSs to share information for beamforming design. Instead of sharing CSI directly, we choose the equivalent channel gains of UE, the received interference of UE, and the sum rate of UE in one cell as the shared information. Different from other DRL-based algorithms which only consider equivalent channel gains and the sum rate of UE, we consider the received interference (also known as the interference temperature) as the crucial information.

3) Extensive experiments are conducted to evaluate the efficiency and scalability of the proposed MADDPG approach by comparing the conventional distributed and centralized solutions. The simulation results show that the proposed MADDPG can reach the state-of-the-art sum rate performance with a much smaller amount of information sharing among BSs.

As far as we know, this is the first attempt to tackle the multi-cell MISO beamforming via MADDPG-based DRL. In contrast to the related work[7], this paper aims to solve the multi-cell sum rate maximization problem in the continuous action space by using the MADDPG method which is more flexible for different wireless environments and is easy for agents (e.g., BSs) to learn since the dimension of action space is much smaller than that of codebook space in Ref. [7].

In this paper, we use $\mathbb{C}^{m\times n}$ and $\mathbb{R}^{m\times n}$ to represent the spaces of the $m\times n$ dimensional complex number and real number, respectively. The superscripts "$*$", "T", and "H" denote the conjugate, the transpose, and the conjugate transpose, respectively. In addition, we use $\jmath \triangleq \sqrt{-1}$, $\mathbb{E}\{\cdot\}$, and $\|\cdot\|$ as the imaginary unit, the expectation operator, and the ℓ_2 norm, respectively.

2 System Model

We consider a wireless cellular downlink system of N cells, in each of which there is a multi-antenna transmitter (e.g., a BS) with M antennas to serve K single-antenna receivers (e.g., UE). We use $\mathcal{N}=\{1,\cdots,N\}$ to denote the set of all BSs. We assume that all UE in this system shares the same frequency band, thereby leading to both intra-cell and inter-cell interference with each UE. As a result, the received signal of the k-th UE in the n-th cell at time t can be expressed as:

$$y_{n,k}(t)=\underbrace{\boldsymbol{h}_{n,n,k}^{\mathrm{T}}(t)\boldsymbol{w}_{n,k}(t)x_{n,k}(t)}_{\text{desired signal}}+\underbrace{\sum_{j=1,j\neq k}^{K}\boldsymbol{h}_{n,n,k}^{\mathrm{T}}(t)\boldsymbol{w}_{n,j}(t)x_{n,j}(t)}_{\text{intra-cell interference}}+\underbrace{\sum_{i=1,i\neq n}^{N}\sum_{j=1}^{K}\boldsymbol{h}_{i,n,k}^{\mathrm{T}}(t)\boldsymbol{w}_{i,j}(t)x_{i,j}(t)}_{\text{inter-cell interference}}+z_{n,k}(t),\tag{1}$$

where $\boldsymbol{h}_{i,n,k}(t)\in\mathbb{C}^{M}$ denotes the downlink channel vector from the BS in the i-th cell to the k-th UE in the n-th cell, $\mathbf{w}_{i,n,k}(t)\in\mathbb{C}^{M}$ denotes the beamforming vector for the j-th UE in the i-th cell, $x_{i,j}$ denotes the transmitted symbol to the j-th UE in the i-th cell, and $z_{i,j}(t)\sim\mathcal{CN}\left(0,\sigma_{n,k}^{2}\right)$ denotes the additive noise with $\sigma_{n,k}^{2}$ being the noise power. Under the single user detection mechanism, the instantaneous SINR and achievable rate of the k-th UE in the n-th cell are given by:

$$\gamma_{n,k}(t)=\frac{\left|\boldsymbol{h}_{n,n,k}^{\mathrm{T}}(t)\boldsymbol{w}_{n,k}(t)\right|^{2}}{\beta_{n,k}^{\mathrm{intra}}(t)+\beta_{n,k}^{\mathrm{inter}}(t)+\sigma_{n,k}^{2}},\tag{2a}$$

$$R_{n,k}(t)=\log_{2}\left(1+\gamma_{n,k}(t)\right),\tag{2b}$$

where $\beta_{n,k}^{\mathrm{intra}}(t)=\sum_{j=1,j\neq k}^{K}|\boldsymbol{h}_{n,n,k}^{\mathrm{T}}(t)\boldsymbol{w}_{n,j}(t)|^{2}$ and $\beta_{n,k}^{\mathrm{inter}}(t)=\sum_{i=1,i\neq n}^{N}\sum_{j=1}^{K}|\boldsymbol{h}_{i,n,k}^{\mathrm{T}}(t)\boldsymbol{w}_{i,j}(t)|^{2}$ represent the intra-cell and inter-cell interferences.

We assume that the BS in each cell is equipped with the uniform rectangular array (URA) structure with $M=M_xM_y$ an-

tenna elements,[1] where M_x and M_y denote the horizontal and vertical scales of the URA, respectively. According to the ray-based channel modeling[10], the dynamic URA channel response of $\boldsymbol{h}_{n,j,k}(t)$ with L-paths for the n-th BS to the k-th UE in the cell j can be expressed as:

$$\boldsymbol{h}_{n,j,k}(t) = \sqrt{\kappa_{n,j,k}} \sum_{l=1}^{L} g_{n,j,k,l}(t) \bar{\boldsymbol{a}}\left(u_{n,j,k,l}\right) \otimes \bar{\boldsymbol{b}}\left(v_{n,j,k,l}\right), \tag{3}$$

where $\kappa_{n,j,k}$ is the large-scale fading factor related to the path loss and shadowing and $g_{n,j,k,l}(t)$ is the dynamic small-scale Rayleigh fading factor. The steering vectors $\bar{\boldsymbol{a}}$ and $\bar{\boldsymbol{b}}$ of URA in Eq. (3) are given by:

$$\bar{\boldsymbol{a}}\left(u_{n,j,k,l}\right) = \left[1, e^{-u_{n,j,k,l}}, \cdots, e^{-(M_x-1)u_{n,j,k,l}}\right]^{\top}, \tag{4a}$$

$$\bar{\boldsymbol{b}}\left(v_{n,j,k,l}\right) = \left[1, e^{-v_{n,j,k,l}}, \cdots, e^{-(M_y-1)v_{n,j,k,l}}\right]^{\top}, \tag{4b}$$

where $u_{n,j,k,l} = \frac{2\pi d_1}{\lambda} \sin\left(\theta_{n,j,k,l}\right) \cos\left(\phi_{n,j,k,l}\right)$, $v_{n,j,k,l} = \frac{2\pi d_2}{\lambda} \cos\left(\theta_{n,j,k,l}\right)$, $d_1 = d_2 = \frac{\lambda}{2}$, and λ is the signal wave length. The elevation angle-of-departure (AoD) $\theta_{n,j,k,l}$ and azimuth AoD $\phi_{n,j,k,l}$ of each path are given by:

$$\theta_{n,j,k,l} \sim \mathcal{U}\left(\theta_{n,j,k} - \frac{\Delta}{2}, \theta_{n,j,k} + \frac{\Delta}{2}\right), \tag{5a}$$

$$\phi_{n,j,k,l} \sim \mathcal{U}\left(\phi_{n,j,k} - \frac{\Delta}{2}, \phi_{n,j,k} + \frac{\Delta}{2}\right), \tag{5b}$$

where $\theta_{n,j,k}$ and $\phi_{n,j,k}$ are the nominal AoD between the cell n and the UE k in cell j, respectively, and Δ is the associated angular perturbation.

To characterize the small-scale fading dynamics of the time varying channel, we utilize the following first-order Gauss-Markov process[11].

$$g_{n,j,k,l}(t+1) = \sqrt{\rho}\, g_{n,j,k,l}(t) + \sqrt{1-\rho}\, \delta_{n,j,k,l}(t), \tag{6}$$

where ρ denotes the fading correlation coefficient between any two consecutive time slots and $\delta_{n,j,k,l}(t) \sim \mathcal{CN}(0,1)$.

3 Problem Statement

Considering the channel variation, we aim to solve the following instantaneous achievable sum-rate maximization problem at the time slot t:

$$\begin{aligned} &\max_{\boldsymbol{w}_{n,k}(t)} R_{\text{sum}}(t) = \sum_{n=1}^{N} \sum_{k=1}^{K} R_{n,k}(t) \\ &\text{s.t.} \sum_{k=1}^{K} \left\| \boldsymbol{w}_{n,k}(t) \right\|^2 \leqslant P_{\max}, \forall n, \end{aligned} \tag{7}$$

where $P_{\max}$ denotes the maximum transmit power for each BS. Unfortunately, Problem (7) is generally NP-hard even with global CSI, and finding its globally optimal solution requires exponential running time[3]. Conventionally, several centralized methods are proposed to find a sub-optimal solution. All centralized algorithms assume that there is a central node to collect global CSI from all BSs, and then the central node computes and returns beamformers of all BSs. However, it is hard to obtain the global CSI for all BSs. Moreover, due to the dynamics of channels, the beamformers are already outdated when the BSs obtain the returns. Therefore, it is more reasonable to apply a distributed approach. However, information sharing design between the BSs is also a problem for the distributed methods. Generally, the BSs communicate with other BSs through the backhaul links. Conventional beamforming methods need the BSs to exchange global or cross-talk CSI, which is an unacceptable burden for the rate-limited backhaul links. Therefore, the amount of shared information for beamforming should be limited, and we try to seek a sub-optimal distributed solution with limited information exchange between the BSs in different cells.

From the perspective of the BS n, the beamformer $\boldsymbol{w}_{n,k}$ can be expressed as:

$$\boldsymbol{w}_{n,k}(t) = \sqrt{P_{n,k}(t)}\, \overline{\boldsymbol{w}}_{n,k}(t), \tag{8}$$

where $P_{n,k}(t) = \left\| \boldsymbol{w}_{n,k}(t) \right\|^2$ denotes the transmit power of the BS n to user k and $\overline{\boldsymbol{w}}_{n,k}(t)$ denotes the corresponding normalized beamformer, which represents the direction of the transmit beam. Note that once the beam direction is fixed, the beam power allocation only needs the equivalent channel and interference information, which significantly reduces the cost of the information exchange[3].

The typical beam direction solutions include the virtual SINR[12] and the weighted minimum-mean-square-error (WMMSE)[13]. However, these solutions are closely coupled with power allocation strategies, which cannot be easily adopted to guide the beam direction design. According to Ref. [14], given global CSI in the multi-cell scenario, the optimal beamformer can be expressed as a linear combination of the conventional zero-forcing (ZF) and maximum ratio transmission (MRT). However, it is difficult to obtain the instantaneous global CSI. This inspires us to apply the available ZF and MRT to give heuristic solutions to our proposed approach based on only local CSI[5]. Specifically, the ZF and the MRT solutions are given by:

1. We assume the URA model here for simplicity. Nevertheless, the proposed scheme can be applicable to arbitrary array geometry.

$$\underline{\boldsymbol{w}}_{n,k}^{\mathrm{ZF}} = \frac{(\boldsymbol{H}_n^{\mathrm{H}}(\boldsymbol{H}_n\boldsymbol{H}_n^{\mathrm{H}})^{-1})_{[:,k]}^{\mathrm{T}}}{\|(\boldsymbol{H}_n^{\mathrm{H}}(\boldsymbol{H}_n\boldsymbol{H}_n^{\mathrm{H}})^{-1})_{[:,k]}^{\mathrm{T}}\|}, \tag{9a}$$

$$\underline{\boldsymbol{w}}_{n,k}^{\mathrm{MRT}} = \frac{\boldsymbol{h}_{n,n,k}^{*}}{\|\boldsymbol{h}_{n,n,k}\|}, \tag{9b}$$

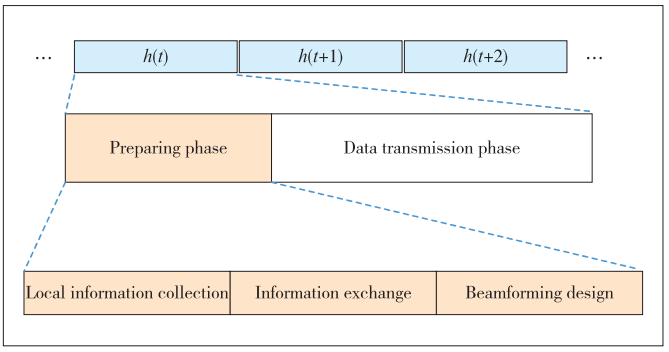
where $\boldsymbol{H}_n \in \mathbb{C}^{K\times M}$ denotes the downlink channel of all K users in the n-th cell. Note that the MRT works well at low SNR regions[15], especially in the case that most UE is at the edge of the cell, since it only focuses on the maximization of the received signal power. In contrast, ZF tries to minimize the received interference for the UE, which makes it outperform the MRT at high SNR regions where it is dominated by intra-cell interference. Therefore, we introduce the DRLbased method to choose an appropriate approach according to the dynamic wireless communication environment, which can be viewed as a typical decision-making problem. On the other hand, the DRL-based approaches, e. g., deep Q-learning[17], have been introduced to solve the power allocation task. However, the conventional deep Q-learning approach can only output discrete power levels, which may make training intractable with the increase of the action dimension. This motivates us to apply the deep deterministic policy gradient (DDPG) approach, which will be introduced in the following section, to tackle the challenging beam direction and power allocation tasks for each BS.

4 Proposed Limited Information Exchange Protocol

In principle, all the BSs share information through the backhaul links between BSs. However, it is an unaffordable burden for the backhaul links to transmit the global CSI among all BSs, especially when the BSs are equipped with large-scale antennas. Therefore, we develop a limited information exchange protocol, in which BSs only need to share a small amount of equivalent channel gain and interference information rather than the global CSI.

Assuming a flat and block-fading downlink channel, we propose a framework for the downlink data transmission process as shown in Fig. 1. In this framework, the channels are invariant during one time slot. Each time slot is divided into two phases. The first phase is a preparation phase for the BSs to collect local information, information exchange and beamforming design. The second phase is the downlink data transmission phase. Conventionally, the BSs only estimate downlink channels in the local information collection phase. To be specific, the BSs send reference symbols to UE first, then the UE estimates the downlink channel according to the reference symbols, and finally give the local CSI back to the corresponding BSs.

In our proposed protocol, in the local information collection phase, the UE needs to give back not only the local CSI but also the received interference from the other BSs. Let us take the UE k in cell n as an example. The BSs need to send orthogonal reference symbols to UE k, so that UE k can estimate the downlink local CSI $\boldsymbol{h}_{n,n,k}(t)$ and the received interference $c_{i,n,k}(t-1) = \sum_{j=1}^{K}|\boldsymbol{h}_{i,n,k}^{\mathrm{T}}(t)\boldsymbol{w}_{i,j}(t-1)|^2, \forall i \in N, i \neq n$ from the other BSs before the BSs update their beamformers.

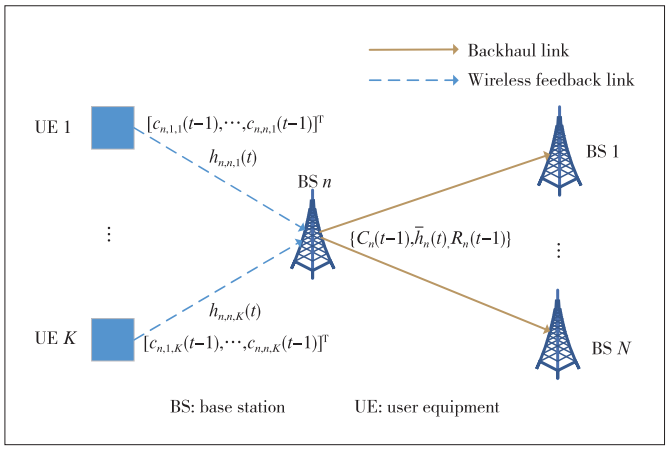


▲ **Figure 1. Framework of the designed downlink data transmission process**

During the information exchange phase, the BSs first calculate the equivalent channel gain of each UE based on the local CSI and the previous beamformer. Meanwhile, the achievable rate of each UE can also be obtained according to Eq. (2b). Then the BSs concatenate the equivalent channel gains, the achievable sum rate of the served UE, and the interference information together, and then send them to the other BSs. Fig. 2 shows the information exchange process of the BS n. In cell n, the BS n collects the feedback information from all UE and calculates the equivalent channel gain of UE as $\bar{\boldsymbol{h}}_{n,k}(t) = |\boldsymbol{h}_{n,n,k}^{\mathrm{T}}(t)\boldsymbol{w}_{n,k}(t-1)|$. Besides, the BS n computes the achievable rate of each UE according to Eq. (2b) and obtains the sum rate $R_n(t-1)$ of UE in the cell n at time slot t-1. Then the BS n concatenates these information as the set $\{\boldsymbol{C}_n(t-1), \bar{\boldsymbol{h}}_n(t), R_n(t-1)\}$, where $\boldsymbol{C}_n(t-1) \in \mathbb{R}^{K\times(N-1)}$ is a matrix formed by concatenating the interference vectors of all UE in cell n and $\bar{\boldsymbol{h}}_n \in \mathbb{R}^K$ is a column vector composed of the equivalent channel of all UE in cell n. Note that in this information protocol, the BSs do not need to share the global or cross-talk CSI and the amount of exchanged information is only related to the number of cells and UE. Although other information exchange protocols try to further cut down the cost of information shared by the only exchange between adjacent cells[7-8], the sum-rate performance cannot be guaranteed when the interference generated by nonadjacent cells becomes nonnegligible. Therefore, we design the BSs to exchange information with all the other BSs.

5 MADDPG-Based Approach for Distributed Multi-Cell Multi-User MISO Beamforming

In this section, we introduce a DTDE MADDPG-based scheme for the MISO-IC system, as illustrated in Fig. 3, where each BS acts as a trainable agent. In the following, we take BS n as an example to elaborate on the online deci-



▲ **Figure 2. Illustration of information exchange process for the BS *n***

sion and offline training processes in detail.

5.1 Online Decision Process

In the online decision process, BS n observes the states from the wireless communication environment and takes actions based on the online policy network.

At the time slot t, the BS n observes the wireless communication environment and collects the state vector $\boldsymbol{s}_n(t)$. To be specific, during the online decision process in the DRL method at the time slot t, BSs firstly collect the information from UE and exchange information with each other according to the proposed information exchange protocol. With the received information from other BSs, the BS n can form the state vector $\boldsymbol{s}_n(t)$. The action $\boldsymbol{a}_n(t)$ is taken by the online policy network based on the observed state. Note that all the distributed agents take actions simultaneously, which means that none of them has instantaneous information about other BSs. To make the DDPG fully explore the action space, the output of the online policy network is added with action noise $\boldsymbol{n}_a \in \mathcal{N}\left(0,\sigma_a^2\right)$. With the training process moving on, the action noise decreases to zero gradually. With the action vector $\boldsymbol{a}_n(t)$ decided, the beamformers $\{\boldsymbol{w}_{n,k}\}$ can be formed and utilized for downlink data transmission. The reward $r(t)$ and the next state vector $\boldsymbol{s}_n(t+1)$ can be obtained in the next time slot $t+1$ through the proposed information exchange protocol. Meanwhile, the transition $\{\boldsymbol{s}_n(t), \boldsymbol{a}_n(t), r(t), \boldsymbol{s}_n(t+1)\}$ is stored in the memory replay buffer. The action vector $\boldsymbol{a}_n(t)$ is designed as

$$\boldsymbol{a}_n(t) = [\boldsymbol{p}_n^{\mathrm{T}}(t), P_{n,\mathrm{sum}}(t), D_n(t)]^{\mathrm{T}}. \tag{10}$$

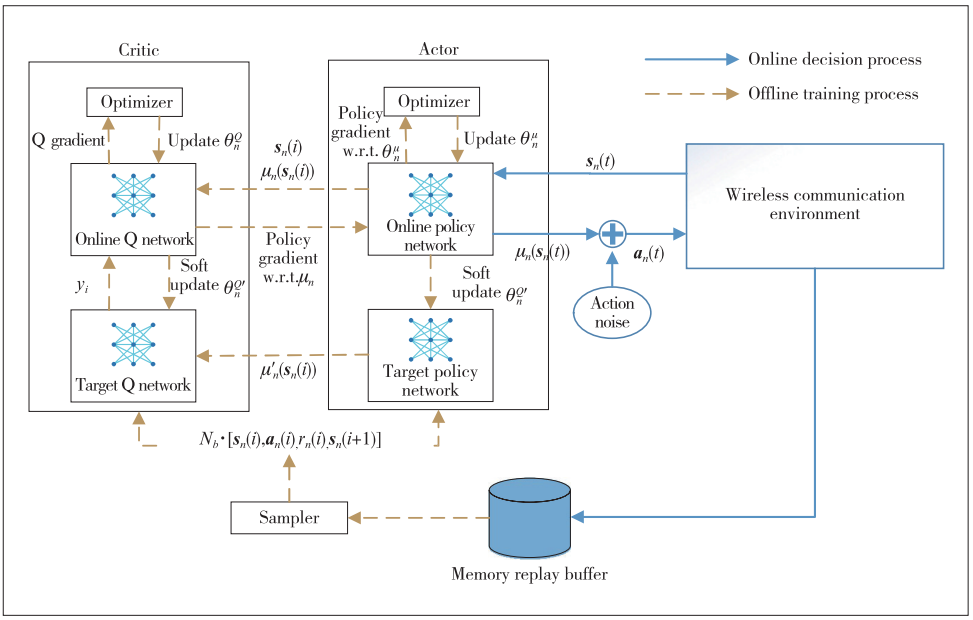
In the action vector $\boldsymbol{a}_n(t)$, $\boldsymbol{p}_n \in \mathbb{R}^K$, $\sum_{k=1}^{K} p_{n,k} = 1$ denotes the normalized allocated power levels for UE and $P_{n,\mathrm{sum}} \in (0,1]$ denotes the normalized total transmit power of the cell n. Then the real transmit power for user k can be expressed as $P_{n,k}(t) = P_{\max} P_{n,\mathrm{sum}}(t) p_{n,k}(t)$. $D_n \in \{0,1\}$ is a Boolean value that denotes the selected beam direction solution in Eq. (8). When D_n=0, the BS n chooses ZF as the beam direction solution; when $D_n = 1$, the BS n chooses MRT. With the selected beam direction $D_n(t)$ and power strategy $P_{n,k}(t)$, the beamformer for UE k becomes

$$\boldsymbol{w}_{n,k}(t) = \sqrt{P_{n,k}(t)}\, \bar{\boldsymbol{w}}_{n,k}^{D_n(t)}(t). \tag{11}$$

The state vector $\boldsymbol{s}_n(t)$ is given by

$$\boldsymbol{s}_n(t) = \left[\mathrm{vec}\left(\overline{\boldsymbol{H}}(t)\right), \mathrm{vec}\left(\overline{\boldsymbol{C}}_n(t-1)\right)\right], \tag{12}$$

where $\overline{\boldsymbol{H}}(t) \in \mathbb{R}^{N\times K}$ denotes the equivalent channel gain of all UE, $\overline{\boldsymbol{H}}(t)_{[i,j]} = \left|\boldsymbol{h}_{i,i,j}^{\mathrm{T}}(t)\boldsymbol{w}_{i,j}(t-1)\right|$; $\overline{\boldsymbol{C}}_n(t-1) \in \mathbb{R}^{(N-1)\times K}$ denotes generated interference from cell n to the UE in the other cells, and $\overline{\boldsymbol{C}}_n(t-1)_{[i,j]} = \sum_{k=1}^{K}\left|\boldsymbol{h}_{n,i,j}^{\mathrm{T}}(t-1)\boldsymbol{w}_{n,k}(t-1)\right|$. For convenience, we use vec(·) to convert the matrix into a row vector by concatenating its rows. Note that all the elements in the state vector $\boldsymbol{s}_n(t)$ can be obtained through the above proposed information exchange protocol . The equivalent channel gain $\overline{\boldsymbol{H}}(t)$ contains the knowledge of receiving signal power of all UE and the generated interference $\overline{\boldsymbol{C}}_n(t-1)$ can lead the agent n to adjust actions to reduce the inter-cell interference to other cells. Since our goal is to maximize the achievable



▲ **Figure 3. Illustration of the MADDPG-based scheme for multi-cell multi-user multiple-input single-output interference channel (MISO-IC) system**

sum rate, we thus set the reward $r(t)=R_{\text{sum}}(t-1)$, which can be calculated based on the shared local information according to the limited information exchange protocol in Section 4.

5.2 Offline Training Process

In the offline training process, the sampler first randomly samples a batch of transition data $\{\boldsymbol{s}_n(i), \boldsymbol{a}_n(i), r(i), \boldsymbol{s}_n(i+1)\}$ from the memory replay buffer for training. By inputting the training transition i into the two target networks, the output of the target Q-network y_i can be expressed as:

$$y_i = r(i) + \eta Q_n'\left(\mathbf{s}_n(i+1), \mu_n'\left(\mathbf{s}_n(i+1)|\theta_n'\right)|\theta_n^{Q'}\right), \tag{13}$$

where η denotes the discount factor, and $\theta_n^{\mu'}$ and $\theta_n^{Q'}$ represent the network parameters of the target policy network μ' and Q-network Q', respectively. The Q-value is defined as the expectation of the future reward that can be obtained from the given state-action pair $\{\mathbf{s}_n(i),\mathbf{a}_n(i)\}$ when applying the strategy μ[18-19]. The Bellman equation of the Q-value can be expressed as:

$$Q^{\mu}(\mathbf{s}(i),\mathbf{a}(i)) = \mathbb{E}\left[r(i) + \eta Q^{\mu}(\mathbf{s}(i+1),\mathbf{a}(i+1))\right], \tag{14}$$

where the Q-value of the state-action pair$\{\mathbf{s}_n(i), \mathbf{a}_n(i)\}$ is composed of an instantaneous reward $r(i)$ and the Q-value of the next state-action pair$\{\mathbf{s}_n(i+1), \mathbf{a}_n(i+1)\}$. Note that the output of the target Q-network y_i is actually the estimated Q-value of the state-action pair $\{\mathbf{s}_n(i),\mathbf{a}_n(i)\}$.

According to the deterministic policy gradient theorem[19], the gradients of the online Q-network and policy network are:

$$\nabla_{\theta_n^Q} = \frac{1}{N_b}\frac{\left[\partial\sum_{i=1}^{N_b}\left(y_i - Q_n\left(\mathbf{s}_n(i),\boldsymbol{a}_n(i)|\theta_n^Q\right)\right)^2\right]}{\partial\theta_n^Q}, \tag{15a}$$

$$\nabla_{\theta_n^{\mu}} = \frac{1}{N_b}\sum_{i=1}^{N_b}\left[\nabla_a Q_n\left(\mathbf{s}_n(i),\boldsymbol{a}_n(i)\right)\nabla_{\theta}\mu_{\theta}\left(\mathbf{s}_n(i)\right)\right], \tag{15b}$$

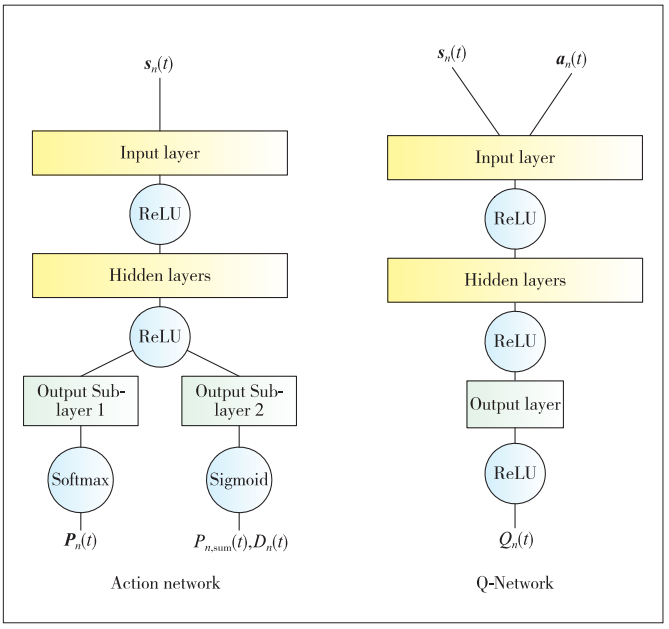
where N_b is the batch size of the sampled training data. The parameters in the online networks are updated by the optimizer. For the target networks, the parameters are softly updated as

$$\theta_n^{Q'} \leftarrow \tau\theta_n^Q + (1-\tau)\theta_n^{Q'}, \tag{16a}$$

$$\theta_n^{\mu'} \leftarrow \tau\theta_n^{\mu} + (1-\tau)\theta_n^{\mu'}, \tag{16b}$$

where $\tau \in (0,1)$ is the soft update factor.

The basic structures of the Q and policy networks, as shown in Fig. 4, are similar, which both include the fully connected input layer, hidden layers and the output layer. To reduce the computational complexity, we design two hidden layers for the Q and policy networks. The number of neurons in the input layer is the same as the dimension of the input vector. Hence, the scale of the input layer in the policy network is the same as the length of the input vector $\boldsymbol{s}_n(t)$. On one hand, the input vector for the Q-network is the concatenating of $\boldsymbol{s}_n(t)$ and $\boldsymbol{\mu}_n(t)$. We apply ReLU as the activation function due to its simplicity. Note that the output layer of the policy network consists of two sub-layers that apply the softmax and sigmoid activation function for $\boldsymbol{p}_n(t)$ and $[P_{\text{n,sum}}(t), D_n(t)]$, respectively. On the other hand, the output of the Q-network is a real value denoting the Q-value of the corresponding state-action pair.



▲ **Figure 4. Structures of the action and Q-networks**

For clarification, we summarize the overall procedure for distributed multi-cell multi-user beamforming in Algorithm 1, referred to as the MADDPG algorithm. The proposed MADDPG algorithm requires the perfect CSI resulting from the proposed information exchange protocol. However, imperfect CSI may lead to the shifting of the objective function in Eq. (7), resulting in significant performance degradation of the current approach. A possible solution to the imperfect CSI is redesigning the reward function based on appropriate historical information, which will be addressed in our future work.

Algorithm 1: MADDPG Algorithm

1: Randomly initialize the weights of critic θ^Q and actor θ^{μ} for all agents.
2: Initialize the weights of target networks as $\theta^{Q'} \leftarrow \theta^Q$, $\theta^{\mu'} \leftarrow \theta^{\mu}$ for all agents.
3: Initialize replay memory buffer for all agents.
4: **repeat**
5: Agent n observes the state $\boldsymbol{s}_n(t)$ in time slot t, $\forall n \in \boldsymbol{N}$.
6: Agent n selects an action $\boldsymbol{a}_n(t) = \boldsymbol{\mu}\left(\boldsymbol{s}_n(t)|\theta^{\mu}\right) + \boldsymbol{n}_a$ accord-

ing to the current policy network output and exploration noise, $\forall n \in \boldsymbol{N}$.
7: Agent n takes an action $\boldsymbol{a}_n(t)$, obtains a reward $r(t)$ and observe a new state $\boldsymbol{s}_n(t+1), \forall n \in \boldsymbol{N}$.
8: Agent n stores the new transition $\{\boldsymbol{s}_n(t), \boldsymbol{a}_n(t), r(t), \boldsymbol{s}_n(t+1)\}$ into memory buffer, $\forall n \in \boldsymbol{N}$.
9: Agent n samples a random batch of N_b transitions $\{\boldsymbol{s}_n(i), \boldsymbol{a}_n(i), r(i), \boldsymbol{s}_n(i+1)\}$ from memory buffer, $\forall n \in \boldsymbol{N}$.
10: Agent n calculates y_i according to Eq. (12), $\forall n \in \boldsymbol{N}$.
11: Agent n updates the online critic network θ_n^Q according to Eq. (14a), $\forall n \in \boldsymbol{N}$.
12: Agent n updates online actor network θ_n^μ according to Eq. (14b), $\forall n \in \boldsymbol{N}$.
13: Agent n updates target networks according to Eqs. (15a) and (15b), respectively, $\forall n \in \boldsymbol{N}$.
14: **until** a termination criterion is reached
15: **End**

5.3 Information Exchange Analysis

We list the required information and the information exchange of different schemes in Table 1. Note that the fractional programming[3] (FP) and the zero-gradient[6] (ZG) need to exchange much more instantaneous CSI than that of MADDPG while the MADDPG only needs to exchange real values of previous information of the wireless environment. Moreover, thanks to the local CSI beam direction design, our proposed MADDPG based scheme does not rely on the number of antennas M and requires much less information exchange than those of FP and ZG, and is therefore suitable for the case of a large number of antennas.

5.4 Computational Complexity Analysis

The computational complexity of the proposed MADDPG algorithm mainly comes from the network computation and the beamformer formation. In Algorithm 1, the agent n firstly initializes the weights of the networks. We denote the number of hidden layers as L_H and the number of neurons in each hidden layer as N_H, and the complexity of the network initialization is $\mathcal{O}(L_H \mathrm{N}_H)$. In the repeat steps, we assume the number of repetitions as N_r, the complexity of Step 6 can be expressed as $\mathcal{O}(NKH + L_H N_H^2)$, which consists of the linear multiplication in hidden layers. In Step 7, the agent n needs to compute the normalized beamformers according to Eqs. (9a) and (9b). The complexity of ZF and MRT is $\mathcal{O}(M^3)$ and $\mathcal{O}(MK)$ and ZF has higher complexity due to matrix inversion operations. Then in Step 10, the target networks need to calculate y_i for each sample I and the complexity of Step 10 is $\mathcal{O}(N_b NKH + N_b L_H N_H^2)$. For the parameter update in Steps 11 – 13, the complexity is also $\mathcal{O}(N_b NKH + N_b L_H N_H^2)$ according to the error back propagation algorithm. Hence, the total computational complexity of the whole MADDPG algorithm, including the online decision and offline training processes, is given as $\mathcal{O}(N_r(N_b NKH + N_b L_H N_H^2 + M^3))$.

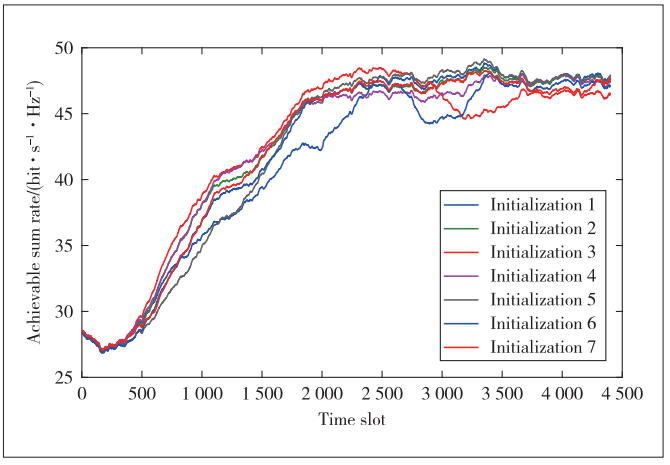
5.5 Convergence Discussion

The convergence behavior of the DRL algorithm, including the proposed MADDPG algorithm, depends on many factors such as the dynamics of the environment, the power of action noise σ_a^2 and the size of the memory replay buffer N_b. Up to now, the theoretical convergence analysis of the the DRL based algorithm is still an open problem and is generally based on empirical attempt. For example, when the action noise σ_a^2 is small, the MADDPG algorithm can converge faster. However, the performance of the MADDPG algorithm will degrade since the agents cannot explore the whole action space. Therefore, we need a large number of simulations to choose appropriate network hyper-parameters for achieving fast convergence and good performance.

To test the convergence behavior of the proposed MADDPG approach, we give an experimental result in Fig. 5, which illustrates the achievable sum rate versus the time slot under different initializations of network weights. The simulation settings are the same as that of Fig. 6 in Section 6. There are 7 simulation curves with different initial network weights in the same environment and all weights are randomly initialized following the standard Gaussian distribution. The simulation result shows that the different network initialization will basically converge to a similar performance around 4 000 time slots. This indicates that the proposed MADDPG method is insensitive to different network initialization.

6 Simulation Results

This section conducts numerical experiments to corroborate the performance of the proposed MADDPG algorithm in a wireless cellular system with (N, K)=(19, 4) and (M_x, M_y)=(8, 4). The distance between the centers of each hexagonal cell is 500 m

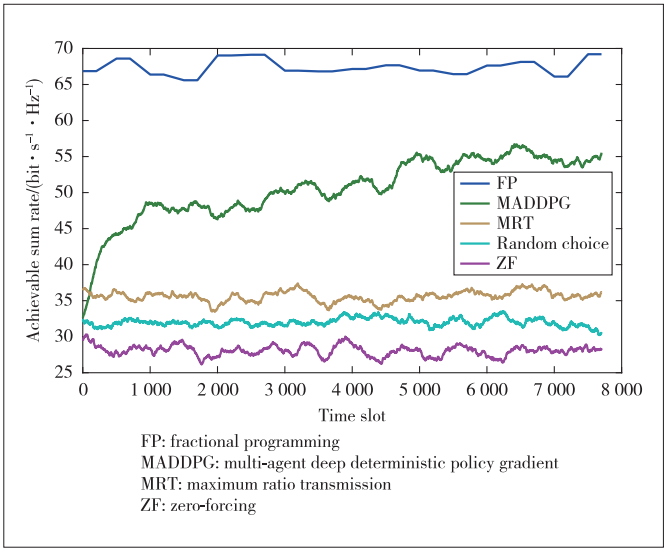


▲ **Figure 5. Convergence behavior of the proposed multi-agent deep deterministic policy gradient (MADDPG) algorithm under different initialization of network weights**

▼**Table 1. Comparison of the information exchange**

Schemes	Required Information	Information Exchange
MADDPG	$\overline{\mathbf{H}}(t),\overline{\mathbf{C}}_n(t-1),R(t-1)$	$\mathcal{O}(NK)$
FP[3]	$\boldsymbol{h}_{i,j,k}(t),\forall i,j,k$	$\mathcal{O}(MNK)$
ZG[6]	$\boldsymbol{h}_{i,j,k}(t),\forall j,k$ for the BS i	$\mathcal{O}(MNK)$
MRT/ZF[5]	$\boldsymbol{h}_{i,i,k}(t),\forall k$	0

FP: fractional programming MADDPG: multi-agent deep deterministic policy gradient
MRT: maximum ratio transmission ZF: zero-forcing
ZG: zero-gradient



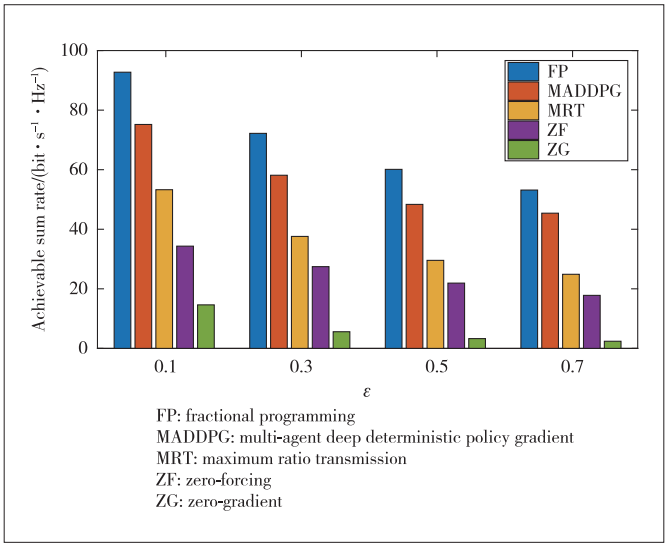
▲**Figure 6. Average achievable rate of various schemes versus the number of time slots, where each point is a moving average over the previous 300-time slots with the UE distribution factor ϵ= 0.3**

and the radius of each cell is r_{cell}=290 m. The first cell is located at the center, cells 2 – 7 are located at the first tier, and cells 8 – 19 are located in the second tier. We only count the achievable rates of cells 1 – 7 since the cells at the second tier suffer no interference from the outer cells. We define an inner region with radius r_{inner} where active UE does not exist. We define the UE distribution factor as $\epsilon = r_{\text{inner}}/r_{\text{cell}}$, where the factor ϵ determines how far the UE is from the BS. The received noise power σ_n^2 is set to 10^{-4} mW. The carrier frequency is f_c = 3.5 GHz. The large-scale fading factor is set as κ = 28+22 lg dis_{3D}+20 lg f_c/dB, where dis_{3D} is the 3D distance between the UE and the BS. The total number of multipath L is 5 and the angular perturbation of each path Δ is 5°. The maximum transmit power of the BSs $P_{\max}$ and the time correlation coefficient ρ are set to 10^5 mW and 0.8, respectively. The action noise is initialized as σ_a^2 = 1.

The MADDPG scheme is deployed with the PyTorch framework and the hyper-parameters are set as follows. Both policy and Q-network parameters are designed as L_H = 2 fully-connected hidden layers with N_H = 200 neurons. The discount factor η is set to 0.6 and the soft update factor τ is equal to 0.01. The size of the memory replay buffer is set to 2 000 and the size of the sampled batch N_b is set to 64. Furthermore, we choose the Adam optimizer to update parameters with the learning rate being 10^{-3}.

Fig. 6 depicts the average achievable rate of various schemes versus the number of time slots. A random choice scheme means that each agent takes a random action in each time slot. For the ZF and MRT[5], the power allocation strategy is $P_{n,k} = P_{\max}\left\|\boldsymbol{h}_{n,k}\right\|^2 / \sum_i \left\|\boldsymbol{h}_{n,i}\right\|^2$. ZF and MRT exhibit the worst performance due to no extra information of the whole wireless environment. We see that the MADDPG based scheme learns to gradually improve the achievable sum rate of the system with the training process, as each agent updates the policy network to learn a better action policy for the system sum-rate maximization. The MADDPG converges to a fairly stable situation in 7 000 time slots and the variance is reasonable since the channels are dynamic. The MADDPG can achieve approximately 85% of the sum-rate performance of the FP algorithm, by using local CSI and limited information exchange only. It is worth noting that although the centralized FP algorithm has the largest achievable sum rate, it has a very high computational cost so we have to simulate the FP scheme every 500 time slots. Besides, FP[3] needs a large amount of instantaneous global CSI, which is unattainable in practical systems.

In Fig. 7, we evaluate the average achievable rate of different schemes vs the UE distribution factor. As the UE distribution factor increases, the average received power of UE can be reduced and the inter-cell interference problem becomes worse. The ZG algorithm, which is derived under high SINR assumption, has the worst performance under the 19 cells scenarios. The FP algorithm with global instantaneous CSI has undoubtedly the best performance in all scenarios. While as the users are getting closer to the cell edge, the performance gap between the FP and our proposed MADDPG is shrinking.



▲**Figure 7. Average achievable rate of various schemes versus the UE distribution factor ϵ**

7 Conclusions

In this paper, we reflect on the instantaneous sum rate maximization problem in the multi-cell MISO interference channel scenario. We propose a MADDPG scheme, in which each BS learns to choose an appropriate beam direction solution and allocate power based on the local CSI and limited exchange information among the BSs. The simulation results show that the proposed MADDPG scheme can achieve a relatively high sum rate with much less information exchange than the conventional centralized and distributed solutions.

References

[1] SOMEKH O, SIMEONE O, BAR-NESS Y, et al. Cooperative multicell zero-forcing beamforming in cellular downlink channels [J]. IEEE transactions on information theory, 2009, 55(7): 3206 – 3219. DOI: 10.1109/TIT.2009.2021371
[2] HUANG Y M, ZHENG G, BENGTSSON M, et al. Distributed multicell beamforming with limited intercell coordination [J]. IEEE transactions on signal processing, 2011, 59(2): 728 – 738. DOI: 10.1109/TSP.2010.2089621
[3] SHEN K M, YU W. Fractional programming for communication systems—part I: power control and beamforming [J]. IEEE transactions on signal processing, 2018, 66(10): 2616 – 2630. DOI: 10.1109/TSP.2018.2812733
[4] ZHANG R, CUI S G. Cooperative interference management with MISO beamforming [J]. IEEE transactions on signal processing, 2010, 58(10): 5450 – 5458. DOI: 10.1109/TSP.2010.2056685
[5] BJÖRNSON E, ZAKHOUR R, GESBERT D, et al. Cooperative multicell precoding: rate region characterization and distributed strategies with instantaneous and statistical CSI [J]. IEEE transactions on signal processing, 2010, 58(8): 4298 – 4310. DOI: 10.1109/TSP.2010.2049996
[6] PARK S H, PARK H, LEE I. Distributed beamforming techniques for weighted sum-rate maximization in MISO interference channels [J]. IEEE communications letters, 2010, 14(12): 1131 – 1133. DOI: 10.1109/LCOMM.2010.12.101635
[7] GE J G, LIANG Y C, JOUNG J, et al. Deep reinforcement learning for distributed dynamic MISO downlink-beamforming coordination [J]. IEEE transactions on communications, 2020, 68(10): 6070 – 6085. DOI: 10.1109/TCOMM.2020.3004524
[8] KHAN A A, ADVE R S. Centralized and distributed deep reinforcement learning methods for downlink sum-rate optimization [J]. IEEE transactions on wireless communications, 2020, 19(12): 8410 – 8426. DOI: 10.1109/TWC.2020.3022705
[9] INDYK P, MOTWANI R. Approximate nearest neighbors: towards removing the curse of dimensionality [C]//The Thirtieth Annual ACM Symposium on Theory of Computing. STOC, 1998: 604 – 613
[10] YING D W, VOOK F W, THOMAS T A, et al. Kronecker product correlation model and limited feedback codebook design in a 3D channel model [C]//Proceedings of 2014 IEEE International Conference on Communications. IEEE, 2014: 5865 – 5870. DOI: 10.1109/ICC.2014.6884258
[11] DONG M, TONG L, SADLER B M. Optimal insertion of pilot symbols for transmissions over time-varying flat fading channels [J]. IEEE transactions on signal processing, 2004, 52(5): 1403 – 1418. DOI: 10.1109/TSP.2004.826182
[12] SCHUBERT M, BOCHE H. Solution of the multiuser downlink beamforming problem with individual SINR constraints [J]. IEEE transactions on vehicular technology, 2004, 53(1): 18 – 28. DOI: 10.1109/TVT.2003.819629
[13] CHRISTENSEN S S, AGARWAL R, DE CARVALHO E, et al. Weighted sum-rate maximization using weighted MMSE for MIMO-BC beamforming design [J]. IEEE transactions on wireless communications, 2008, 7(12): 4792 – 4799. DOI: 10.1109/T-WC.2008.070851
[14] JORSWIECK E A, LARSSON E G, DANEV D. Complete characterization of the Pareto boundary for the MISO interference channel [J]. IEEE transactions on signal processing, 2008, 56(10): 5292 – 5296. DOI: 10.1109/TSP.2008.928095
[15] LIM Y G, CHAE C B, CAIRE G. Performance analysis of massive MIMO for cell-boundary users [J]. IEEE transactions on wireless communications, 2015, 14(12): 6827 – 6842. DOI: 10.1109/TWC.2015.2460751
[16] MENG F, CHEN P, WU L N, et al. Power allocation in multi-user cellular networks: deep reinforcement learning approaches [J]. IEEE transactions on wireless communications, 2020, 19(10): 6255 – 6267. DOI: 10.1109/TWC.2020.3001736
[17] HESTER T, VECERIK M, PIETQUIN O, et al. Deep Q-learning from demonstrations [EB/OL]. [2022-02-02]. https://arxiv. org/abs/1704.03732. DOI: 10.1609/aaai.v32i1.11757
[18] DONG S K, CHEN J R, LIU Y, et al. Reinforcement learning from algorithm model to industry innovation : a foundation stone of future artificial intelligence [J]. ZTE communications, 2019, 17(3): 31 – 41. DOI: 10.12142/ZTECOM.201903006
[19] SILVER D, LEVER G, HEESS N, et al. Deterministic policy gradient algorithms [C]//Proceeding of International Conference on Machine Learning. ICML, 2014: 387 – 395

Biographies

JIA Haonan received his BS and MS degrees in communication engineering from the University of Electronic Science and Technology of China, in 2019 and 2022, respectively. His research interests focus on deep learning with application to wireless communications.

HE Zhenqing (zhenqinghe@uestc.edu.cn) received his PhD degree in communication and information system from the University of Electronic Science and Technology of China (UESTC) in 2017. Since 2018, he has been with the National Key Laboratory of Science and Technology on Communications, UESTC, where he is currently an associate professor. His main research interests include statistical signal processing, wireless communications, and machine learning. He was a recipient of the IEEE Communications Society Heinrich Hertz Prize Paper Award in 2022.

TAN Wanlong received his BS degree in communication engineering from Jilin University, China in 2020. He is currently pursuing his MS degree in communication engineering with the University of Electronic Science and Technology of China. His research interests include wireless communications and reconfigurable intelligent surface.

RUI Hua received his BS, MS and PhD degrees from Nanjing University of Aeronautics and Astronautics, China in 1999, 2002, and 2005, respectively. He currently works as a senior pre-research expert and the head of the 6G Future Wireless Lab in ZTE Corporation. He has been engaged in wireless communication product and new technology pre-research, including 3G/4G/WIFI/5G/6G network architecture and key technologies. His main research direction is the 6G wireless communication technology. He has published more than 20 invention patents and papers in related fields. He has been engaged in more than 10 industry technical standards and white papers including 3GPP 3G/4G/5G series standards and IEEE 802.11 series standards.

LIN Wei received her BS and MS degrees in communication and information system from Northwestern Polytechnical University, China in 2002 and 2005 respectively. At present, she works in ZTE Corporation as a senior algorithm engineer in the Algorithm Department. Her research interests include 6G wireless communication physical layer technology and wireless AI technology. She has applied for more than 20 invention patents in related fields.

Predictive Scheme for Mixed Transmission in Time-Sensitive Networking

LI Zonghui[1], YANG Siqi[1], YU Jinghai[2], HE Fei[3], SHI Qingjiang[4,5]

(1. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China;
2. ZTE Corporation, Shenzhen 518057, China;
3. School of Software, Tsinghua University, Beijing 100084, China;
4. School of Software Engineering, Tongji University, Shanghai 201804, China;
5. Shenzhen Research Institute of Big Data, Shenzhen 518172, China)

DOI: 10.12142/ZTECOM.202204010

https: //kns.cnki.net/kcms/detail/34.1294.TN.20221028.0858.002.html, published online October 28, 2022

Manuscript received: 2022-01-04

Abstract: Time-sensitive networking (TSN) is an important research area for updating the infrastructure of industrial Internet of Things. As a product of the integration of the operation technology (OT) and the information technology (IT), it meets the real-time and deterministic nature of industrial control and is compatible with Ethernet to support the mixed transmission of industrial control data and Ethernet data. This paper systematically summarizes and analyzes the shortcomings of the current mixed transmission technologies of the bursty flows and the periodic flows. To conquer these shortages, we propose a predictive mixed-transmission scheme of the bursty flows and the periodic flows. The core idea is to use the predictability of time-triggered transmission of TSN to further reduce bandwidth loss of the previous mixed-transmission methods. This paper formalizes the probabilistic model of the predictive mixed transmission mechanism and proves that the proposed mechanism can effectively reduce the loss of bandwidth. Finally, based on the formalized probabilistic model, we simulate the bandwidth loss of the proposed mechanism. The results demonstrate that compared with the previous mixed-transmission method, the bandwidth loss of the proposed mechanism achieves a 79.48% reduction on average.

Keywords: time-sensitive networking; 802.1Qbv; 802.1Qbu; guard band strategy; preemption strategy

Citation (IEEE Format): Z. H. Li, S. Q. Yang, J. H. Yu, et al., "Predictive scheme for mixed transmission in time-sensitive networking," *ZTE Communications*, vol. 20, no. 4, pp. 78 – 88, Dec. 2022. doi: 10.12142/ZTECOM.202204010.

1 Introduction

At present, the vigorous development of artificial intelligence and the industrial Internet of Things (IoT) presents new requirements and challenges for traditional industrial control networks[1], for example, high-bandwidth and highly reliable transmission to support comprehensive IoT sensing and breaking the barriers between information technology (IT) networks and operation technology (OT) networks to realize the integration and real-time linkage of IT and OT. However, traditional industrial control networks widely use bus-type networks, such as the controller area network (CAN)[2] in the field of automotive and numerical control machine tools and Multifunction Vehicle Bus (MVB)[3] in the field of rail transportation. Their low transmission bandwidth is not conducive to the access of more and more sensor nodes, which affects the efficiency of data transmission and seriously restricts the development of industrial IoT. Industrial Ethernet as an alternative to bus-based networks, has a wide range of standards[4]. The real-time and deterministic mechanisms adopted by different industrial Ethernet standards are different from each other, which makes it hard to achieve connectivity between them. To solve the low bandwidth of the bus-based networks and the poor compatibility of existing industrial Ethernet standards, IEEE 802.1 initiated the establishment of time-sensitive networking (TSN)[5] working group in November 2012, responsible for extending the standard Ethernet Net 802.3 to support the real-time and deterministic data transmission of industrial control and realize the integration of IT and OT.

According to different requirements, the TSN divides flows into three categories: first, periodic flows, mainly used in industrial control to meet the real-time and deterministic requirements of industrial applications; second, bursty real-time flows, mainly used for bursty services that have certain delay

This research is sponsored in part by the National Key Research and Development Project under Grants Nos. 2018YFB1308601 and 2017YFE0119300, in part by the National Natural Science Foundation of China under Grant No. 62002013 and the Project funded by China Postdoctoral Science Foundation Grants Nos. 2019M660439 and 2020T130049, in part by the Industry-University-Research Cooperation Fund of ZTE Corporation.

requirements, such as message data, video and audio data in train control networks; third, bursty non-real-time flows, mainly used for services that do not require real-time transmission, such as file transfer, web browsing, etc. For periodic flows, TSN introduces a time-triggered (TT) transmission mechanism[6-8], which takes into account the topology, bandwidth, cache and other network resources and the real-time and deterministic requirements of applications to calculate the sending time of flows in each network device (including switches and terminals) with global scheduling, and then the devices send flows periodically at these time points. Such a transmission method can customize the end-to-end delay of each flow to meet the period and delay requirements of different control services for different industrial applications. The jitter of delay depends on the accuracy of time synchronization, that is, the maximum time deviation between any two devices in a time-synchronized network. TSN uses simplified IEEE 1588[9] to achieve network time synchronization, which is standardized as IEEE 802.1AS[10]. Generally, the accuracy of time synchronization can reach the microsecond or even sub-microsecond level. Periodic flows are also called time-triggered flows. Both bursty real-time and non-real-time flows use the best-effort transmission and provide different quality of service by prioritization[11-12] and traffic shaping like the credit-based shaper (CBS)[13-14]. Therefore, if no distinction is necessary, the two kinds of flows are collectively referred to as bursty flows, abbreviated as best-effort (BE) flows.

In order to achieve mixed transmission of bursty and periodic flows, TSN first defines a time-aware shaper (TAS) in 802.1Qbv[15]. The TAS stores periodic flows in high-priority queues and bursty flows in low-priority queues. Periodic flows are transmitted at precise sending points that are transformed into a gate control list (GCL) of the TAS. The GCL periodically turns on the high-priority queues and turns off the low-priority queues at the precise sending points to realize the accurate transmission of periodic flows. After the periodic flows are sent, the high-priority queues are turned off, and in the meantime, the low-priority queues are turned on to transmit bursty flows.

TAS uses GCL to accurately reserve bandwidth for periodic flows, but it does not solve the problem of wasting reserved bandwidth caused by the lack of periodic flows. Moreover, due to the uncertainty of bursty flows, it is possible that the bursty flows are being sent when the periodic flow starts to be sent. To avoid the conflicts between the bursty flows and the periodic flows, 802.1Qbv defines a guard band strategy, but the strategy leads to a waste of bandwidth. In order to save bandwidth, 802.1Qbu[16] defines a frame preemption strategy, but it causes delay jitters of periodic service flows. To avoid delay jitters, the mixed strategy of the guard band and frame preemption still results in a waste of bandwidth. In order to solve the bandwidth wastage problem caused by the mixed strategy, we propose a predictive mixed transmission mechanism for the bursty flows and periodic flows.

This paper constructs a probabilistic model of the predictive mixed transmission mechanism, and proves that the mechanism can effectively reduce bandwidth loss while avoiding the conflicts between the periodic flows and the bursty flows. By simulating the arrival of the bursty flows under different probability distributions, the predictive mixed transmission mechanism reduces the expectation of bandwidth loss to one-fifth of that compared with the previous mixed strategy, namely the combination of guard band (802.1 Qbv) and frame preemption (802.1 Qbu). Our main contributions are fourfold as follows.

• First, we propose a predictive mixed transmission mechanism to further reduce the bandwidth loss by the predictability of time-triggered transmission.

• Second, we formalize the predictive mechanism to minimize the bandwidth loss by computing the optimized preemption positions for bursty frames.

• Third, we present probabilistic models of mixed transmission strategies and prove that the proposed predictive mechanism can effectively reduce bandwidth loss.

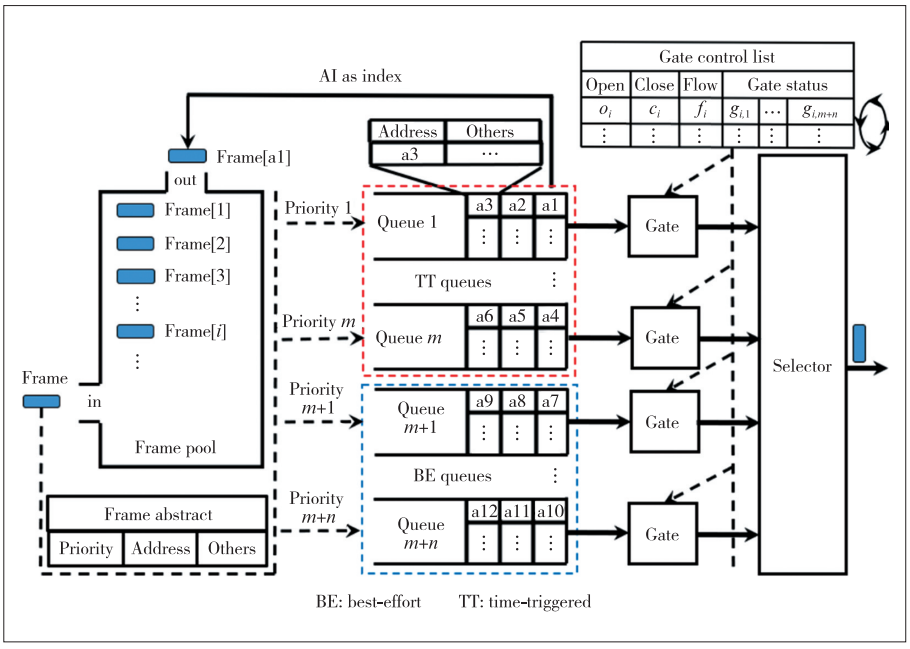
• Finally, we verify the effectiveness of the proposed predictive mechanism by simulating the probabilistic models.

The rest of the paper is organized as follows. Section 2 reviews related work. The background of the mixed transmission of TT and BE flows is described in Section 3. Section 4 presents the proposed predictive mixed transmission mechanism, gives the corresponding algorithm and mathematical model, and proves its advantages in reducing bandwidth loss by comparing it with the previous mixed-transmission strategies. Section 5 conducts experimental tests by simulating the probabilistic models of different mixed-transmission strategies. Finally, we conclude this paper in Section 6.

2 Related Work

TAS is the core mechanism of TSN to realize the deterministic real-time transmission of the periodic flow, which is standardized as 802.1Qbv, and Fig. 1 illustrates the TAS in 802.1Qbv.

A frame is received and stored in the frame pool. The abstract information, such as priority, length, and the address in a frame pool, is usually extracted from the frame when it is received. The abstract information is stored in different queues according to priority. The priority queues are divided into two types: storing periodic flows and storing bursty flows. Periodic flows are transmitted deterministically with the gate control list (GCL) and bursty flows are transmitted in the interval of periodic flows. Different output selectors, such as the strict priority transmission and the credit-based traffic shaper, are used to guarantee Quality of Service (QoS) of bursty flows. The table items of GCL usually include w_i (the duration of the window), o_i (the start time of the window), $f_{i,1}\cdots f_{i,j}$ (the periodic flows that need to be transmitted within the duration of the



▲ **Figure 1. Time-aware shaper (TAS) defined by IEEE 802.1Qbv**

window), and gate status (consisting of 0 or 1, where 0 means gate control is turned on and 1 means gate control is turned off). GCL is executed in order of o_i to control the gates of different queues. At the start time of the window, the gate of the corresponding queue is turned on and the gates of other queues are turned off to realize the accurate transmission of periodic flows at the scheduled time. As soon as the TT flows are sent, the corresponding gate is turned off and the gates of other queues are turned on to enable the transmission of bursty flows. After GCL finishes executing the last entry, it starts from the first entry again and loops periodically.

Because of the uncertainty of bursty flows, when the sending points of periodic flows arrive, the bursty flows may be transmitted. In order to avoid conflicts between bursty flows and periodic flows, 802.1Qbv defines a guard band strategy to turn off the bursty flow queues at the time Δt prior to the sending points of periodic flows so that the remained part of bursty frames can be sent within Δt time. The Δt is the guard band which ensures that periodic flows will not conflict with bursty flows when it is sent, but the size of the guard band is the length of the maximum frame of bursty flows, which leads to a waste of bandwidth.

To save bandwidth, 802.1Qbu[16] defines a frame preemption strategy. That is, when a bursty flow is being sent and a periodic flow is ready to be sent, the bursty flow is filled with the correct cyclic redundancy check (CRC), and the transmission is interrupted. And the transmission is not resumed until the transmission of the periodic flow is completed. Each preemption will cause an additional 24 bytes (4-byte CRC, 12-byte minimum inter-frame spacing, 6-byte leading code, 1-byte preempted-frame start, and 1-byte frame number) of bandwidth loss and delay jitter. Furthermore, since the minimum length of an Ethernet frame is 64 bytes, to prevent the sent length and remaining length from being less than 64 bytes, the minimum frame length to be preempted is 124 bytes. Therefore, in the worst case, the delay jitter of periodic flows caused by frame preemption is 123 bytes. In order to avoid the delay jitter of 123 bytes, combining the guard band strategy of 802.1Qbv and the frame preemption strategy of 802.1Qbu, the size of Δt can be set to 123 bytes, and the frame preemption strategy is executed at Δt prior to the sending points of the periodic flows. The mixed strategy avoids the delay jitter caused by frame preemption, and at the same time reduces the size of the guard band to 123 bytes. But as long as the preemption is successful, the 123-byte guard band consumes only 4 bytes (CRC), resulting in a waste of 119 bytes, and an additional 20 bytes of bandwidth waste (including 12-byte minimum inter-frame spacing, 6-byte preamble, 1-byte preemption frame start character, and 1-byte frame sequence number) for the remaining transmission of the preempted frame.

To further reduce bandwidth wastage of the mixed strategy namely the combination of 802.1Qbv and 802.1Qbu, this paper proposes a predictive mixed transmission mechanism for bursty flows and periodic flows. Its core idea is to use the predictability of time-triggered transmission in TSN:

• The upcoming periodic flow is predictable because it can be obtained by querying the GCL. So, when the bursty flow is to be sent, we first calculate the remaining time to the sending point of the upcoming periodic flow. If the remaining time is enough to finish sending the bursty flow, the bursty flow is sent immediately; otherwise, it will be sent after the periodic flow.

• The current bursty flow to be sent is predictable because the flow is the header frame in bursty flow queues. So, when there is no enough time left to send the complete frame, the optimal preemption position can be calculated based on the frame length of the bursty flow and the time left to the sending point of the upcoming periodic flow, to minimize bandwidth loss.

3 Background

This section details the existing TSN standards for the mixed transmission of bursty flows and periodic flows, and analyzes their impact on bandwidth loss and delay jitter.

3.1 Guard Band Strategy

We define the sending time point of a periodic flow f_i as o_i, and Δt is the guard band, the size of which is the maximum frame length of bursty flows. To formalize the bandwidth loss (also denoted as GuardLoss) of the guard band strategy, we define the length of the bursty flow as a random variable X when a periodic flow f_i conflicts with a bursty flow at the start time of GCL. The maximum length of bursty flows is denoted as $L_{BE}^{\max}$, and the minimum length as $L_{BE}^{\min}$. At the sending point of f_i, the sent length of the bursty frame is defined as a random variable Y.

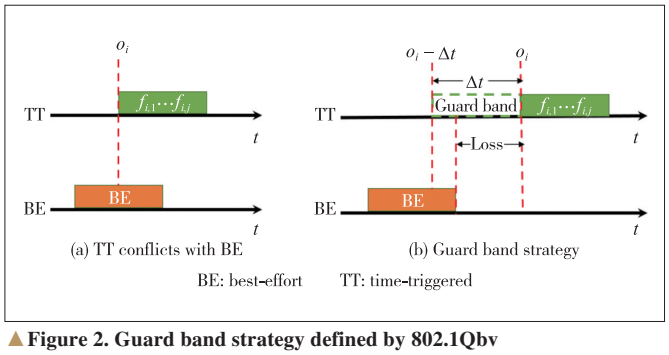
When the sending time point of a periodic flow (TT) arrives and if a bursty flow has not finished its transmission yet, a conflict happens. Fig. 2(a) shows a conflict that the i-th entry in GCL is sent at the sending time o_i, and the BE data have not finished transmission yet. To resolve the conflict, 802.1Qbv defines a guard band strategy, as shown in Fig. 2(b). It turns off the transmission gates of bursty flow queues at Δt prior to the arrival of the periodic flow sending time o_i, that is, at $o_i - \Delta t$. The Δt time must be big enough to make any bursty flow being sent complete so that there is no conflict with bursty flows when periodic flows are sent. Therefore, the size of Δt is the maximum frame length of bursty flows, and Δt is called the guard band.

The guard band strategy ensures the conflict-free transmission of periodic flows and bursty flows. But depending on the arrival timing of bursty flows, the part of bandwidth not occupied by burst flows is wasted, as illustrated in the "Loss" part of Fig. 2b. The size of the guard band is $L_{BE}^{\max}$ and thus the unused length of the guard band is $L_{BE}^{\max} - (X - Y)$. The bandwidth loss caused by the guard b of f_i can be expressed as follows:

$$f_i.\text{GuardLoss} = L_{BE}^{\max} - (X - Y). \tag{1}$$

Periodic flows and bursty flows are conflict-free transmission, so the jitter caused by the guard band strategy is 0:

$$f_i.\text{GuardLoss} = 0. \tag{2}$$

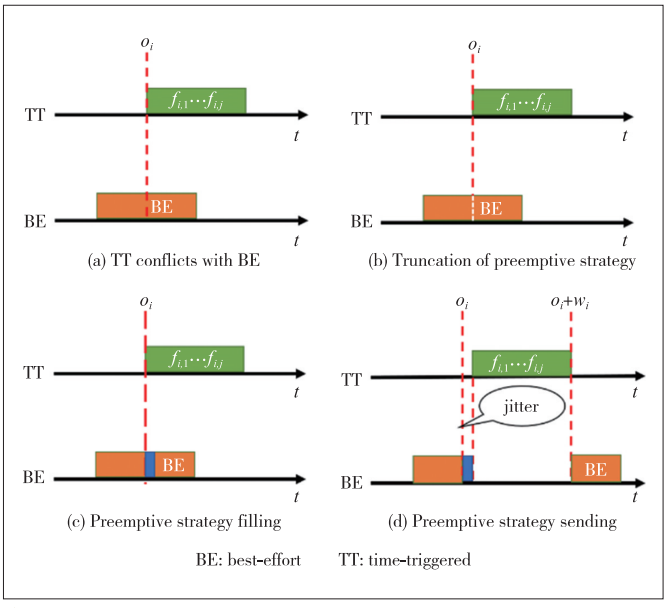


▲ **Figure 2. Guard band strategy defined by 802.1Qbv**

3.2 Preemption Strategy

To reduce bandwidth loss of the guard band strategy, 802.1Qbu defines a preemption strategy, as shown in Figs. 3 (b), 3(c), and 3(d). Fig. 3(a) illustrates a periodic flow in conflict with a bursty flow. Fig. 3(b) shows a periodic flow truncating a bursty frame at the moment of transmission. Fig. 3(c) illustrates the truncated bursty frame filled with a 4-byte CRC and interrupting its transmission and then starting the transmission of the periodic flow. Fig. 3(d) illustrates that the transmission of the remaining part of the truncated frame in the bursty flow is resuming after the periodic flow is completed.

In order to ensure that the truncated frame is a legal Ethernet frame, the preemptive strategy requires that the length of the two parts of the truncated frame cannot be less than the minimum Ethernet frame length, namely 64 bytes. Therefore, the minimum length of an Ethernet frame that can be truncated is 124 bytes (60 bytes and 64 bytes). Meantime, due to the truncation, the original frame is divided into two frames to be sent, so the additional required bandwidth includes 4-byte CRC, 12-byte minimum inter-frame spacing, 6-byte preamble, 1-byte preempted frame start and 1-byte frame number, a total of 24 bytes. The following still uses random variables X and Y to analyze the bandwidth loss and delay jitter caused by the preemption strategy.



▲ **Figure 3. Preemption strategy defined by 802.1Qbu**

1) When the bursty flow length is less than 124 bytes, that is, $L_{BE}^{\min} \leqslant X < 124$, the frame cannot be truncated, and the bandwidth loss (denoted as PreemptionLoss) and delay jitter (denoted as PreemptionJitter), are formulated as follows:

$$\begin{aligned} &f_i.\text{PreemptionLoss} = 0, \text{ if } L_{BE}^{\min} \leqslant X < 124 \\ &f_i.\text{PreemptionJitter} = X - Y, \text{ if } L_{BE}^{\min} \leqslant X < 124. \end{aligned} \tag{3}$$

2) When the length of the bursty flow is greater than or equal to 124 bytes, that is, $124 \leqslant X < L_{BE}^{\max}$.

• If $0 \leqslant Y < 60$, the periodic flow f_i cannot be truncated until the bursty flow has been sent out of 60 bytes. As a result, bandwidth loss (PreemptionLoss) and delay jitter (PreemptionJitter) are as follows:

$$\begin{aligned} &f_i.\text{PreemptionLoss} = 24, \text{ if } 124 \leqslant X < L_{BE}^{\max}, 0 \leqslant Y < 60 \\ &f_i.\text{PreemptionJitter} = (60 - Y) + 4, \text{ if } 124 \leqslant X < L_{BE}^{\max}, 0 \leqslant Y < 60. \end{aligned} \tag{4}$$

• If $60 \leqslant Y$ and the remaining unsent part of the bursty flow is greater than or equal to 64 bytes, that is, $64 \leqslant X - Y$, the periodic flow f_i can directly cut off the bursty flow. As a result, the bandwidth loss (PreemptionLoss) and delay jitter (PreemptionJitter) are as follows:

$$\begin{aligned} &f_i.\text{PreemptionLoss} = 24, \text{if } 124 \leqslant X < L_{BE}^{\max}, 60 \leqslant Y, 64 \leqslant X - Y \\ &f_i.\text{PreemptionJitter} = 4, \text{if } 124 \leqslant X < L_{BE}^{\max}, 60 \leqslant Y, 64 \leqslant X - Y. \end{aligned} \tag{5}$$

• If 60≤Y and the remaining unsent part of the bursty flow is less than 64 bytes, that is, X−Y<64, the periodic flow f_i cannot intercept the bursty flow. As a result, the bandwidth loss (PreemptionLoss) and delay jitter (PreemptionJitter) are as follows:

$$\begin{aligned} &f_i.\text{PreemptionLoss} = 0, \text{if } 124 \leqslant X < L_{BE}^{\max}, 60 \leqslant \text{Y}, \text{X} - \text{Y} < 64 \\ &f_i.\text{PreemptionJitter} = X - Y, \text{if } 124 \leqslant X < L_{BE}^{\max}, 60 \leqslant \text{Y}, \text{X} - \text{Y} < 64. \end{aligned} \tag{6}$$

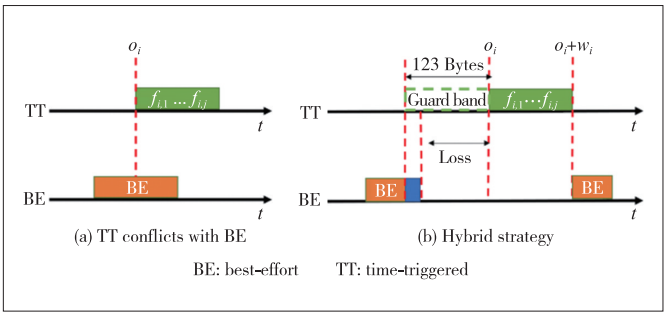
In summary, when the periodic flow f_i conflicts with the bursty flow, the bandwidth loss and delay jitter caused by the preemption strategy are formalized as follows:

$$f_i.\text{PreemptionLoss} = \begin{cases} 0, & \text{if } L_{BE}^{\min} \leqslant \text{X} < 124, \\ 24, & \text{if } 124 \leqslant X < L_{BE}^{\max}, 1 \leqslant \text{Y} < 60, \\ 24, & \text{if } 124 \leqslant X < L_{BE}^{\max}, 60 \leqslant \text{Y}, 64 \leqslant \text{X} - \text{Y}, \\ 0, & \text{if } 124 \leqslant X < L_{BE}^{\max}, 60 \leqslant \text{Y}, \text{X} - \text{Y} < 64. \end{cases} \tag{7}$$

$$f_i.\text{PreemptionJitter} = \begin{cases} X - Y, & \text{if } L_{BE}^{\min} \leqslant X < 124, \\ (60 - Y) + 4, & \text{if } 124 \leqslant X < L_{BE}^{\max}, 1 \leqslant Y < 60, \\ 4, & \text{if } 124 \leqslant X < L_{BE}^{\max}, 60 \leqslant Y, 64 \leqslant X - Y, \\ X - Y, & \text{if } 124 \leqslant X < L_{BE}^{\max}, 60 \leqslant Y, X - Y < 64. \end{cases} \tag{8}$$

3.3 Mixed Strategy of Guard Band and Preemption

Although the preemptive strategy reduces the bandwidth loss compared with the guard band strategy, it brings in additional delay jitter and weakens the certainty of time-triggered transmission. To eliminate the delay jitter of the preemptive strategy and reduce the bandwidth loss of the guard band strategy, we combine the guard band with the preemption strategy. Fig. 4 illustrates the mixed strategy.



▲ **Figure 4. Mixed strategy of guard band and preemption**

To eliminate the delay jitter of up to 123 bytes caused by the preemptive strategy, the mixed strategy sets the guard band to 123 bytes. That is, we close the queues of bursty flows at 123 bytes prior to the start of periodic flows, and follow the preemption strategy to preempt bursty flows at this time. The bandwidth loss and delay jitter caused by the mixed strategy are analyzed as follows:

1) Since the mixed strategy brings in a 123-byte guard band that eliminates the delay jitter caused by the preemptive strategy, the delay jitter caused by the mixed strategy is 0.

2) The emergence of the guard band in the mixed strategy increases the bandwidth loss of the preemptive strategy.

• If the length of a bursty flow is less than 124 bytes, that is, $L_{BE}^{\min} \leqslant X < 124$, the frame cannot be preempted, and the unused part of the guard band is the loss of bandwidth denoted as MixedLoss:

$$f_i.\text{MixedLoss} = 123 - (X - Y), \text{ if } L_{BE}^{\min} \leqslant \text{X} < 124. \tag{9}$$

• If the length of a bursty flow is greater than or equal to 124 bytes, that is, $124 \leqslant \text{X} < L_{BE}^{\max}$. At the beginning of the guard band, $(o_i - 123)$, if the sent part of the bursty flow is less than 60 bytes, that is, $0 \leqslant Y < 60$, it cannot be preempted until the sent part reaches 60 bytes. The loss of bandwidth includes the unused part of the guard band and the additional number of bytes caused by preemption:

$$f_i.\text{MixedLoss} = \big(123 - (60 - Y + 4)\big) + 24, \text{if } 124 \leqslant X < L_{BE}^{\max}, 0 \leqslant \text{Y} < 60. \tag{10}$$

• If the length of a bursty flow is greater than or equal to 124 bytes, it means that $124 \leqslant X < L_{BE}^{\max}$. At the beginning of the guard band, $(o_i - 123)$, if the sent part of the bursty flow

is greater than or equal to 60 bytes, namely, $60 \leqslant Y$, and the remaining part is also greater than or equal to 64 bytes, namely, $64 \leqslant X - Y$, the bursty frame can be directly cut off. The loss of bandwidth includes the unused part of the guard band and the additional number of bytes caused by preemption:

$$f_i.\text{MixedLoss} = (123 - 4) + 24,\ \text{if}\ 124 \leqslant X < L_{BE}^{\max}, 60 \leqslant Y, 64 \leqslant X - Y. \quad (11)$$

• If the length of a bursty flow is greater than or equal to 124 bytes, it means that $124 \leqslant X < L_{BE}^{\max}$. At the beginning of the guard band, $(o_i - 123)$, if the sent part of the bursty flow is greater than or equal to 60 bytes, namely, $60 \leqslant Y$, but the remaining part is less than 64 bytes, namely, $X - Y < 64$, the bursty frame cannot be truncated, and the unused part of the guard band is the loss of bandwidth:

$$f_i.\text{MixedLoss} = 123 - (X - Y),\ \text{if}\ 124 \leqslant X < L_{BE}^{\max}, 60 \leqslant Y, X - Y < 64. \quad (12)$$

In summary, the bandwidth loss caused by the mixed strategy is presented as follows:

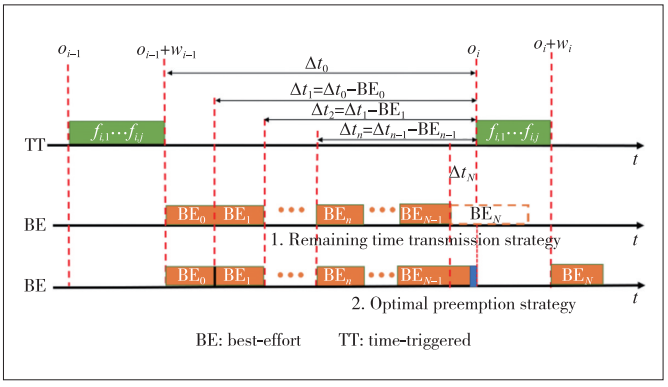
$$f_i.\text{MixedLoss} = \begin{cases} 123 - (X - Y), & \text{if}\ L_{BE}^{\min} \leqslant X < 124, \\ 83 + Y, & \text{if}\ 124 \leqslant X < L_{BE}^{\max}, \\ & 0 \leqslant Y < 60, \\ 143, & \text{if}\ 124 \leqslant X < L_{BE}^{\max}, \\ & 60 \leqslant Y, 64 \leqslant X - Y, \\ 123 - (X - Y), & \text{if}\ 124 \leqslant X < L_{BE}^{\max}, \\ & 60 \leqslant Y, X - Y < 64. \end{cases} \quad (13)$$

4 Predictive Mixed Transmission Mechanism

To conquer the shortcomings of the existing mixed transmission mechanism for the bursty flow and the periodic flow, this part presents the proposed predictive mixed transmission mechanism including its principle, probability model, and algorithms in detail.

4.1 Remaining Time Transmission Strategy

Bursty flows are always sent in the gap between periodic flows, and the size of the gap is predictable. Fig. 5 shows two adjacent items $i - 1$ and i in GCL. When the $(i - 1)$-th item finishes sending its corresponding periodic flows, bursty flows start to be sent and stop when the i-th entry starts to be executed. The duration for sending bursty flows is the gap. In Fig. 5, Δt_0 is the initial value of the gap, namely, from the end time of the execution of the $(i - 1)$-th item, $o_{i-1} + w_{i-1}$, to the start time of the i-th entry, o_i. With the transmission of bursty flows, $BE_0, BE_1, \cdots$, going on, when BE_n is to be sent, the remaining gap is $\Delta t_n = \Delta t_{n-1} - BE_{n-1}$. We define that the frame is sent immediately if the remaining time is sufficient to send the frame completely. After the frame is sent, it is evaluated again whether the remaining time is sufficient to completely send the next bursty frame, and if possible, continue to send, until the remaining time is not enough to send the frame completely. Algorithm 1 illustrates the process of the remaining time transmission strategy. The remaining time Δt_N shown in Fig. 5 is not enough to send the frame BE_N completely, and the transmission is terminated. As a result, the remaining time Δt_N is the bandwidth loss caused by the transmission strategy. According to the definition of the random variable Y, the bandwidth loss denoted as RemainedTimeLoss is presented as follows:



▲ **Figure 5. Remaining time transmission strategy and optimal preemption strategy**

$$f_i.\text{RemainedTimeLoss} = Y. \quad (14)$$

Algorithm 1: Remaining Time Transmission Strategy

Input: BE, o_{i-1}, w_{i-1}, o_i
Output: Δt
1 **begin**
2 // The execution of entry i-1 is completed
3 SetTimer$(o_{i-1} + w_{i-1})$;
4 $\Delta t = o_i - (o_{i-1} + w_{i-1})$;
5 // Initialization remaining time
6 **while** (BE.Queues.top().length $\leqslant \Delta t$) **do**
7 // Check whether the header frame can be sent completely
8 Frame frame = BEQueues.dequeue();
9 // Fetch header frame
10 Transmit(frame); // Send frame
11 // Update remaining time
12 $\Delta t = \Delta t - BE$.length;
13 **end**
14 **end**

4.2 Optimal Preemption Strategy

In order to further reduce the bandwidth loss caused by the remaining time transmission strategy without causing any addi-

tional delay jitter, as shown in Fig. 5, when the remaining time Δt_N is not enough to send the frame BE_N completely, the optimal preemption is proposed and illustrated in Fig. 5. It predicts the optimal preemption position (the position corresponding to the first bit of the frame) is based on the remaining time Δt_N and the frame length BE_N.length, and minimizes the bandwidth loss, namely minimizing Δt_N − position. Moreover, the preemption position needs to satisfy the following conditions:

1) The part of the frame before the preemption position and the filled 4-byte CRC due to truncation must be sent within Δt_N, otherwise, delay jitter will be brought in.

$$\Delta t_N \geqslant \text{position} + 4 . \tag{15}$$

2) The part of the frame before the preemption position needs to be greater than or equal to 60 bytes since the minimum length of an Ethernet frame is 64 bytes.

$$\text{position} \geqslant 60 . \tag{16}$$

3) The remaining part of the frame after the preemption position needs to be greater than or equal to 64 bytes since the minimum length of an Ethernet frame is 64 bytes.

$$BE_N.\text{length} - \text{position} \geqslant 64 . \tag{17}$$

Therefore, the problem of the optimal preemption strategy can be formalized as:

$$\min_{\text{position}} \left(\Delta t_N - \text{position}\right).$$

The constraints are:

$$\begin{cases} \Delta t_N \geqslant \text{position} + 4 \\ \text{position} \geqslant 60 \\ BE_N.\text{length} - \text{position} \geqslant 64 \\ BE_N.\text{length} > \Delta t_N \end{cases} . \tag{18}$$

We solve the problem above and give the optimal positions in terms of different Δt_N and BE_N.length.

• When BE_N.length < 124, BE_N cannot be preempted, the bandwidth loss is Δt_N, and the position is 0.

• When BE_N.length ⩾ 124, Δt_N < 64, BE_N cannot be preempted, the bandwidth loss is Δt_N, and the position is 0.

• When BE_N.length ⩾ 124, Δt_N ⩾ 64, BE_N.length − (Δt_N − 4) ⩾ 64, BE_N can be preempted, and the preempted position is position=(Δt_N − 4). The bandwidth loss is 24 bytes of bandwidth consumption caused by frame preemption.

• When BE_N.length ⩾ 124, Δt_N ⩾ 64, BE_N.length − (Δt_N − 4) < 64, BE_N can also be preempted, and the preempted position is position= BE_N.length − 64. The bandwidth loss is Δt_N − (BE_N.length − 64)+ 24 = Δt_N − BE_N.length + 88.

That is,

$$\text{position} = \begin{cases} 0, & BE_N.\text{length} < 124 \\ 0, & BE_N.\text{length} \geqslant 124, \Delta t_N < 64 \\ \Delta t_N - 4, & BE_N.\text{length} \geqslant 124, \Delta t_N \geqslant 64, \\ & BE_N.\text{length} - \Delta t_N \geqslant 60 \\ BE_N.\text{length} - 64, & BE_N.\text{length} \geqslant 124, \Delta t_N \geqslant 64, \\ & BE_N.\text{length} - \Delta t_N < 60 \end{cases} . \tag{19}$$

According to the definition of random variables X and Y, X is equal to BE_N.length and Y is equal to BE_N. So, we directly give the probability model of bandwidth loss caused by the optimal preemption strategy as below:

$$f_i.\text{OptPreemptionLoss} = \begin{cases} Y, & X < 124 \\ Y, & X \geqslant 124, Y < 64 \\ 24, & X \geqslant 128, Y \geqslant 64, X - Y \geqslant 60 \\ (Y - X) + 88, & X \geqslant 128, Y \geqslant 64, X - Y < 60 \end{cases} . \tag{20}$$

When the remaining time transmission strategy cannot continue sending a busty frame, the optimal preemption strategy can be applied to send the busty frame by evaluating the optimal preemption position. So, the predictive mixed transmission mechanism consists of the two strategies. Algorithm 2 gives the whole process of the proposed predictive mixed transmission mechanism.

4.3 Guaranteed Advantages

Compared with the guard band strategy defined in 802.1Qbv, the proposed remaining time transmission strategy can iteratively use the gap between periodic flows till the remaining time is insufficient to send the current bursty frame. The core improvement of the strategy is to use the remaining time to adapt to the frame length of bursty flows, instead of selecting the maximum length as the fixed size of the guard band. We prove that the remaining time transmission strategy is better than the guard band strategy by their probabilistic models of bandwidth loss.

Theorem 1: The bandwidth loss of the remaining time transmission strategy is better than the guard band strategy of 802.1Qbv.

Proof: The bandwidth-loss probability model of the guard band strategy is:

$$f_i.\text{GuardLoss} = L_{BE}^{\max} - (X - Y) . \tag{21}$$

Algorithm 2: Predictive Mixed Transmission Mechanism

Input: BE, o_{i-1}, w_{i-1}, o_i
Output: position

```
1 begin
2     // The execution of entry i−1 is completed
3     SetTimer(o_{i-1} + w_{i-1});
4     // Initialization remaining time
5     Δt = o_i − (o_{i-1} + w_{i-1});
6     // Initialization remaining time
7     while (BE.Queues.top().length ⩽ Δt) do
8       // Check whether the header frame can be sent completely
9       Frame frame = BEQueues.dequeue();
10      // Fetch header frame
11      Transmit(frame); // Send frame
12      // Update remaining time
13      Δt = Δt − frame.length;
14    end
15    // Optimal Preemption Strategy
16    length = BE.Queues.top().length;
17    switch (Δt, length) do
18      case length < 124 do
19            position = 0;
20            break;
21      end
22      case length ⩾ 124, Δt < 64 do
23            position = 0;
24            break;
25      end
26      case length ⩾ 124, Δt ⩾ 64,
            length − (Δt − 4) ⩾ 64 do
27            position = Δt − 4;
28            break;
29      end
30      case length ⩾ 124, Δt ⩾ 64,
            length − (Δt − 4) < 64 do
31            position = BE_N.length − 64;
32            break;
33      end
34    end
35    Preemption(BEQueues,position);
36 end
```

The bandwidth-loss probability model of the remaining time transmission strategy is:

$$f_i.\text{RemainedTimeLoss} = Y \ . \tag{22}$$

Since $L_{BE}^{\max} - X \geqslant 0$, $f_i.\text{GuardLoss} = L_{BE}^{\max} - (X - Y) = (L_{BE}^{\max} - X) + Y \geqslant Y = f_i.\text{RemainedTimeLoss}$. Thus, $f_i.\text{GuardLoss} \geqslant f_i.\text{RemainedTimeLoss}$.

Therefore, the bandwidth loss of the remaining time transmission strategy is better than that of the guard band strategy.

In order to further reduce the bandwidth loss, this paper proposes an optimal preemption strategy. The strategy further reduces bandwidth loss by selecting the optimal preemption position when the remaining time is insufficient to completely send the current burst frame. Compared with the mixed strategy of the guard band strategy in 802.1Qbv and the frame preemption strategy in 802.1Qbu, the proposed optimal preemption strategy has obvious advantages. To prove the advantage, we give Theorem 2 as follows.

Theorem 2: The proposed optimal preemption strategy is better than the mixed strategy of the guard band strategy and the frame preemption strategy.

Proof: The bandwidth-loss probability model of the mixed strategy of guard band strategy and frame preemption strategy is:

$$f_i.\text{MixedLoss} = \begin{cases} 123 - (X - Y), & X < 124, \\ 83 + Y, & 124 \leqslant X, Y < 60, \\ 143, & 124 \leqslant X, 60 \leqslant Y, 64 \leqslant X - Y, \\ 123 - (X - Y), & 124 \leqslant X, 60 \leqslant Y, X - Y < 64. \end{cases} \tag{23}$$

The bandwidth-loss probability model of the optimal preemption strategy is:

$$f_i.\text{OptPreemptionLoss} = \begin{cases} Y, & X < 124 \\ Y, & X \geqslant 124, Y < 64 \\ 24, & X \geqslant 124, Y \geqslant 64, X - Y \geqslant 60 \\ (Y - X) + 88, & X \geqslant 124, Y \geqslant 64, X - Y < 60. \end{cases} \tag{24}$$

To prove the advantage of the proposed strategy, we compare the bandwidth loss in terms of different X and Y as below.

1) When $X < 124$, $f_i.\text{MixedLoss} = 123 - (X - Y) = (123 - X) + Y \geqslant Y = f_i.\text{OptPreemptionLoss}$.

2) When $124 \leqslant X$ and $Y < 60$, $f_i.\text{MixedLoss} = 83 + Y > Y = f_i.\text{OptPreemptionLoss}$.

3) When $124 \leqslant X$, $60 \leqslant Y$ and $64 \leqslant X - Y$, $f_i.\text{MixedLoss} = 143$.

- When $60 \leqslant Y < 64$, $f_i.\text{OptPreemptionLoss} = Y < 64 < 147 = f_i.\text{MixedLoss}$.
- When $64 \leqslant Y$, $f_i.\text{OptPreemptionLoss} = 24 < 143 = f_i.\text{MixedLoss}$.

4) When $124 \leqslant X$, $60 \leqslant Y$ and $X - Y < 64$, $f_i.\text{MixedLoss} = 123 - (X - Y) = (Y - X) + 123 \geqslant 60$.

- When $60 \leqslant Y < 64$, $f_i.\text{OptPreemptionLoss} = Y > Y + (123 - X) = f_i.\text{MixedLoss}$. We discuss different values of Y as below.

a) If $Y = 61$, and $124 \leqslant X < 125$, then when $X = 124$, $f_i.\text{MixedLoss} = 60$, $f_i.\text{OptPreemptionLoss} = 61$

b) If $Y = 62$, and $124 \leqslant X < 126$, then when $X = 124$, we have $f_i.\text{MixedLoss} = 61$, $f_i.\text{OptPreemptionLoss} = 62$, when $X =$

125, we have f_i.MixedLoss = 60, f_i.OptPreemptionLoss = 62

c) If Y = 63, and 124 ⩽ X < 127, then

when X = 124, we have f_i.MixedLoss = 62, f_i. OptPreemptionLoss = 63;

when X = 125, f_i.MixedLoss = 61, f_i.OptPreemptionLoss = 63;

when 126, we have f_i.MixedLoss = 60, f_i.OptPreemptionLoss = 63.

• When 64 ⩽ Y and 60 ⩽ $X - Y$ < 64, f_i.OptPreemptionLoss = 24 < −64 + 123 < $(Y - X)$ + 123 = f_i.MixedLoss.

• When 64 ⩽ Y and $X - Y$ < 60, f_i.OptPreemptionLoss = $(Y - X)$ + 88 < $(Y - X)$ + 123 = f_i.MixedLoss.

Above all, only when Y =61, 62, or 63, the mixed strategy saves bandwidth of no more than 3 bytes than that of the optimal preemption strategy. Since the variable Y represents the random bit position of a preempted BE frame at the specific time point of a TT frame, Y is not equal to 61, 62, or 63 with a high probability, and the bandwidth loss of the optimal preemption strategy is significantly less than that of the mixed strategy when Y is not equal to 61, 62, or 63. So, the optimal preemption strategy is better than the mixed strategy in the sense of probability.

5 Results and Analysis

This section conducts experimental tests to compare the proposed predictive mixed transmission mechanism with the previous mechanisms by simulating their probability models.

5.1 Experimental Setup

The experiments set X bursty flows to obey uniform distribution, binomial distribution, poisson distribution, and normal distribution within the range of length [64, 1 518]. Y is the uniform distribution number of the transmitted bytes of BE frames at the sending time points of TT frames. We use MATLAB programming to implement the bandwidth-loss probability models of all strategies.

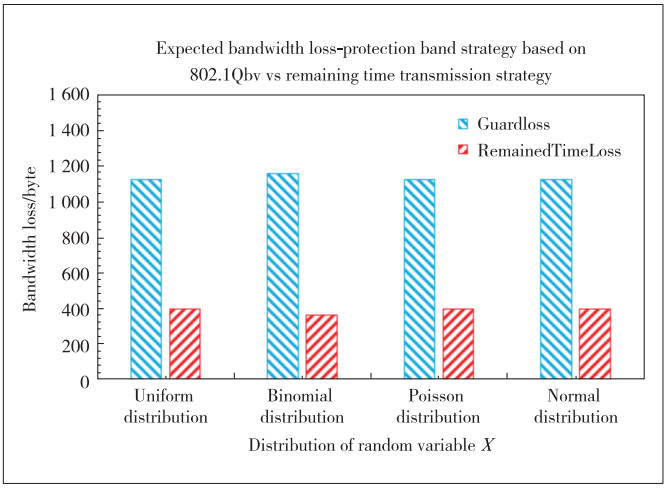
5.2 Experimental Results

First, we evaluate the expected bandwidth loss under the proposed remaining time transmission strategy and the guard band strategy, respectively. As illustrated in Table 1 and Fig. 6, the expected bandwidth loss of the remaining time transmission strategy is less than 400 bytes while the expected bandwidth loss of the guard band strategy is more than 1 100 bytes in all X distributions. As a result, the expected bandwidth loss of the remaining time transmission strategy is about one third of the expected bandwidth loss of the guard band strategy. And then, we evaluate the expected bandwidth loss under the proposed optimal preemption strategy and the mixed strategy of guard band and frame preemption, respectively. Table 2 and Fig. 7 are the expected bandwidth loss comparison of the optimal preemption strategy and the mixed strategy when X obeys uniform distribution, binomial distribution, Poisson distribution, and normal distribution. In all distributions, the expected bandwidth loss of the optimal strategy is less than 30 bytes while the expected bandwidth loss of the mixed strategy is more than 130 bytes. As a result, we achieve a 79.48% reduction of the expected bandwidth loss on average from the mixed strategy to the optimal preemption strategy. And different probabilistic distributions have a little effect on the expected bandwidth loss, which demonstrates that the proposed strategy has the consistent advantage of saving bandwidth.

Furthermore, Tables 3, 4, 5 and 6 illustrate the detailed comparison of different ranges of X and Y in uniform distribution, binomial distribution, Poisson distribution, and normal distribution, respectively. For all different ranges of X and Y, the optimal preemption strategy saves bandwidth better than

▼ **Table 1. Expected bandwidth loss: the remaining time transmission strategy (RemainedTimeLoss) vs the guard band strategy (Guardloss) of 802.1QBV**

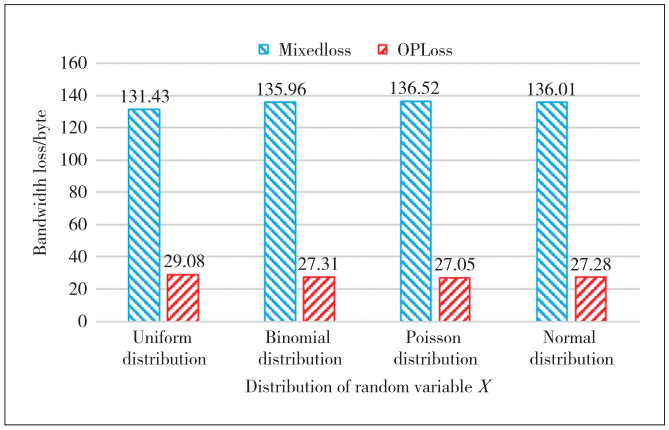
X Distribution Within the Range of Length [64, 1 518]	RemainedTimeLoss/byte	Guardloss/byte
Uniform distribution	395.5	1 122.5
Binomial distribution	363.75	1 154.2
Poisson distribution	395.5	1 122.5
Normal distribution	395.75	1 122.3



▲ **Figure 6. Comparison of the expected bandwidth loss between the remaining time transmission strategy and the guard band strategy of 802.1Qbv**

▼ **Table 2. Expected bandwidth loss: the optimal preemption strategy (OPLoss) vs the mixed strategy (MixedLoss) of the guard band and the frame preemption**

X Distribution Within the Range of Length [64, 1 518]	OPLoss/byte	MixedLoss/byte	Reduced Rate/byte
Uniform distribution	29.08	131.43	77.87%
Binomial distribution	27.31	135.96	79.91%
Poisson distribution	27.05	136.52	80.19%
Normal distribution	27.28	136.01	79.94%



▲**Figure 7. Comparison of the expected bandwidth loss between the optimal preemption strategy (OPLoss) and the mixed strategy (MixedLoss) of the guard band and the frame preemption**

▼**Table 3. Expected bandwidth loss of each part: the optimal preemption strategy (OPLoss) vs the mixed strategy (MixedLoss) in Uniform distribution**

Uniform Distribution Within the Range of Length [64, 1 518]	OPLoss/byte	MixedLoss/byte
$X < 124$	1.93	3.14
$X \geqslant 124$, $Y < 60$	3.04	11.61
$X \geqslant 124$, $Y \geqslant 60$, $X - Y \geqslant 64$	17.89	106.61
$X \geqslant 124$, $Y \geqslant 60$, $X - Y < 64$	6.22	10.07

▼**Table 4. Expected bandwidth loss of each part: the optimal preemption strategy (OPLoss) vs the mixed strategy (MixedLoss) in Binomial distribution**

Binomial Distribution (p=0.5) Within the Range of Length [64, 1 518]	OPLoss/byte	MixedLoss/byte
$X < 124$	0	0
$X \geqslant 124$, $Y < 60$	2.43	9.27
$X \geqslant 124$, $Y \geqslant 60$, $X - Y \geqslant 64$	19.91	118.64
$X \geqslant 124$, $Y \geqslant 60$, $X - Y < 64$	4.97	8.04

▼**Table 5. Expected bandwidth loss of each part: the optimal preemption strategy (OPLoss) vs the mixed strategy (MixedLoss) in poisson distribution**

Poisson Distribution Within the Range of Length [64, 1 518]	OPLoss/byte	MixedLoss/byte
$X < 124$	0	0
$X \geqslant 124$, $Y < 60$	2.24	8.53
$X \geqslant 124$, $Y \geqslant 60$, $X - Y \geqslant 64$	20.24	120.58
$X \geqslant 124$, $Y \geqslant 60$, $X - Y < 64$	4.57	7.4

that of the mixed strategy.

6 Conclusions

We first analyze the mixed transmission strategies of bursty flows and periodic flows in TSN, and point out that the mixed strategies of 802.1Qbv-based guard band strategy and 802.1Qbu-based frame preemption strategy can be improved.

▼**Table 6. Expected bandwidth loss of each part: the optimal preemption strategy (OPLoss) vs the mixed strategy (MixedLoss) in normal distribution**

Normal distribution within the range of length [64, 1 518]	OPLoss/byte	MixedLoss/byte
$X < 124$	0.016	0.028 9
$X \geqslant 124$, $Y < 60$	2.41	9.18
$X \geqslant 124$, $Y \geqslant 60$, $X - Y \geqslant 64$	19.94	118.83
$X \geqslant 124$, $Y \geqslant 60$, $X - Y < 64$	4.92	7.96

Then, we propose the predictive mixed transmission mechanism based on the prediction of time-triggered transmission. The proposed mechanism consists of the remaining time transmission strategy and the optimal preemption strategy. We present the probability models and algorithms of the proposed mechanism, and prove its advantages in terms of reducing bandwidth loss. Finally, we simulate the proposed mechanism by its probability model. Compared with the mixed strategy of guard band and frame preemption, we achieve a 79.48% reduction of the expected bandwidth loss of different probability distributions on average.

References

[1] HERMANN M, PENTEK T, OTTO B. Design principles for industrie 4.0 scenarios [C]//The 49th Hawaii International Conference on System Sciences. IEEE, 2016: 3928 – 3937
[2] ISO. Road vehicles: controller area network (CAN) (part 2): high-speed medium access unit. ISO 11898 [S]. 2016
[3] International Electrotechnical Commission. Electric railway equipment: Train bus (Part 2): train communication network conformance testing. IEC 61375 [S]. 2007
[4] DECOTIGNIE J D. Ethernet-based real-time and industrial communications [J]. Proceedings of the IEEE, 2005, 93(6): 1102 – 1117. DOI: 10.1109/JPROC.2005.849721
[5] LO BELLO L, STEINER W. A perspective on IEEE time-sensitive networking for industrial communication and automation systems [J]. Proceedings of the IEEE, 2019, 107(6): 1094 – 1120. DOI: 10.1109/JPROC.2019.2905334
[6] SAE International Group. Time-triggered Ethernet. Aerospace standard: AS6802 [S]. 2011
[7] SAE International Group. TTP Communication Protocol. Aerospace standard: AS6003 [S]. 2011
[8] STEINER W. An evaluation of SMT-based schedule synthesis for time-triggered multi-hop networks [C]//The 31st IEEE Real-Time Systems Symposium. IEEE, 2010: 375 – 384. DOI: 10.1109/RTSS.2010.25
[9] IEEE. Standard for a precision clock synchronization protocol for networked measurement and control systems. IEEE std 1588-2002 [S]. 2002. DOI: 10.1109/IEEESTD.2002.94144
[10] IEEE. IEEE standard for local and metropolitan area networks-timing and synchronization for time-sensitive applications in bridged local area networks. IEEE std 802 1AS-2011 [S]. 2011
[11] LI Z H, WAN H, DENG Y D, et al. A flattened-priority framework for mixed-criticality systems [J]. IEEE transactions on industrial electronics, 2020, 67 (11): 9862 – 9872. DOI: 10.1109/TIE.2019.2956406
[12] LI Z H, WAN H, DENG Y D, et al. A resource-efficient priority scheduler for time-sensitive networking switches [J]. CCF transactions on networking, 2020, 3(1): 21 – 34. DOI: 10.1007/s42045-020-00034-x
[13] IEEE. IEEE standard for local and metropolitan area networks-audio video bridging (AVB) systems [S]. 2011
[14] IEEE. IEEE standard for local and metropolitan area networks-virtual bridged local area networks amendment 12: Forwarding and queuing enhancements for time-sensitive streams. IEEE std 802 1Qav-2009 [S]. 2010

[15] IEEE. IEEE standard for local and metropolitan area networks-bridges and bridged networks-amendment 25: Enhancements for scheduled traffic. IEEE Std 802.1Q-2011 [S]. 2011
[16] IEEE. IEEE standard for local and metropolitan area networks: bridges and bridged networks: amendment 26: frame preemption. IEEE std 802 1Qbu-2016 [S]. 2016

Biographies

LI Zonghui received his BS degree in computer science from Beijing Information Science and Technology University, China in 2010, and MS and PhD degrees from the Institute of Microelectronics and the School of Software, Tsinghua University, China in 2014 and 2019, respectively. He is currently an associate professor in the School of Computer and Information Technology, Beijing Jiaotong University, China. His research interests include embedded and high performance computing, real-time embedded systems, especially for industrial control networks and time-sensitive networking.

YANG Siqi received her BS degree in network engineering from Hebei University, China. She is currently working toward her master's degree at Beijing Jiaotong University, China. Her research interest is real-time networks.

YU Jinghai (yu.jinghai@zte.com.cn) received his master's degree from Nanjing University of Posts and Telecommunications, China in 1999. He is currently working in the Data System Department of ZTE Corporation, with more than 20 years of research and design experience in data network products including BIER, Detnet, TSN, Switch and Router, Data Center and SDN. He has won the 21st China Patent Silver Award and the first prize of the Science and Technology Award of the China Communications Society.

HE Fei is an associate professor at the School of Software of Tsinghua University, China. He received his PhD degree from Tsinghua University in 2008. His research interests include model checking, program verification and automated logic reasoning. He has published over 70 papers in academic journals and international conferences. He is currently on the editor board of *Theory of Computing Systems and Frontiers of Computer Science*. He has served as the PC member for many formal conferences, including ICSE, ESEC/FSE, CONCUR, FMCAD, SAT, ATVA, APLAS, ICECCS, SETTA, etc.

SHI Qingjiang received his PhD degree in electronic engineering from Shanghai Jiao Tong University, China in 2011. From September 2009 to September 2010, he visited Prof. Z.-Q. (Tom) LUO's research group at the University of Minnesota, USA. In 2011, he worked as a research scientist at Bell Labs China. From 2012, he was with the School of Information and Science Technology at Zhejiang Sci-Tech University, China. From Feb. 2016 to Mar. 2017, he worked as a research fellow at Iowa State University, USA. From Mar. 2018, he has been a full professor with the School of Software Engineering at Tongji University, China. He is also with the Shenzhen Research Institute of Big Data. His interests lie in algorithm design and analysis with applications in machine learning, signal processing and wireless networks. So far he has published more than 70 IEEE journals and filed about 30 national patents. He has received the Outstanding Technical Achievement Award in 2021, the Huawei Technical Cooperation Achievement Transformation Award (2nd Prize) in 2022, the Golden Medal at the 46th International Exhibition of Inventions of Geneva in 2018, the First Prize of Science and Technology Award from China Institute of Communications in 2017, the National Excellent Doctoral Dissertation Nomination Award in 2013, the Shanghai Excellent Doctoral Dissertation Award in 2012, and the Best Paper Award from the IEEE PIMRC'09 conference.

Label Enhancement for Scene Text Detection

MEI Junjun[1,2], GUAN Tao[1,2], TONG Junwen[1,2]
(1. State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen 518055, China;
2. ZTE Corporation, Shenzhen 518057, China)

DOI: 10.12142/ZTECOM.202204011
https://kns.cnki.net/kcms/detail/34.1294.TN.20221125.1359.004.html, published online November 26, 2022
Manuscript received: 2021-12-28

Abstract: Segmentation-based scene text detection has drawn a great deal of attention, as it can describe the text instance with arbitrary shapes based on its pixel-level prediction. However, most segmentation-based methods suffer from complex post-processing to separate the text instances which are close to each other, resulting in considerable time consumption during the inference procedure. A label enhancement method is proposed to construct two kinds of training labels for segmentation-based scene text detection in this paper. The label distribution learning (LDL) method is used to overcome the problem brought by pure shrunk text labels that might result in sub-optimal detection performance. The experimental results on three benchmarks demonstrate that the proposed method can consistently improve the performance without sacrificing inference speed.

Keywords: label enhancement; scene text detection; semantic segmentation

Citation (IEEE Format): J. J. Mei, T. Guan, and J. W. Tong, "Label enhancement for scene text detection," *ZTE Communications*, vol. 20, no. 4, pp. 89 - 95, Dec. 2022. doi: 10.12142/ZTECOM.202204011.

1 Introduction

In recent years, with the wide application of scene text recognition, scene text detection, as a prerequisite step of scene text recognition, has drawn more and more attention from academia and industry due to the various scales and shapes of different text instances (e.g., horizontal texts, multi-oriented texts and curved texts).

The purpose of scene text detection is to generate a proper region that can locate the corresponding text instance. In the early years of scene text detection, algorithms, usually inspired by general object detection, were designed to regress the text bounding boxes in form of rectangles or quadrangles with certain orientation. However, most of the regression-based algorithms require complex anchor design for multi-oriented text detection, which may fail when handling with text instances of complex shapes, e.g., the curved texts. In order to detect unregular text instances, segmentation-based detection, which can describe the text instance pixel-wisely, has drawn a great deal of attention. To improve the performance of segmentation-based detection, the existing methods can be roughly divided into two directions. On the one hand, several innovative models have been proposed for separating the text instances lying close to each other, such as Differentiable Binarization (DB)[1] and Progressive Scale Expansion Network (PSENet)[2]. Take PSENet[2] as an example, WANG et al. designed a progressive scale expansion network to predict the different scales of kernels for each text instance. Then a post-processing module was employed to gradually expand the minimal scale kernel to the text instance with complete shape. On the other hand, a lot of efforts are made to simplify the post-processing module for segmentation-based detection. Inspired by PSENet, a DB module introduced approximate function to binarization, which is differentiable to simplify the post-processing pipeline.

From the perspective of the label utilized for supervision, traditional segmentation-based detection algorithms, such as PSENet and DB, usually utilize shrunk text regions as training labels. The shrunk text regions could produce large margins between different text instances, which makes it effective to separate different text instances lying close to each other and thus simplify the post-processing module. However, we want to argue that pure shrunk text regions may be accompanied with at least two problems. On the one hand, there is apparent difference between a shrunk text instance and a real one, which might incur some difficulties for the convergence of conventional segmentation-based models. On the other hand, the shrunk text regions are unfriendly to small text instances since too small text regions may be ignored during the training period. In this way, it may cause

This work was supported by ZTE Industry-University-Institute Cooperation Funds under Grant No.HC-CN-20200717012.

the decrease of positive labels and result in sub-optimal detection performance.

Inspired by label enhancement (LE)[3], we utilize the idea of label distribution learning (LDL)[4] and propose a label enhancement method to overcome the problem brought by pure shrunk text labels. Moreover, following DB[1], we use removable training branches which are supervised by enhanced labels to speed up our model. Compared with the baseline, the proposed method improves the performance significantly, which achieves F-measure of 87.3% on the MSRA Text Detection 500 Database (MSRA-TD500) and 85.6% on the Total-Text dataset. In summary, there are at least three contributions of our work:

• The label distribution learning method is used for characterizing text regions.

• The label enhancement method is improved to generate labels for segmentation-based text detection.

• The performance of the proposed method is comparable to the state of the art without sacrificing the inference speed.

2 Related Work

Scene text detection has made significant progress in recent years and a large number of deep learning based methods have been proposed. Specifically speaking, those efforts can be divided into two categories: regression-based methods and segmentation-based methods.

2.1 Regression-Based Methods

Regression-based methods, inspired by general object detection initially, usually regard the regions of different text instances as bounding boxes with specific orientation. The anchor idea in general object detection was followed by Connectionist Text Proposal Network (CTPN)[5] for predicting the text slices which are then connected by a recurrent neural network. Based on CTPN[5], TextBoxes[6] modified the anchor scales and the shapes of convolutional kernels to predict the text instances with various aspect ratios. There are several representative works for multi-oriented text instances in the regression-based network. On the basis of the faster region-based convolutional neural network (R-CNN)[7], the rotation region proposal network (RRPN)[8] developed rotation proposals of the region proposal network (RPN) part to detect the text with various orientations. The deep matching prior network (DMPNet)[9] and TextBoxes++[10] found another way to apply quadrilateral regression for the detection of multi-oriented text instance. Also, Efficient and Accurate Scene Text Detector (EAST)[11] and DeepReg[12] are anchor-free methods by directly predicting the rotation angles and quadrilateral text boxes for multi-oriented text instances. However, most of regression-based networks may fall short of presenting accurate bounding boxes for the text instances with irregular shapes, which should be the basic element for scene text detection for a regression-based network.

2.2 Segmentation-Based Methods

Compared with regression-based models, segmentation-based methods can predict the proper regions for unregular text instances pixel-wisely. The pipeline of segmentation-based methods usually consists of two key parts: the first part is to make pixel-level prediction by fully convolutional networks (FCN)[13] and the second part is to convert them to proper text regions by pre-defined post-processing algorithms. ZHANG et al.[14] firstly utilized FCN to extract the text regions and then detected character candidates from these text regions by MSRA-based algorithms. Meanwhile, YAO et al.[15] utilized FCN to predict the text regions with respect to three classes: text/non-text, character classes and character linking orientations. Then, in order to distinguish different text instances lying close to each other correctly, PixelLink[16] and PSENet[2] were proposed. For PixelLink, the core idea is to replace traditional semantic segmentation by instance segmentation. While for PSENet, various kernels with different scales are utilized on different text instances to find a proper kernel with the minimal scale, and then appropriate post-processing is applied to acquire correct text instances. Recently, in order to speed up traditional segmentation-based methods to fit in real-world applications, LIAO et al.[1] proposed a DB module to avoid the complicated post-processing module during the inference stage. The DB module has two core advantages. On the one hand, DB utilizes the removable branch that can be removed during inference for simplicity. On the other hand, the ability of differentiability for the DB module can help to find the adaptive threshold for the post-processing module, which will simplify the procedure for post-processing. However, traditional DB modules only utilize shrunk text regions for supervision, which may cause sub-optimal detection performance. In order to improve the detection performance, we propose a framework that utilizes, besides shrunk text regions, the label ambiguity by adding a removable branch for LDL. The proposed framework results in better performance than the traditional ones.

3 Methodology

In this section, we will describe the proposed model in detail. Technically speaking, we firstly introduce the idea of label enhancement and the way to extend the traditional label enhancement method. Then, we present the structure of our framework including the overall pipeline and the components. After that, we describe the way to generate labels for supervision and the optimization process of the whole network.

3.1 Label Enhancement

Compared with the traditional supervised learning methods that only learn a single label or multiple logical labels, LDL[4] or deep label distribution learning (DLDL)[17] learns the distribution among all the labels. In order to overcome the challenge that most training sets only contain single or multiple logical labels instead of label distribution, the idea of label en-

hancement (LE)[3] is proposed. Formally, label enhancement can be described as below:

Given a training set $S = \{(\boldsymbol{x}_i, \boldsymbol{l}_i) | 1 \leqslant i \leqslant n\}$, where $\boldsymbol{x}_i \in \chi$ and $\boldsymbol{l}_i \in \{0, 1\}^c$, LE recovers the label distribution $\boldsymbol{d}_i$ of $\boldsymbol{x}_i$ from the logical label vector $\boldsymbol{l}_i$, and thus transforms S into a LDL training set $\mathcal{E} = \{(\boldsymbol{x}_i, \boldsymbol{d}_i) | 1 \leqslant i \leqslant n\}$.

The traditional methods proposed for label enhancement usually concentrate on an one-dimensional label such as age or emotion. However, the labels of semantic segmentation include the description of instances in two aspects: classification and localization. It is difficult for traditional LE to recover the label distribution in aspect of localization from their segmentation labels. In order to apply label distribution learning in our model, we extend traditional LE by constructing the correlated labels with respect to the localization and their semantic labels so that we can utilize multiple labels to describe one text instance in segmentation-based scene text detection. The detail of label distribution learning in our model can be found in Section 3.2 and the way to generate multiple labels in Section 3.3.

3.2 Network Design

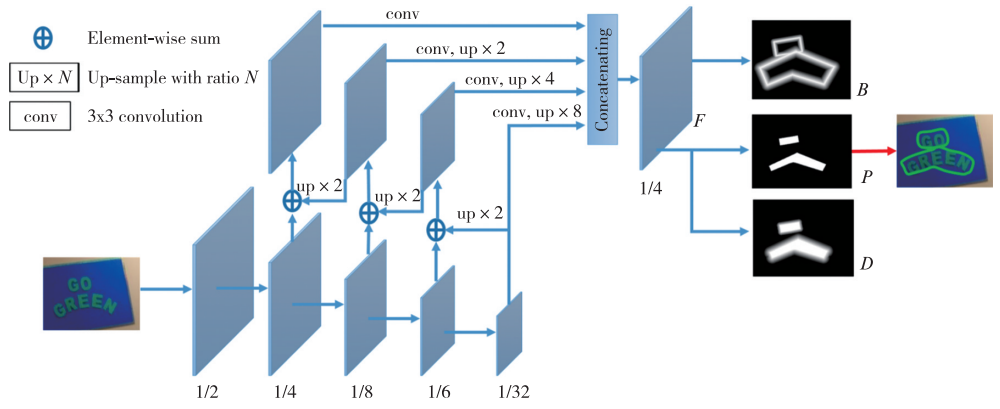
The overall pipeline of the proposed model (Fig. 1) includes two major submodules named Feature Pyramid Module and LDL Module. After an image is fed into our model, the feature pyramid module firstly processes this image as the input and the output is the fused feature map F, which consists of multiple feature maps with various scales. After that, the fused feature map F is fed into the LDL module to predict three-score maps named the probability map P, the distribution map D and the border map B by two independent FCN respectively. For these three score maps, the border map B is generated by a single FCN branch, while the probability map P and the distribution map D are generated by another single branch due to the similarity between the probability map and the distribution map. In order to speed up our model during inference, the branch to generate the distribution map D and the border map B are removable so that we could only predict the probability map P during inference phase.

The feature pyramid module, as the first core component in our model, is constructed to produce feature maps with multiple scales. Inherited from DB, this module is built based on the residual network (ResNet)[18] with stage conv3, conv4 and conv5 modulated by 3 × 3 deformable convolutional layers. For the implementation, once the feature maps are generated by conv3, conv4 and conv5 sequentially, they will be upsampled and added to the feature map in the previous stage. Then, all the added feature maps are scaled to 1/4 of the original image size and concatenated to obtain the fused feature F.

LDL[4] and DLDL[17] utilize constrained weights as the description degree of correlated labels to deal with the label ambiguity, which can also be viewed as weight normalization of correlated labels. In the training period, we utilize the labels to calculate training losses. Thus the weighted labels are actually a kind of weighted loss in loss calculation with labels. Based on this idea, the architecture of the LDL module in our model has only two FCN branches. Each FCN branch is stacked with one 3×3 convolutional layer and two transposed convolutional layers with BatchNorm and rectified at both the linear activation function (ReLU) layers inserted into the convolutional layers and Softmax layers utilized to generate the score maps at the end of FCN.

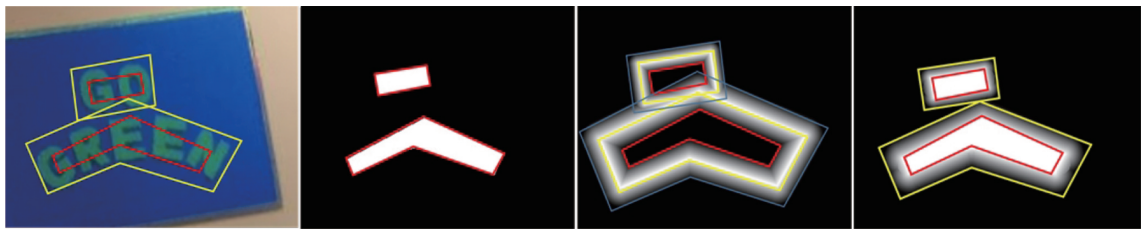
3.3 Label Generation

In order to perform label distribution learning in our model, there are at least three correlated labels utilized during the training phase for the three kinds of score maps named the probability map P, distribution map D and border map B, as shown in Fig. 2. The label generation for the probability map is inspired by DB[1]. Given an original text polygon label G,



Notes: The red arrow stands for the inference phase. "1/2", "1/4", ... and "1/32" indicate the scale ratios compared to the input image.
B: Border map *D*: Distribution map *F*: Fused feature *P*: Probability map

▲**Figure 1. Overall pipeline of the proposed network**



Notes: The red line is G_s, the yellow line is G, and the blue line is G_d.

▲ **Figure 2. Label generation for text regions: (a) training image; (b)probability map; (c)border map; (d)distribution map**

the shrunk text region is generated by shrinking G to G_s. The shrinking offset D is calculated from the polygon perimeter L and its area A via the Vatti clipping algorithm:

$$D = \frac{A(1 - r^2)}{L}, \tag{1}$$

where r is the shrink ratio that is set to 0.4 empirically. In order to generate the corresponding labels for the distribution map, inspired by DLDL[17], the distance map is generated by Eq. 2 with each value representing a description degree for the pixel to be positive. Then the distribution map is generated by adding the distance map to the probability map pixel-wisely.

$$\text{distance}(i,j) = \begin{cases} 0, & G(i,j) = 0 \\ 1, & G_s(i,j) = 1 \\ \dfrac{\text{dist}(i,j,G)}{\text{dist}(G,G_s)}, & \text{otherwise} \end{cases}, \tag{2}$$

where $G(i,j)$ and $G_s(i,j)$ represent the pixel values for row i and column j in the corresponding maps G and G_s respectively, and $\text{dist}(i,j,G)$ represents the minimal distance between pixel (i,j) and the border of G. On the basis of $\text{dist}(i,j,G)$, $\text{dist}(G,G_s)$ represents the distance between the borders of G and G_s with respect to the direction to obtain $\text{dist}(i,j,G)$. For the border map, we firstly dilate G to G_d with the same scale D. Then two distance maps can be produced from G_s and G_d to G. Finally, the border map can be obtained by adding the two distance maps pixel by pixel.

3.4 Optimization

The loss function L in our model can be formulated as a weighted sum of the loss for three score maps, namely the loss for the probability map L_s, the loss for the distribution map L_d and the loss for the border map L_b:

$$L = \alpha \times L_s + L_d + L_b, \tag{3}$$

where α is empirically set to 2.0 in order to give more prominence to the probability map whose ground truths are directly generated by the logical ground truth. Similar weight has been used in PSENet[2] for the probability map and its original logical ground truth. Following DB[1], we use the binary cross-entropy (BCE) loss in both L_s and L_d. To overcome the imbalanced distribution of positives and negatives, hard negative mining is applied to the BCE loss. To deal with the unbalance of the text and non-text regions, we only compute the loss inside the dilated text polygon G_d. L_s and L_d are formulated as follows:

$$L_s = L_d = \sum_{i \in R_s} y_i \log_2 x_i + (1 - y_i)\log(1 - x_i), \tag{4}$$

where R_s indicates the selected region. The ratio of positives and negatives is 1:3. We apply L_1 loss for L_b, which is computed inside the dilated text polygon G_d:

$$L_b = \sum_{i \in R_d} \left| y_i^* - x_i^* \right|, \tag{5}$$

where R_d indicates the selected region of dilated polygon G_d and y^* is the label for the border map.

4 Experiments

In this section, we will demonstrate the effectiveness of our framework by extensive experiments. We first introduce prevalent datasets for scene text detection briefly and then present the implementation of the proposed model. Ablation studies are also conducted to verify the effectiveness of our architecture. Finally, we compare our model with the existing state-of-the-art methods on several benchmarks, such as ICDAR MLT-2017 dataset, Total-Text, MSRA-TD500 dataset and ICDAR-2015 dataset, to show the success of our model.

4.1 Datasets

ICDAR MLT-2017 dataset[19] is a multi-language dataset consisting of 7 200 training images, 1 800 validation images and 9 000 testing images. Following DB[1], we utilize the training and validation set to pre-train our model.

Total-Text[20] is a classical dataset which contains sufficient

text instances with arbitrary shapes, such as the curved text. In detail,1 255 images and 300 testing images are utilized for training and testing respectively with each text instance labelled with word-level annotation by polygon.

MSRA-TD500 dataset[21] is another multi-language dataset with English and Chinese scripts. It consists of 300 training images and 200 testing images with each text instance multi-oriented and labelled in the text-line level. For a better comparison with the previous methods, extra 400 training images from HUST-TR400 are included during our experiments.

ICDAR-2015 dataset[22] is the most commonly used benchmark featured by abundant text instances with various orientations. Since all the images are collected by Google glasses without considering image quality, position or viewpoints, all the text instances are more challenging for detection due to various brightness, scales and viewpoints. There are 1 000 images for training and 500 images for inference in this dataset with each text instance labelled with word-level annotation.

4.2 Implementation Details

During the implementation, ResNet is chosen as the backbone of the proposed model and trained on the ImageNet dataset. All models are pre-trained on the MLT-2017 dataset for 100 000 iterations and finally fine-tuned on the corresponding real-world dataset for 1 200 epochs. The hardware utilized in our experiments is only a single Titan RTX GPU. For the optimizer in our model, we choose Stochastic Gradient Descent (SGD) with the batch size 8, momentum 0.9 and weight decay 0.000 1. In addition, following DB[1], we utilize a poly learning rate strategy in which the current learning rate is calculated by $r_{\text{init}} \times \left(1 - \text{iter}/\max_{\text{iter}}\right)^{\text{power}}$, where the initial learning rate r_{init} and power is set to 0.007 and 0.9 respectively.

4.3 Ablation Study

We conduct an ablation study on the MSRA-TD500 to verify the effectiveness of our proposed method. We take the model which is only supervised by the probability map label as our baseline. The results are shown in Table 1.

As shown in the table, our proposed method enhances the performance considerably for both ResNet-18 and ResNet-50 backbones on the MSRA-TD500 dataset. For the ResNet-18 backbone, the training with additional distribution map (Dis) and that with additional distribution and border maps (Dis+Bor) achieve 2.9% and 3.2% performance gain in terms of F-measure respectively. For the ResNet-50, they consistently bring 1.7% and 2.2% improvements respectively. Both of the enhanced labels can boost the detection performance significantly.

4.4 Comparisons with Previous Methods

In this section, we will verify the proposed method on three standard benchmarks including the MSRA-TD500, Total-Text and ICDAR-2015 datasets by comparing the results with previous state-of-the-art methods.

▼ **Table 1. Ablation study results with different settings on MSRA-TD500 dataset**

Method	Precision/%	Recall/%	F-measure/%
ResNet-18	84.7	77.0	80.6
ResNet-18 + Dis	86.5	80.6	83.5
ResNet-18 + Dis + Bor	88.1	79.9	83.8
ResNet-50	90.5	77.9	83.7
ResNet-50 + Dis	90.9	80.6	85.4
ResNet-50 + Dis + Bor	**93.8**	**81.7**	**87.3**

Bor: training with the border map ResNet: residual network
Dis: training with additional distribution map

1) Curved text detection

Following DB, we firstly pre-train our model on the MLT-2017 dataset for 100 000 iterations and then fine-tune it on the Total-Text for 1 200 epochs. The comparison results between our model and the previous methods are listed in Table 2, where we can conclude at least three highlights for our methods:

• Compared with the baseline DB, our model achieves better result considering F-measure consistently, which can verify the effectiveness of our model.

• The precision of our model outperforms current state-of-the-art methods by a large margin. Combining the results in Tables 1 and 2, we think the reason for the improvement is that label ambiguity is utilized by label distribution learning based on the enhanced label in our method, especially for the border map during the training phase.

• Our model achieves comparable performance to the existing state-of-the-art methods according to F-measure.

2) Multi-language text detection

We also evaluate the proposed method on the MSRA-TD500 to test its ability for multi-language text detection. As shown in Table 3, our method based on the ResNet-50 backbone achieves an F-measure of 87.3%, surpassing the sate-of-the-art methods by more than 1.2%.

3) Multi-oriented text detection

In order to verify the generalization ability for the proposed method on multi-oriented scene text detection, we evaluate our network on the ICDAR-2015, a traditional dataset featured by multi-oriented text instances. The comparison results are listed in Table 4. As shown in the table, our model achieves higher precision than the previous state-of-the-art methods except Corner[23] whose recall is too low to fit in the real-world applications, which verifies our model can overcome false positives effectively. Take F-measure into account, our performance is still comparable to the previous state-of-the-art methods, although the relatively lower recall drags down our F-measure. This indicates the effectiveness of the proposed method with respect to multi-oriented scene text detection.

▼Table 2. Detection results on Total-Text dataset

Method	Precision/%	Recall/%	F-measure/%
TextSnake[24]	82.7	74.5	78.4
ATRR[25]	80.9	76.2	78.5
Mask TextSpotter[26]	82.5	75.6	78.6
TextField[27]	81.2	79.9	80.6
LOMO*[28]	87.6	79.3	83.3
CRAFT[29]	87.6	79.9	83.6
CSE[30]	81.4	79.1	80.2
PSENet-1s[2]	84.0	78.0	80.9
TextFuseNet-ResNet-50[31]	83.2	87.5	85.3
DB-ResNet-50 (800)[1]	87.1	82.5	84.7
Ours-ResNet-50 (800)	89.1	82.4	85.6

Note: The values in the bracket mean the height of the input images and "*" indicates testing with multiple scales.
ATRR: Adaptive Text Region Representation
CRAFT: Character Region Awareness for Text Detection
CSE: Conditional Spatial Expansion
DB: differentiable binarization
LOMO: Look More than Once
PSENet: Progressive Scale Expansion Network
ResNet: residual network

▼Table 3. Detection results on MSRA-TD500 dataset

Method	Precision/%	Recall/%	F-measure/%
Text-CNN[32]	71	61	69
DeepReg[12]	77	70	74
RRPN[8]	82	68	74
RRD[33]	87	73	79
MCN[34]	88	79	83
PixelLink[16]	83	73.2	77.8
Corner[23]	87.6	76.2	81.5
TextSnake[24]	83.2	73.9	78.3
Scene text detection with bootstrapping and semantics-aware text border techniques[35]	83.0	77.4	80.1
MSR[36]	87.4	76.7	81.7
CRAFT[29]	88.2	78.2	82.9
SAE[37]	84.2	81.7	82.9
DB-ResNet-50 (736)[1]	91.5	79.2	84.9
An accurate segmentation-based detector[38]	88.8	83.5	86.1
Ours-ResNet-50 (736)	93.8	81.7	87.3

Note: The values in the bracket mean the height of the input images.
CRAFT: Character Region Awareness for Text Detection
CSE: Conditional Spatial Expansion
DB: differentiable binarization
MCN: Markov Clustering Network
MSR: Multi-Scale Shape Regression Network
ResNet: residual network
RRD: Rotation-Sensitive Regression Detector
RRPN: Rotation Region Proposal Network
SAE: shape-aware embedding
Text-CNN: Text-Attentional Convolutional Neural Network

5 Conclusions

In this paper, we propose a label distribution learning method for text region detection. The label enhancement is used to construct two kinds of training labels for segmentation-based scene text detection. The experimental results on benchmarks demonstrate that the proposed method can consistently improve the model performance without sacrificing the inference speed. In the future, we will try to construct enhanced labels for different applications in text detection.

▼Table 4. Detection results on the ICDAR-2015 dataset.

Method	Precision/%	Recall/%	F-measure/%
CTPN[5]	74.0	52.0	61.0
Corner[23]	94.1	70.7	80.7
PSENet-1s[2]	86.9	84.5	85.7
TextBoxes++[10]	87.8	78.5	82.9
PixelLink[16]	85.5	82.0	83.7
LOMO*[28]	91.3	83.5	87.2
An accurate segmentation-based detector[38]	90.0	85.1	87.5
CRAFTS[39]	89.0	85.3	87.1
DB-Resnet50 (1 152)[1]	91.8	83.2	87.3
An end-to-end trainable network (ResNet50)[40]	89.3	85.7	87.5
Ours-ResNet50 (1 152)	92.4	83.8	87.8

Note: The values in the bracket mean the height of the input images and "*" indicates testing with multiple scales.
CRAFTS: Character Region Attention for Text Spotting
CTPN: Connectionist Text Proposal Network
DB: differentiable binarization
LOMO: Look More than Once
PSENet: Progressive Scale Expansion Network
ResNet: residual network

References

[1] LIAO M H, ZOU Z S, WAN Z Y, et al. Real-time scene text detection with differentiable binarization and adaptive scale fusion [J]. IEEE transactions on pattern analysis and machine intelligence, 2022, early access. DOI: 10.1109/TPAMI.2022.3155612
[2] WANG W H, XIE E Z, LI X, et al. Shape robust text detection with progressive scale expansion network [C]//Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2019: 9336 – 9345
[3] XU N, LIU Y P, GENG X. Label enhancement for label distribution learning [J]. IEEE transactions on knowledge and data engineering, 2021, 33(4): 1632 – 1643. DOI: 10.1109/TKDE.2019.294704020
[4] GENG X, YIN C, ZHOU Z H. Facial age estimation by learning from label distributions [J]. IEEE transactions on pattern analysis and machine intelligence, 2013, 35(10): 2401 – 2412. DOI: 10.1109/TPAMI.2013.51
[5] TIAN Z, HUANG W L, HE T, et al. Detecting text in natural image with connectionist text proposal network [C]//European Conference on Computer Vision. Springer, 2016: 56 – 72. DOI: 10.1007/978-3-319-46484-8_4
[6] LIAO M, SHI B, BAI X. Textboxes: a fast text detector with a single deep neural network [C]//Thirty-First AAAI Conference on Artificial Intelligence. AAAI, 2017. DOI: 10.1609/aaai.v31i1.11196
[7] REN S Q, HE K M, GIRSHICK R, et al. Faster R-CNN: towards real-time object detection with region proposal networks [J]. IEEE transactions on pattern analysis and machine intelligence, 2017, 39(6): 1137 – 1149. DOI: 10.1109/TPAMI.2016.2577031
[8] MA J Q, SHAO W Y, YE H, et al. Arbitrary-oriented scene text detection via rotation proposals [J]. IEEE transactions on multimedia, 2018, 20(11): 3111 – 3122. DOI: 10.1109/TMM.2018.2818020
[9] LIU Y L, JIN L W. Deep matching prior network: toward tighter multi-oriented text detection [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2017: 3454 – 3461. DOI: 10.1109/CVPR.2017.368
[10] LIAO M H, SHI B G, BAI X. TextBoxes++: a single-shot oriented scene text

detector [J]. IEEE transactions on image processing, 2018, 27(8): 3676 – 3690. DOI: 10.1109/TIP.2018.2825107
[11] ZHOU X, YAO C, WEN H, et al. East: an efficient and accurate scene text detector [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2017: 2642 – 2651. DOI: 10.1109/CVPR.2017.283
[12] HE W H, ZHANG X Y, YIN F, et al. Deep direct regression for multi-oriented scene text detection [C]//IEEE International Conference on Computer Vision. IEEE, 2017: 745 – 753. DOI: 10.1109/ICCV.2017.87
[13] LONG J, SHELHAMER E, DARRELL T. Fully convolutional networks for semantic segmentation [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2015: 3431 – 3440. DOI: 10.1109/CVPR.2015.7298965
[14] ZHANG Z, ZHANG C, SHEN W, et al. Multi-oriented text detection with fully convolutional networks [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2016, pp. 4159 – 4167. DOI: 10.1109/CVPR.2016.451
[15] YAO C, BAI X, SANG N, et al. Scene text detection via holistic, multi-channel prediction [EB/OL]. (2016-07-05) [2021-06-01]. https://arxiv. org/abs/1606.09002
[16] DENG D, LIU H F, LI X L, et al. Pixellink: detecting scene text via instance segmentation [C]//Thirty-Second AAAI Conference on Artificial Intelligence. AAAI, 2018. DOI: 10.1609/aaai.v32i1.12269
[17] GAO B-B, XING C, XIE C-W, et al. Deep label distribution learning with label ambiguity [J]. IEEE transactions on image processing, 2017, 26(6): 2825 – 2838. DOI: 10.1109/TIP.2017.2689998
[18] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2016: 770 – 778. DOI: 10.1109/CVPR.2016.90
[19] NAYEF N, YIN F, BIZID I, et al. ICDAR2017 robust reading challenge on multi-lingual scene text detection and script identification-RRC-MLT [C]//14th IAPR International Conference on Document Analysis and Recognition (ICDAR). IAPR, 2017: 1454 – 1459. DOI: 10.1109/ICDAR.2017.237
[20] CHNG C K, CHAN C S. Total-text: a comprehensive dataset for scene text detection and recognition [C]//14th IAPR International Conference on Document Analysis and Recognition (ICDAR). IAPR, 2017: 935 – 942. DOI: 10.1109/ICDAR.2017.157
[21] YAO C, BAI X, LIU W Y, et al. Detecting texts of arbitrary orientations in natural images [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2012: 1083 – 1090. DOI: 10.1109/CVPR.2012.6247787
[22] KARATZAS D, GOMEZ-BIGORDA L, NICOLAOU A, et al. ICDAR 2015 competition on robust reading [C]//13th International Conference on Document Analysis and Recognition (ICDAR). IEEE, 2015: 56 – 1160. DOI: 10.1109/ICDAR.2015.7333942
[23] LYU P Y, YAO C, WU W H, et al. Multi-oriented scene text detection via corner localization and region segmentation [C]//IEEE Conference on Computer Vision and Pattern Recognition, IEEE, 2018: 7553 – 7563. DOI: 10.1109/CVPR.2018.00788
[24] LONG S B, RUAN J Q, ZHANG W J, et al. TextSnake: a flexible representation for detecting text of arbitrary shapes [C]//European Conference on Computer Vision. Springer, 2018: 20 – 36. DOI: 10.1007/978-3-030-01216-8_2
[25] WANG X B, JIANG Y Y, LUO Z B, et al. Arbitrary shape scene text detection with adaptive text region representation [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2019: 6442 – 6451. DOI: 10.1109/CVPR.2019.00661
[26] LYU P Y, LIAO M H, YAO C, et al. Mask TextSpotter: An end-to-end trainable neural network for spotting text with arbitrary shapes [C]//European Conference on Computer Vision. Springer, 2018: 67 – 83. DOI: 10.1007/978-3-030-01264-9_5
[27] XU Y C, WANG Y K, ZHOU W, et al. TextField: learning a deep direction field for irregular scene text detection [J]. IEEE transactions on image processing, 2019, 28(11): 5566 – 5579. DOI: 10.1109/TIP.2019.2900589
[28] ZHANG C Q, LIANG B R, HUANG Z M, et al. Look more than once: an accurate detector for text of arbitrary shapes [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2019: 10544 – 10553. DOI: 10.1109/CVPR.2019.01080
[29] BAEK Y, LEE B, HAN D, et al. Character region awareness for text detection [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2019: 9357 – 9366. DOI: 10.1109/CVPR.2019.00959
[30] LIU Z C, LIN G S, YANG S, et al. Towards robust curve text detection with conditional spatial expansion [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2019: 7261 – 7270. DOI: 10.1109/CVPR.2019.00744
[31] YE J, CHEN Z, LIU J H, et al. Textfusenet: scene text detection with richer fused features [C]//Twenty-Ninth International Joint Conference on Artificial Intelligence. IJCAI, 2020: 516 – 522. DOI: 10.24963/ijcai.2020/72
[32] HE T, HUANG W L, QIAO Y, et al. Text-attentional convolutional neural network for scene text detection [J]. IEEE transactions on image processing, 2016, 25(6): 2529 – 2541. DOI: 10.1109/TIP.2016.2547588
[33] LIAO M H, ZHU Z, SHI B G, et al. Rotation-sensitive regression for oriented scene text detection [C]//IEEE Conference on Computer Vision and Pattern Recognition. IEEE, 2018: 5909 – 5918. DOI: 10.1109/CVPR.2018.00619
[34] LIU Z, LIN G, YANG S, et al. Learning markov clustering networks for scene text detection [C]//IEEE Conference on Computer Vision and Pattern Recognition. IEEE, 2018. DOI: 10.1109/CVPR.2018.00725
[35] XUE C H, LU S J, ZHAN F N. Accurate scene text detection through border semantics awareness and bootstrapping [C]//European Conference on Computer Vision. Springer, 2018: 355 – 372. DOI: 10.1007/978-3-030-01270-0_22
[36] XUE C H, LU S J, ZHANG W. MSR: multi-scale shape regression for scene text detection [EB/OL]. (2019-01-09) [2021-06-01]. https://arxiv. org/abs/1901.02596
[37] TIAN Z T, SHU M, LYU P Y, et al. Learning shape-aware embedding for scene text detection [C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2019: 4229 – 4238. DOI: 10.1109/CVPR.2019.00436
[38] LIU X, ZHOU G J, ZHANG R, et al. An accurate segmentation-based scene text detector with context attention and repulsive text border [C]//IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). IEEE, 2020: 2344 – 2352. DOI: 10.1109/CVPRW50498.2020.00283
[39] BAEK Y, SHIN S, BAEK J, et al. Character region attention for text spotting [C]//European Conference on Computer Vision. Springer, 2020: 504 – 521. DOI: 10.1007/978-3-030-58526-6_30
[40] QIN S, BISSACCO A, RAPTIS M, et al. Towards unconstrained end-to-end text spotting [C]//IEEE International Conference on Computer Vision. IEEE, 2019: 4704 – 4714. DOI: 10.1109/ICCV.2019.00480

Biographies

MEI Junjun is a chief R&D engineer of ZTE Corporation in the field of audio and video, engaged in the research of the overall architecture of the integrated video cloud network and key technologies such as computer vision, audio and video coding, and audio and video transmission. He has presided over the R&D and design of a number of system solutions.

GUAN Tao (guan.tao@zte.com.cn) is the senior system architect of ZTE Corporation, mainly engaged in the architecture design and algorithm research of video systems and industrial digital systems. He has participated in standard organizations, initiated and compiled the formulation of a number of communication standards, and applied for more than 20 national invention patents.

TONG Junwen received his BE and ME degrees in control science and engineering from Nanjing University, China in 2017 and 2020, respectively. He now works with ZTE Corporation. His current research interests include object detection, semantic segmentation and optical character recognition in industrial scenarios.

A Content-Aware Bitrate Selection Method Using Multi-Step Prediction for 360-Degree Video Streaming

GAO Nianzhen[1], YU Yifang[2], HUA Xinhai[2], FENG Fangzheng[1], JIANG Tao[1]

(1. Huazhong University of Science and Technology, Wuhan 430074, China;
2. ZTE Corporation, Shenzhen 518057, China)

DOI: 10.12142/ZTECOM.202204012

https: //kns.cnki.net/kcms/detail/34.1294.TN.20221026.1118.002.html, published online October 26, 2022

Manuscript received: 2021-12-12

Abstract: A content-aware multi-step prediction control (CAMPC) algorithm is proposed to determine the bitrate of 360-degree videos, aiming to enhance the quality of experience (QoE) of users and reduce the cost of video content providers (VCP). The CAMPC algorithm first employs a neural network to generate the content richness and combines it with the current field of view (FOV) to accurately predict the probability distribution of tiles being viewed. Then, for the tiles in the predicted viewport which directly affect QoE, the CAMPC algorithm utilizes a multi-step prediction for future system states, and accordingly selects the bitrates of multiple subsequent steps, instead of an instantaneous state. Meanwhile, it controls the buffer occupancy to eliminate the impact of prediction errors. We implement CAMPC on players by building a 360-degree video streaming platform and evaluating other advanced adaptive bitrate (ABR) rules through the real network. Experimental results show that CAMPC can save 83.5% of bandwidth resources compared with the scheme that completely transmits the tiles outside the viewport with the Dynamic Adaptive Streaming over HTTP (DASH) protocol. Besides, the proposed method can improve the system utility by 62.7% and 27.6% compared with the DASH official and viewport-based rules, respectively.

Keywords: DASH; content-aware FOV prediction; bitrate adaptation; multi-step prediction; generalized predictive control

Citation (IEEE Format): N. Z. Gao, Y. F. Yu, X. H. Hua, et al., "A content-aware bitrate selection method using multi-step prediction for 360-degree video streaming," *ZTE Communications*, vol. 20, no. 4, pp. 96 – 109, Dec. 2022. doi: 10.12142/ZTECOM.202204012.

1 Introduction

With the rapid development of 5G technologies, the immersive viewing experience led by Virtual Reality (VR) is becoming increasingly popular. The 360-degree video, which is one of the most critical portions of VR applications, has attracted a good deal of attention on some commercial streaming platforms, such as Youtube and Bilibili. Although the 360-degree video brings a brand-new experience to users, it confronts new challenges as well. Compared with conventional 2D video streaming, the delivery of 360-degree video has much more bandwidth requirements due to its panorama feature.

Driven by the characteristic of the user field of view (FOV), researchers are exploring a solution that spatially divides a 360-degree video into small parts called tiles and transmits them in different video qualities to cope with the large consumption of bandwidth. In addition, benefitting from the Dynamic Adaptive Streaming over HTTP (DASH) Protocol, adaptive bitrate (ABR) algorithms have made an enormous contribution to video streaming, especially over dynamic wireless network conditions. By pre-coding the video into multi-bitrate, the client may request video segments of different qualities to meet the challenge of network fluctuations.

Therefore, tile-based hyper text transfer protocol (HTTP) adaptive streaming is a promising approach to achieving a better quality of experience (QoE) in a 360-degree video streaming system. The HTTP server usually crops the panoramic video into multiple tiles spatially, and then slices and encodes each tile into multi-bitrate segments. The client requests the most appropriate bitrate version of each tile based on his viewport and current network status, decodes these tiles, and then renders them into a 360-degree video for playback. In general, the tile that overlaps viewports is delivered in high quality, while other tiles outside the FOV are delivered in lower quality. Due to the human visual characteristics, the user can only see the FOV areas, so a significant reduction in the video bitrate outside the viewport will not affect the users' experience; on the contrary, it can save bandwidth and transmission costs, and avoid net-

This work was supported in part by ZTE Corporation under Grant No. 2021420118000065.

work congestion in the case of multiple users.

In fact, due to the randomness of the user's viewing angle and wireless network bandwidth, the low prediction accuracy will lead to an inappropriate bitrate version selected by the tiles in the viewport. To handle these prediction errors, the QoE is guaranteed by delivering tiles around the prediction viewport at high quality and keeping the buffer at a reasonable range without stopping the playback waiting buffer. In order to reasonably allocate the wireless network bandwidth resources, it is necessary to estimate the future viewport distribution and network state, and determine the bitrate version of the prefetched segments that match the overall network capacity.

Specifically, we propose a bandwidth resource scheduling algorithm content-aware multi-step predictive control (CAMPC) for 360-degree video streaming, which uses an online predictor to obtain throughput estimation. The content perception score obtained by the offline machine learning method and online user viewport trace is used to predict the probability distribution of future user viewport locations. For tiles with high viewport probability, the change of buffer occupation in the next period is predicted based on the throughput estimation. The bitrate decision is made by optimizing the predicted QoE within the viewport and the future buffer occupancy prediction. The remaining total bandwidth will be distributed according to the distribution probability for tiles with low viewport probability. The main contributions are shown as follows.

• We develop a content-aware method to predict the user's viewport location. The grayscale image is obtained by a trained semantic segmentation model with each frame of the video after spatial partition as input, and the numbers of different grayscale pixels are calculated to obtain the content richness of the current frame. Since users prefer to view the frame with richer content, the probability distribution of future viewing is obtained by the weighted content richness with the current user viewport.

• We propose a multi-step predictive bitrate adaptation algorithm to generate prospective bitrate decisions for players with high probability in the future viewport, which includes predicting network throughput using the Kalman filter, predicting buffer occupation, and solving predictive control problems using the generalized predictive control method.

• We provide experimental tests by building a 360-degree video streaming platform to implement the proposed bandwidth resource scheduling algorithm and evaluate the network status algorithm through the practical network. Experimental results show that compared with the existing online bandwidth resource scheduling algorithms, the proposed algorithm can save bandwidth while ensuring the quality of user experience. Compared with the complete transmission of 360-degree videos, the bandwidth can be saved by 83.5% in the tiles out of the viewport, and the CAMPC can improve the system utility by 62.7% and 27.6% compared with low-on-latency-plus (LOLP) and DYNAMIC solutions which have been integrated to the official DASH.js player in v3.2.0 and the most straightforward viewport-based bitrate adaptation algorithm.

The rest of the paper is organized as follows. Section 2 surveys related work on a tile-based 360-degree video streaming over DASH. Section 3 presents the system structure and QoE model for evaluation. Section 4 proposes the FOV prediction algorithm combining FOV and content priority. The bandwidth prediction and the bitrate selection algorithm are in Section 5. Section 6 describes the system implementation and throughput measurement in reality besides the performance evaluation. Finally, Section 7 concludes the paper and outlines future directions.

2 Background and Motivation

The 360-degree video is constructed by camera splicing. To play a 360-degree video, the client needs to run on a custom 360-degree video player or head-mounted displays (HMDs) to render the video. Some commercial 360-degree video content providers usually employ a simple approach that streams the entire panoramic content regardless of the viewport[1], such as the widely used equirectangular projection (ERP) format, which causes considerable waste of wireless bandwidth resource, as users always pay attention to only a tiny portion of the panoramic scene in their viewports.

Inspired by these observations, several studies have abandoned traditional flat video transmission methods and begun to propose tile-based solutions that adaptively fetch only the content inside the predicted FOV or fetch the content in FOV with higher quality than the parts out of FOV to meet the demand of 360-degree video streaming systems. XIE et al.[2] leveraged a probabilistic approach to prefetch tiles countering viewport prediction errors, apparently reduced the side effects caused by wrong head movement prediction, and designed a QoE-driven viewport adaptation system. QIAN et al.[3] adopted a viewport-adaptive approach and formulated an optimization algorithm to determine the tile quality, achieving high bandwidth reduction and video quality enhancement on Long Term Evolution (LTE). SONG et al.[4] proposed a two-tier streaming architecture using scalable video coding (SVC) techniques, which included two layers, namely, the basic layer (BL) and the enhanced layer (EL). In contrast, a fast-switching strategy was proposed by generating multiple video streams with different start times for each encoded enhanced layer chunk, which can be randomly accessed at any instant to adapt to the user viewport change immediately to achieve the optimal trade-off between video quality and streaming robustness.

According to the above research, tile-based 360-degree video transmission methods have been proven to save many bandwidth resources, whereas viewport prediction and bandwidth prediction are two of the most critical factors. To a great extent, the user's FOV would be influenced by the video content. Conventional viewport prediction approaches pay atten-

tion to the past viewing behavior of many users who have watched the same or similar videos, based on the head movement trajectory in the dataset. SUN et al.[5] developed a truncated linear prediction method by which we only use past samples that are monotonically increasing or decreasing for extrapolation. EPASS360[6] studied the similarity of multi-user viewing spatial locations, looking for similarities in patterns across a wide range of data through a deep learning LSTM network. These approaches apply only to the video on demand (VOD) case because the past viewing behavior is not available for live video streaming for the first time. The Pano[7] drew researchers' attention to the content of the video. FENG et al.[8] developed a new viewport prediction scheme for live 360-degree video streaming using video content-based motion tracking and dynamic user interest modeling. QIAO et al.[9] studied human attention over the viewport of 360-degree videos and proposed a novel visual saliency model to predict fixations over 360 videos through the multi-task deep neural networks (DNN) method. YUAN et al.[10] proposed a simple yet effective rate adaptation algorithm to determine the requested bitrate for downloading the current video segment and preserved both the quality and the smoothness of tiles in FoV. WEI et al.[11] proposed a hybrid control scheme presented for segment-level continuous bitrate selection and tile-level bitrate allocation for 360-degree streaming over mobile devices to increase users' quality of experience.

On the other hand, to optimize QoE in the DASH video streaming system, the bitrates decided by the client-side ABR algorithm should meet the bandwidth requirements. Throughput-based methods often employ various mechanisms to predict the end-to-end available bandwidth, such as Exponential Weighted Moving Average (EWMA) and Support Vector Regression. The estimation accuracy of throughput will affect the allocation decision. SOBHANI et al.[12] utilized Autoregressive-Moving-Average (ARMA)[13] and Generalized Autoregressive Conditional Heteroscedastic (GARCH) in order to predict the average and the variance of bandwidth. YUAN et al.[14] proposed an ensemble rate adaptation framework for DASH, which aims to leverage the advantages of multiple methods involved in the framework to improve the QoE of users. The buffer-based algorithm, such as BOLA[15], formulated bitrate adaptation as a utility maximization problem, devised an online control algorithm, and used Lyapunov optimization techniques to minimize rebuffering and maximize video quality.

However, to achieve a fast and smooth response among multiple players of the 360-degree video at the same time, ABR algorithms should quickly adapt to sustainable changes while avoiding the bit rate jitter caused by sudden throughput changes. Existing methods are inherently unable to achieve this goal because they cannot determine whether a current change is transient or persistent with a single step of predictive information. Thus, our work uses the idea of combining content awareness with the current viewport to calculate the viewing probability of spatial video blocks and provides efficient network state quantification and prediction algorithms.

3 Proposed Framework

3.1 System Architecture

As shown in Fig. 1, the framework of the 360-degree video transmission system consists of a server and a set of video players. The server includes a preprocessing module and a sending module. The preprocessing module converts a 360-degree video from the ERP format to the Cubemap Projection (CMP) and separates it into six tiles spatially so that each tile corresponds to a cube map. Then each tile is divided into a set of temporal segments and encoded at different bitrate levels according to DASH, and the information which describes the structure of bitrate representations for each tile is stored in the media presentation description (MPD). The sending module sends the segments at a specific bitrate selected by the ABR controller of the player.

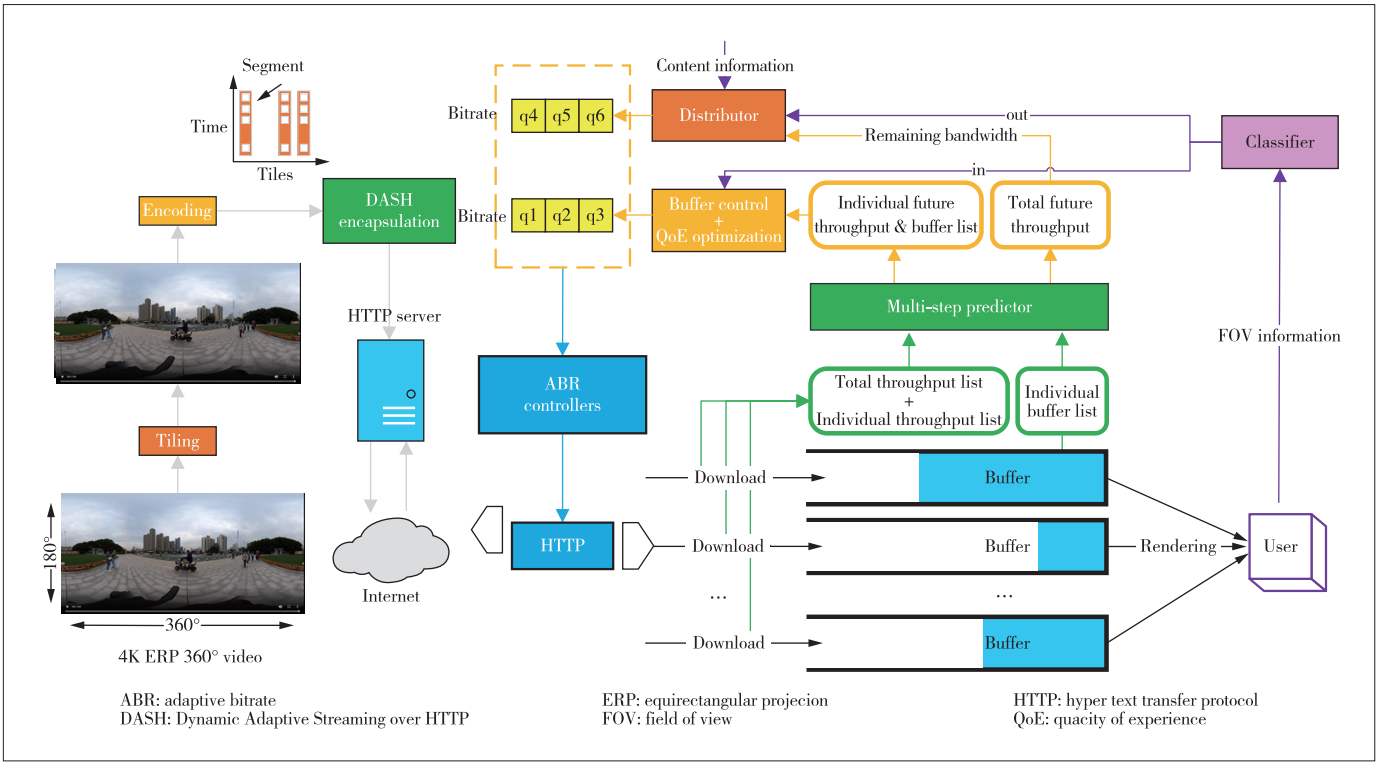
The client includes a receiving module, video players, a system monitor, multi-step predictors, and bitrate decision engines. The receiving module receives and decodes the tiles to reconstruct the 360-degree video. Players extract and display the viewport corresponding to the current viewing direction of the user. The system monitor is responsible for monitoring the viewport, network status (e.g., throughput), and player status (e.g., buffer occupancy). Multi-step predictors and bitrate decision engines assist ABR controllers to compute the bitrate level of the next segment and return it to the server. Each multi-step predictor module calculates the future throughput through the network status, and the bitrate decision engines obtain the bitrate level by optimizing the target based on the multi-step throughput and buffer occupancy prediction.

3.2 Problem Formulation

The server divides a 360-degree video into N tiles of the same size in space corresponding to a cube map, and each tile V is initialized to a DASH player. Then, each tile is sliced into $M \times K$ segments, indicating that there are M optimal bitrate versions divided into K segments in time, and each segment has the exact duration of L seconds. The system encapsulates and stores $N \times M \times K$ segments in an HTTP server for adaptive streaming.

The serial number of the tile V is represented by i, where $i \in \mathbb{Z}$. V^{in} and V^{out} indicate that the current tile is located inside and outside the viewport, respectively. For V^{in}, the quality of experience is determined by three factors: the selected bitrate version, the bitrate fluctuation range, and the rebuffering time. Spatial tiles that are not in the viewport will not affect QoE. For this reason, the value of QoE is given by:

$$\phi(V_i) = \sum_{k=1}^{K} r(V_{i,k}^{\text{in}}) - \sum_{k=1}^{K-1} \left| r(V_{i,k+1}^{\text{in}}) - r(V_{i,k}^{\text{in}}) \right| - \mu \sum_{k=1}^{K} T_{V_{i,k}^{\text{in}}}, \quad (1)$$



▲**Figure 1. Streaming video system structure**

where $r(V_{i,k}^{in})$ is the bitrate version when the player V_i starts to download chunk $V_{i,k}^{in}$, $T_{v_{i,k}}$ is the rebuffering time of chunk $V_{i,k}^{in}$, and μ is the rebuffering penalty which is generally set to $\mu = 4.3$.

The system ensures that the bandwidth is saved as much as possible when the QoE is the highest. The system utility includes the QoE and the bandwidth consumed compared with the situation where players request all chunks at the highest bitrate, which is:

$$\phi(V) = \omega_u \sum_{\substack{V_i \in V^{in} \\ i=1}}^{N} \alpha_i \phi(V_i) + \omega_o \sum_{\substack{V_j \in V^{out} \\ j=1}}^{N} \frac{\bar{D}_{V_j} - D_{V_j}}{\bar{D}_{V_j}}, \quad (2)$$

where $(\alpha_1,\alpha_2,\cdots,\alpha_N)$ is the importance of the tile depending on the percentage in the viewport, V_i indicates the tile inside the viewport, V_j indicates the tile outside the viewport, $\bar{D}_{V_j}$ and D_{V_j} respectively represent the bandwidth consumed by the player V_j if chunks are buffered at the highest bitrate and the bandwidth consumed by the actual download, and $\frac{\bar{D}_{V_j} - D_{V_j}}{\bar{D}_{V_j}}$ means the bandwidth saving rate of the player V_j. ω_u and ω_o are the weights of QoE and transmission cost respectively. A higher ω_u means more emphasis on the QoE and vice versa. We take $\omega_u = 0.5$ and $\omega_t = 0.5$.

We find a sequence of suitable bitrate versions for each tile V_i to schedule bandwidth resources that maximize the system utility and satisfy:

$$\begin{cases} \sum_{\substack{V_i \in V^{in} \\ i=1}}^{N} \sum_{k=1}^{K} r(V_{i,k}) \leqslant C \\ r(V_{i,k}) \in R \end{cases}. \quad (3)$$

Our solution consists of the following aspects:

- Prediction of the probability distribution of the viewport on spatial tiles, including viewport estimation and prediction based on content;
- Computation of multi-player total bandwidth and estimation of the bitrate constraint C (or throughput);
- Decision on the optimal version of each tile.

In the following section, we will address each of these aspects.

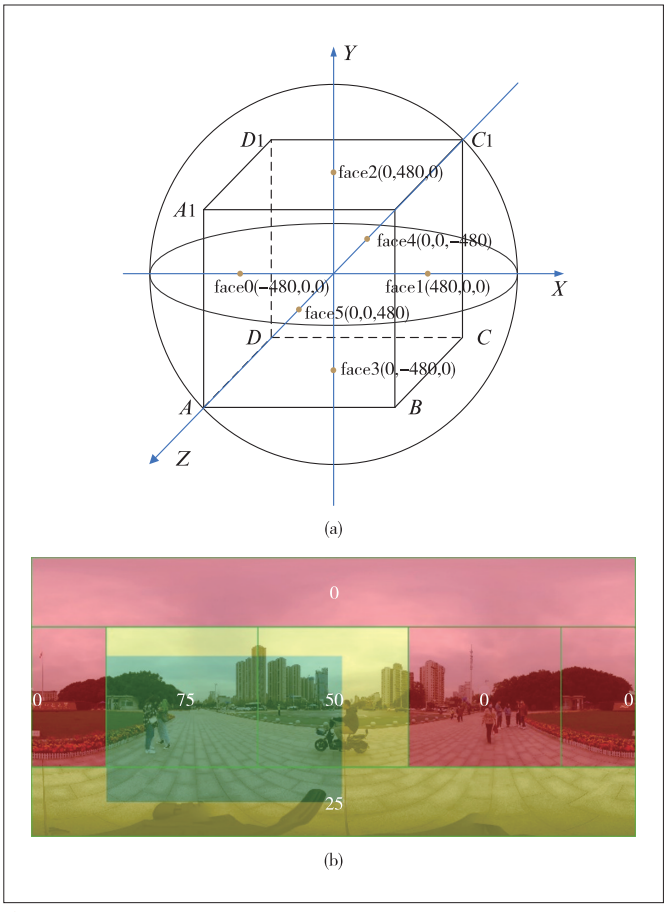
4 Viewport Prediction

A distinctive feature of 360-degree video is that the attention is not evenly distributed. Therefore, the viewport-driven stream is an effective solution to the improvement of the quality of the 360-degree video, but it is always challenging to predict the viewpoint trajectory accurately. Recent studies have proposed adaptive bitrate algorithms based on FOV prediction, but these algorithms have the following shortcomings. Firstly, it lacks consideration for the video content itself. Secondly, there is a strong dependence on the FOV, and any FOV prediction error

probably causes a decline in video quality and even significant rebuffering. Therefore, in this section, we propose a viewport prediction approach based on the priority of FOV and content.

4.1 FOV priority

The system divides the 360-degree video into six faces corresponding to a cube map as in Fig. 2(a), where six video tiles are placed on the six faces of the cube. The browser renders it into a sphere, and the VR user is located in the center of the sphere to observe the surface of the sphere. The red point is the center point on each surface of the cube, with the Cartesian coordinates of the point in brackets. The spherical coordinates of each tile mapped on the sphere are shown in Table 1, expressed in the form of latitude and longitude, and the latitude and longitude centers mean the spherical coordinate of the center of the tile. In Fig. 2(b), the green area shows the user's FOV, the yellow area indicates that a part of the current tile is inside the FOV and may be viewed later, and the red area illustrates that the current tile is absolutely outside the FOV. We calculate the overlap between the tile and FOV according to Table 2 to get the priority of the tile.



▲ **Figure 2. (a) 360-degree video segmentation that the content-aware multi-step prediction control algrithm (CAMPC) uses to judge the importance of tiles; (b) example of FOV priority allocation according to FOV at a certain moment**

The higher the value, the higher the proportion of the tile in the FOV, and the higher the bitrate version should be buffered later.

The FOV of common head-mounted devices is about 110 degrees. Since the final verification scene is a browser window, obviously it is easier to obtain the spherical coordinates of the center of the window. We define the priority of each tile based on the relative position of each face and the center of the viewport. As shown in Table 2, the system divides the priority into five levels: 100, 75, 50, 25, and 0. In order to obtain the final FOV priority, the adaptive bitrate algorithm traverses latitude and longitude in order from high score to low score to find the mapping interval of the two dimensions.

▼**Table 1. Spherical coordinates of tiles**

	Latitude Range	Latitude Center	Longitude Range	Longitude Center
V_1	[225°, 315°]	270°	[45°, 135°]	90°
V_2	[45°, 135°]	90°	[45°, 135°]	90°
V_3	[0°, 360°]	*	[0°, 45°]	0
V_4	[0°, 360°]	*	[135°, 180°]	180°
V_5	[135°, 225°]	180°	[45°, 135°]	90°
V_6	[315°, 45°]	0°	[45°, 135°]	90°

▼**Table 2. Tile priority and spherical coordinates mapping relations**

Priority	100	75	50	25	0
V_1	(90°, 270°)	(45°~135°, 225°~315°)	(10°~170°, 225°~315°) (45°~135°, 180°~360°)	(10°~170°, 180°~360°)	Others
V_2	(90°, 90°)	(45°~135°, 45°~135°)	(10°~170°, 45°~135°) (45°~135°, 0°~180°)	(10°~170°, 0°~180°)	Others
V_3	(0°~5°,*)	(5°~10°,*)	(0°~45°,*)	(0°~90°,*)	(90°~180°,*)
V_4	(175°~180°,*)	(170°~175°,*)	(135°~180°,*)	(90°~180°,*)	(0°~90°,*)
V_5	(90°, 0°)	(45°~135°, 135°~225°)	(10°~170°, 135°~225°) (45°~135°, 270°~90°)	(10°~170°, 270°~90°)	Others
V_6	(90°, 180°)	(45°~135°, 315°~45°)	(10°~170°, 315°~45°) (45°~135°, 90°~270°)	(10°~170°, 90°~270°)	Others

4.2 Content Priority

Different from predicting the future viewport based only on the online viewport, the system server will convert the original video into frames in advance, and perform operations such as gradient calculation and semantic segmentation through the pre-trained neural network model, to get the priority of bitrate allocation shown in Fig. 2(b).

In this work, we mainly use FC-DenseNets with U-Net structure as a model for extracting features. Through the 56-layer network, the model analyzes content features and then classi-

fies and slices them. After training 300 samples in 300 epochs through the model, a better checkpoint is obtained, and the following semantic segmentation results are obtained by using the own dataset as the test data. Among them, the segmented category must be consistent with the category applied in training.

The original image shown in Fig. 3(a) is inputted into the trained network model to obtain segmentation results as in Fig. 3 (b) and then transformed into an image with only 0 and 255 grayscales as shown in Fig. 3(c). Despite some errors and the defect that there are unclear boundaries of categories, the results are generally sufficient to judge the priority of content perception. We count the number of black and white pixels on the obtained grayscale image. The whiter pixels there are, the richer the image content. The higher priority of content perception means that in the MPD file of the video tiles, the bandwidth attribute corresponding to each bitrate level will be relatively higher. In other words, the video segment has a larger file size than the segment with a lower perception priority, containing complex content that may grab the user's attention. After the above process is performed on each frame of the original video, the average value of the content richness of each video segment can be calculated, and this information is stored in the JavaScript Object Notation (JSON) file used for the request for the terminal to read while allocating bandwidth among multi-players.

4.3 Probability Distributions of Future FOV

The viewport distribution probability α_i of any tile V_i in the future is determined by the FOV priority S_F and content perception priority S_C. The total priority α_i of a tile can be calculated by $S = \omega_F S_F + \omega_C S_C$, where ω_F represents the weight of S_F, ω_C represents the weight of S_C, and they depend on the current occupancy of the buffer $B_{f,k}$:

- $B_{f,k} \geqslant B_r - L$ (when $\omega_F = 0.3, \omega_C = 0.7$) means that when the video buffer is sufficient, more emphasis is placed on the score based on the richness of video content, where B_r represents the length of the safe buffer that players want to keep, and L represents the duration of the video segment.
- $B_{f,k} \leqslant L$ (when $\omega_F = 0.8, \omega_C = 0.2$) means that the FOV score is more emphasized while the insufficient buffered video is facing the danger of rebuffering.
- $L \leqslant B_{f,k} \leqslant B_r - L$ and $\omega_F = 0.5, \omega_C = 0.5$ represent that when the video buffer occupancy is within the normal range, the content score and the FOV score are jointly influenced by the priority.

S represents the importance of the impact of the current face on the QoE. Since the calculation method for the total score of each tile may be different, it is necessary to normalize the score S by $\alpha_i = \frac{S_i}{\sum_{j=1}^{N} S_j}$, and finally, get a set of probability distributions $(\alpha_1, \alpha_2, \cdots, \alpha_N)$ of future FOV.

5 Adaptive Bitrate

5.1 Video Streaming Model

The download process of video slices is modeled as a time sequence[16], with the start download time of chunk $V_{i,k}$ as the sampling point. At this time, the buffer occupancy is represented as $b(V_{i,k})$. After $V_{i,k}$ is downloaded, the buffer is consumed for $\frac{r(V_{i,k})L}{c(V_{i,k})}$ as the user watches the video and is filled with L seconds when the time has passed. Therefore, when the download of $V_{i,k}$ has been completed, the buffer occupancy can be expressed as:

$$b(V_{i,k+1}) = b(V_{i,k}) - \frac{r(V_{i,k})L}{c(V_{i,k})} + L. \tag{4}$$

The premise is $b(V_{i,k}) > \frac{r(V_{i,k})L}{c(V_{i,k})}$ to ensure that the content of the chunks in the buffer is enough to play without rebuffering. Similarly, in the case before downloading chunk $V_{i,k}$, we have

$$b(V_{i,k}) = b(V_{i,k-1}) - \frac{r(V_{i,k-1})L}{c(V_{i,k-1})} + L. \tag{5}$$

(a) Original image (b) Segmentation image (c) Binary image

▲ **Figure 3. Analyzing the priority of content perception under the semantic segmentation model**

In order to describe the relationship between the bitrate change and the buffer occupancy evolution, we make a subtraction between Eqs. (4) and (5). Since previous studies showed that the throughput of a cellular network would not change significantly for a period of time, we assume $c(V_{i,k+1}) = c(V_{i,k})$, and $\xi(V_{i,k})$ is used to ex-

press the impact of this assumption, which obtainins that

$$b(V_{i,k+1}) = 2b(V_{i,k}) - b(V_{i,k-1}) - \frac{\Delta r(V_{i,k})L}{c(V_{i,k})} + \xi(V_{i,k}) . \quad (6)$$

The adaptive bitrate algorithm among multi-players needs to balance a set of conflicting QoE elements such as video quality maximization, rebuffering events minimization, and quality fluctuations. For chunks in V^{in} that directly affect the QoE, we optimize the QoE metrics over the multi-step prediction horizon and at the same time control the future buffer occupancy. And for chunks in V^{out} of which the importance is obviously less than chunks inside FOV, we subtract the predicted bandwidth and the used bandwidth to obtain the currently available bandwidth, and then according to $(\alpha_1,\alpha_2,\cdots,\alpha_N)$ we allocate the remaining bandwidth to each tile. Note that the tiles contained in sets V^{in} and V^{out} are updated in real-time as the FOV changes.

Since the network status, in reality, is hard to predict accurately, it requires the algorithm performance to be robust to the prediction error. Therefore, minimizing buffer control error achieves quality maximization and rebuffering minimization simultaneously by keeping buffer occupancy at a constant level B_r. However, due to changes in throughput, accurate control of buffer occupancy requires frequent quality switching. Since buffer occupancy changes will not affect QoE directly and switching bitrates reduces QoE, it should tolerate some buffer occupancy fluctuations but limit the variability of video quality. Therefore, the optimization goal is designed to minimize the buffer control error and the weighted combination of the bitrate change $\Delta r(V_{i,k}) = r(V_{i,k}) - r(V_{i,k-1})$ between two consecutive video chunks. Then the total cost function from chunks 1 to K for any tiles in V^{in} is expressed as

$$J_1^K = E\{\sum_{k=1}^{K}[b(V_{i,k+1}) - b_r(V_{i,k+1})]^2 + \sum_{k=1}^{K}[\lambda_k \Delta r(V_{i,k})]^2\}, \quad (7)$$

where λ_k is the penalty of changing the bitrate at $V_{i,K}$. The algorithm controls $b(V_{i,k+1})$ to smoothly reach $b_r(V_{i,k+1})$ along the trajectory $b_r(V_{i,k+1}) = \beta b(V_{i,k}) + (1-\beta)B_r$, where $\beta \in [0,1)$. A smaller β means moving towards $b_r(V_{i,k+1})$ faster. The definition of the cost function allows us to meet the requirements of different users for video playback. A larger λ is employed if users are more concerned about smooth playback. A trimmer is adopted in cases where they do not care about bitrate variations.

When the average throughput $c(V_{i,k}),\cdots,c(V_{i,K})$ of downloading K chunks in the future is known, the bitrate $r(V_{i,k}),\cdots,r(V_{i,K})$ allocated to each chunk can be obtained by minimizing the cost function. Therefore, the bitrate selection for $V_{i,K}$ in V^{in} can be formulated as an optimal predictive control problem over an N-step horizon.

$$\min \hat{J}_{k+1}^{k+T} = E\{\sum_{t=1}^{T}[\hat{b}(V_{i,k+t}|V_{i,k}) - b_r(V_{i,k+t})]^2 + \sum_{t=1}^{T}[\lambda_t \Delta r(V_{i,k+t-1})]^2\}$$

$$\text{s.t.}\begin{cases} b(V_{i,k+1}) = 2b(V_{i,k}) - b(V_{i,k-1}) - \dfrac{\Delta r(V_{i,k})L}{c(V_{i,k})} + \xi(V_{i,k}) \\ b_r(V_{i,k+1}) = \beta b(V_{i,k}) + (1-\beta)B_r, \beta \in [0,1) \\ b(V_{i,1}) = L, b(V_{i,k}) \in [L, B_m] \\ r(V_{i,k}) \in R, \lambda_t = \lambda(V_{i,T-t+1}) \end{cases}, \quad (8)$$

where the $\hat{b}(V_{i,k+t}|V_{i,k})$ is the t-step ahead estimated value of the buffer occupancy while downloading $V_{i,k+1}$ up to $V_{i,k+t}$, and λ_t is the discount rate for switching bitrate from $r(V_{i,k+t}^{\text{in}})$ to $r(V_{i,k+t+1}^{\text{in}})$. And as the number of prediction steps increases, λ_t is gradually reduced to $\lambda(V_{i,T-t+1})$, representing that the far future will have less impact on the current cost.

With the bandwidth prediction $\hat{c}[V_{i,k}, V_{i,k+T-1}]$ of the future K chunks as the input, the prediction optimization controller outputs the bitrate $r(V_{i,k})$ selected for $V_{i,K}$ so that the QoE indicators achieve the expected balance.

5.2 Link Bandwidth Predictor

The algorithm first gets the real-time throughput and then uses the Kalman filter method to obtain the predicted value used in the bitrate selector for control optimization.

The Kalman filter dynamically adjusts parameters to output the estimated value for online prediction. The prediction is based on two equations: a dynamic state equation that describes the dynamics hidden state (e.g., the predicted bandwidth) and a static output equation describing the relationship between the hidden state and the measured value (e.g., throughput). The Kalman filter method, which can filter out temporary throughput fluctuations and reflect the stable change, matches the observations in the previous work that the evolution of the throughput within a session exhibits stateful characteristics and the throughput is essentially Gaussian within each state.

The throughput prediction model based on the Kalman filter employs a classic time series model and an auto-regressive model assuming $c(V_{i,k+1}) = \sum_{j=0}^{p} a_j c(V_{i,k-j}) + w(V_{i,k})$, where $\{a_j\}_{j=0}^{p}$ is the weight parameter and $w(V_{i,k})$ is Gaussian noise with zero mean, satisfying $W = E[w(V_{i,k})^2]$. Existing works[17-18] have shown that the network throughput is piecewise stationary. The statistical properties, including mean and variance, do not change over tens of seconds or minutes. We assume the dynamic state model is $c(V_{i,k+1}) = c(V_{i,k}) + w(V_{i,k})$, where $c(V_{i,k})$ represents the average download speed that needs to be estimated during the downloading process of

the video chunk $V_{i,k}$.

Let $v(V_{i,k})$ denote the video throughput measurement when downloading chunk $V_{i,k}$. Recent studies show that the observed throughput fluctuates around the link capacity following Gaussian. Therefore, $v(V_{i,k})$ is modeled as the summation of capacity $c(V_{i,k})$ and measurement noise $q(V_{i,k})$ denoted by $Q = E[q(V_{i,k})^2]$. Finally, the whole system model is given by:

$$\begin{cases} c(V_{i,k+1}) = c(V_{i,k}) + w(V_{i,k}) \\ v(V_{i,k}) = c(V_{i,k}) + q(V_{i,k}) \end{cases}. \tag{9}$$

The Kalman filter consists of model prediction and measurement correction. In the prediction stage, the Kalman filter uses the estimated value of the previous link capacity $\hat{c}(V_{i,k-1})$ to predict the current state:

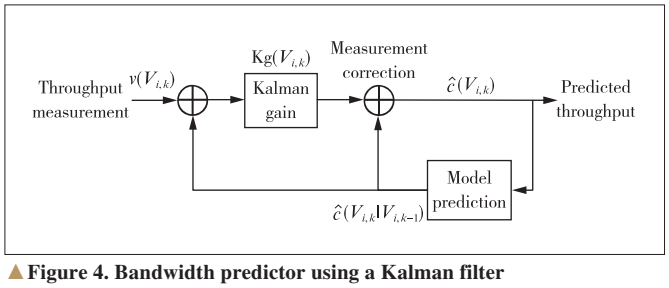
$$\hat{c}(V_{i,k}|V_{i,k-1}) = \hat{c}(V_{i,k-1}). \tag{10}$$

Then the initial estimate of capacity $\hat{c}(V_{i,k}|V_{i,k-1})$ is corrected to a new estimated value $\hat{c}(V_{i,k})$ by the measurement correction model. The correction equation is:

$$\hat{c}(V_{i,k}) = \hat{c}(V_{i,k}|V_{i,k-1}) + Kg(V_{i,k})\left[v(V_{i,k}) - \hat{c}(V_{i,k}|V_{i,k-1})\right]. \tag{11}$$

Fig. 4 shows how to obtain a new estimate $\hat{c}(V_{i,k})$. The difference between the initial estimate $\hat{c}(V_{i,k}|V_{i,k-1})$ and the measured throughput $v(V_{i,k})$ is multiplied by the Kalman gain $\mathrm{Kg}(V_{i,k})$, which then serves as a correction to the initial estimate $\hat{c}(V_{i,k})$. The estimation produced by the Kalman filter is attributed to two terms: the previous estimate $\hat{c}(V_{i,k-1})$ and the throughput $v(V_{i,k})$. The Kalman gain $\mathrm{Kg}(V_{i,k})$ balances contributions of the two terms: a larger one means more weight is given to the measured value; conversely, a smaller one denotes that the model trusts the estimated value more. The updated process of the Kalman gain is:

$$\mathrm{Kg}(V_{i,k}) = \frac{P(V_{i,k-1}) + W}{P(V_{i,k-1}) + W + Q}, \tag{12}$$



▲ **Figure 4. Bandwidth predictor using a Kalman filter**

where $P(V_{i,k})$ is the system error defined as $P(V_{i,k}) = E\left[\left(\hat{c}(V_{i,k}) - c(V_{i,k})\right)^2\right]$. This value will be recursively modified at each step:

$$P(V_{i,k}) = \left(1 - \mathrm{Kg}(V_{i,k})\right)\left(P(V_{i,k-1}) + W\right). \tag{13}$$

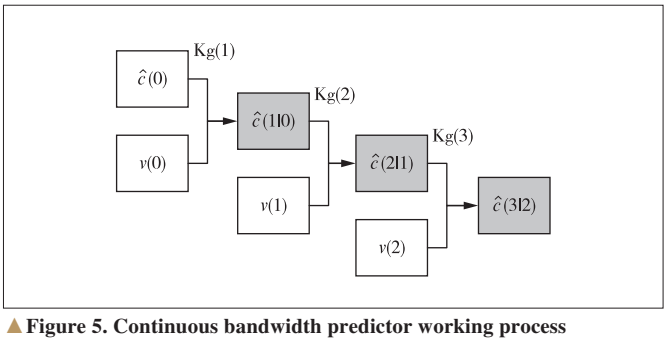
The above process is executed continuously, obtaining the predicted throughput as the gray blocks in Fig. 5 while buffering the next chunk every time. In order to obtain the multi-step bandwidth prediction value, the average throughput of five video chunks in the future is predicted at each step. Since the average throughput measurements $v(V_{i,k+1}), v(V_{i,k+2}), v(V_{i,k+3})$, and $v(V_{i,k+4})$ are unknown when downloading chunks $V_{i,k}$, the network throughput can be approximately stable for a while[17-18]. Therefore, it is assumed that the measurement throughput $v(V_{i,k})$ of the next chunks meets $v(V_{i,k+1}) = v(V_{i,k+2}) = v(V_{i,k+3}) = v(V_{i,k+4}) = v(V_{i,k})$. Fig. 6 shows the prediction iteration process, which is the continuation of the one-step Kalman filter. Blocks of the same color have the same predicted value, and the gray blocks have the same value as the same block in Fig. 5. Various parameter initialization problems involved in the process are described in Section 6.

5.3 Bitrate Selector

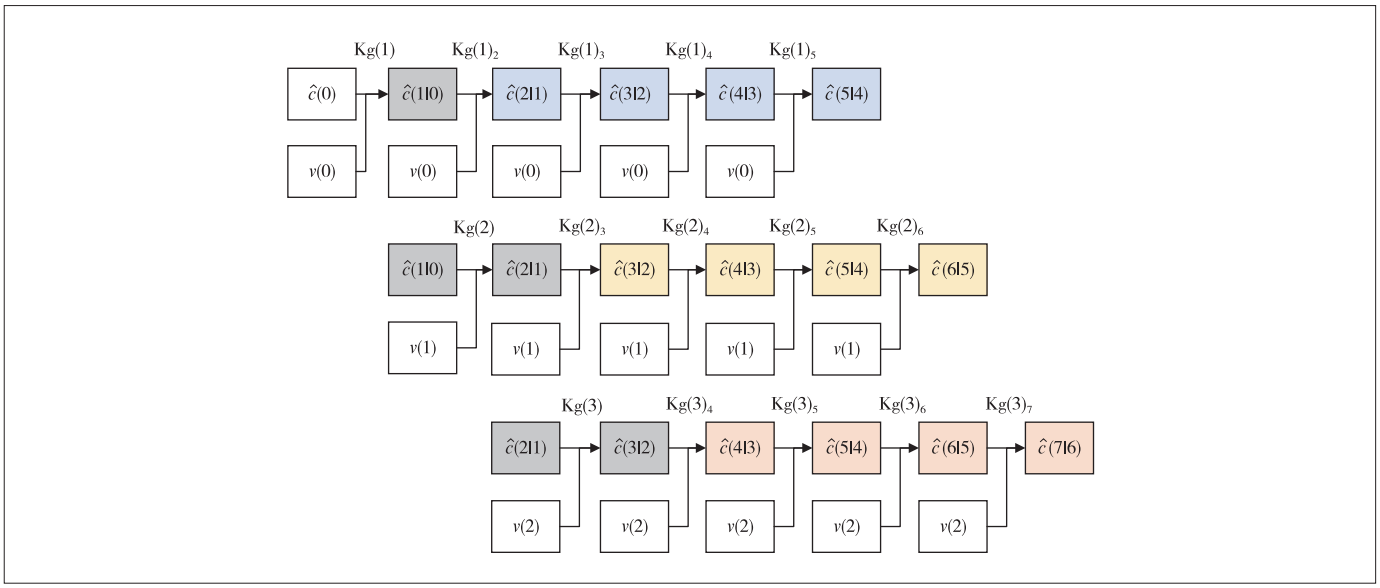
The CAMPC selects the bitrate according to the minimization cost function in Eq. (8) within the prediction range. To solve it, we first obtain the multi-step prediction of buffer occupancy based on the predicted link bandwidth. With the future buffer occupancy expressed by a bitrate function, the cost function can be derived to be only relevant to the variable video bitrate. Then, the bitrate that minimizes the cost function can be obtained.

After obtaining the average throughput $c(V_{i,k}),\cdots,c(V_{i,K})$ of downloading K chunks in the future, the buffer occupation of the t-step is defined as $b(V_{i,k})$ and $b(V_{i,k-1})$, experiencing a recursive process:

$$\hat{b}(V_{i,k+t}|V_{i,k}) = (t+1)b(V_{i,k}) - tb(V_{i,k-1}) - \frac{N\Delta r(V_{i,k})L}{c(V_{i,k})} - \cdots - \frac{2\Delta r(V_{i,k+t-2})L}{c(V_{i,k+t-2})} - \frac{\Delta r(V_{i,k+t-1})L}{c(V_{i,k+t-1})}. \tag{14}$$



▲ **Figure 5. Continuous bandwidth predictor working process**



▲ **Figure 6. Multi-step bandwidth predictor working process**

Then the buffer occupation of the player V_i is finally given by the following:

$$\hat{B}=\begin{bmatrix}\hat{b}(V_{i,k+1})\\ \hat{b}(V_{i,k+2})\\ \cdots\\ \hat{b}(V_{i,k+K})\end{bmatrix}=\begin{bmatrix}2b(V_{i,k})-b(V_{i,k-1})\\ 3b(V_{i,k})-2b(V_{i,k-1})\\ \cdots\\ (T+1)b(V_{i,k})-Tb(V_{i,k-1})\end{bmatrix}+\begin{bmatrix}-\dfrac{L\Delta r(V_{i,k})}{c(V_{i,k})}\\ -\dfrac{2L\Delta r(V_{i,k})}{c(V_{i,k})}-\dfrac{L\Delta r(V_{i,k+1})}{c(V_{i,k+1})}\\ \cdots\\ -\dfrac{TL\Delta r(V_{i,k})}{c(V_{i,k})}\cdots-\dfrac{2L\Delta r(V_{i,k+T-2})}{c(V_{i,k+T-2})}-\dfrac{L\Delta r(V_{i,k+T-1})}{c(V_{i,k+T-1})}\end{bmatrix}. \tag{15}$$

Among them, $\Delta r(V_{i,k+T-2})$ is replaced by $z^{-1}\Delta r(V_{i,k+T-1}),\cdots$, and $\Delta r(V_{i,k+1})$ is replaced by $z^{-T+2}\Delta r(V_{i,k+T-1})$. Similarly $b(V_{i,k})$ is replaced by $z^{-1}b(V_{i,k})$, and then the $\hat{b}(V_{i,k+T})$ is formulated as:

$$\begin{aligned}&\hat{b}(V_{i,k+T})=(T+1-Tz^{-1})b(V_{i,k})+\\&\left(-\frac{L}{\hat{c}(V_{i,k+T-1})}-\frac{2L}{\hat{c}(V_{i,k+T-2})}z^{-1}-\cdots-\frac{TL}{\hat{c}(V_{i,k})}z^{-T+1}\right)=\\&G_T(z^{-1})b(V_{i,k})+F_T(z^{-1})\Delta r(V_{i,k+t-1})\ .\end{aligned} \tag{16}$$

The vector of future buffer occupancy is $\hat{B}=\boldsymbol{GB}(V_{i,k})+\boldsymbol{F}\Delta R$, which can be written as:

$$\hat{B}=\begin{bmatrix}2&-1\\3&-2\\4&-3\\\vdots&\vdots\\T+1&-T\end{bmatrix}\begin{bmatrix}b(V_{i,k})\\b(V_{i,k-1})\end{bmatrix}+\begin{bmatrix}-\dfrac{L}{c(V_{i,k})}&0&\cdots&0\\-\dfrac{2L}{c(V_{i,k})}&-\dfrac{L}{c(V_{i,k+1})}&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\-\dfrac{TL}{c(V_{i,k})}&-\dfrac{(N-1)L}{c(V_{i,k+1})}&\cdots&-\dfrac{L}{c(V_{i,k+T-1})}\end{bmatrix}\begin{bmatrix}\Delta r(V_{i,k})\\\Delta r(V_{i,k+1})\\\cdots\\\Delta r(V_{i,k+T-1})\end{bmatrix}. \tag{17}$$

Substituting $\hat{B}=\boldsymbol{GB}(V_{i,k})+\boldsymbol{F}\Delta R$ into the cost function Eq. (8), we get:

$$\begin{aligned}&\min \hat{J}_{k+1}^{k+T}=E\{\sum_{t=1}^{T}[\boldsymbol{GB}(V_{i,k})+\boldsymbol{F}\Delta R-B_r]^T\\&[\boldsymbol{GB}(V_{i,k})+\boldsymbol{F}\Delta R-B_r]+\Delta R^T\Lambda\Delta R\}\\&\text{s.t.}\begin{cases}\hat{B}=[\hat{b}(V_{i,k+1}),\hat{b}(V_{i,k+2}),\cdots,\hat{b}(V_{i,k+T})]^T\\\Delta R=[\Delta r(V_{i,k}),\Delta r(V_{i,k+1}),\cdots,\Delta r(V_{i,k+T-1})]^T\\B(V_{i,k})=[b(V_{i,k}),b(V_{i,k-1})]^T\\B_r=[B_r,B_r,B_r,B_r,B_r]^T\\\Lambda=\text{diag}(\lambda_1,\lambda_2,\cdots,\lambda_T)\ .\end{cases}\end{aligned} \tag{18}$$

In order to minimize the cost, let $\frac{\partial \hat{J}_{k+1}^{k+T}}{\partial \Delta R} = 0$, and then we get $\Delta R = (F^T F + \Lambda)^{-1} F^T (B_r - GB(V_{i,k}))$. The final bandwidth allocation takes the first vector of ΔR, that is $\Delta r(V_{i,k})$, and the bitrate finally selected for the chunk $V_{i,k}$ is $h(V_{i,k})$. We assume $H(V_{i,k}) = \{h_1, h_2, h_3, \cdots, h_m\}$ to be the set of available bitrate versions for chunk $V_{i,k}$, where $h(V_{i,k}) = h_i$ satisfies $h_i < r(V_{i,k-1}) + \Delta r(V_{i,k})$ and $h_{i+1} > r(V_{i,k-1}) + \Delta r(V_{i,k})$.

The above bandwidth scheduling method helps spatial tiles V^{in} with high probability in the future viewport allocated bandwidth. For tiles V^{out} segmentation with low probability in the FOV, the system first uses the one-step bandwidth predictor to obtain the predicted link capacity. After the bandwidth allocation of the V^{in}, the difference between the predicted value and the consumed value indicates the currently available bandwidth, which will be scheduled to each tile out of FOV according to the weight $(\alpha_1, \alpha_2, \cdots, \alpha_N)$ given in Section 4.

6 Evaluation

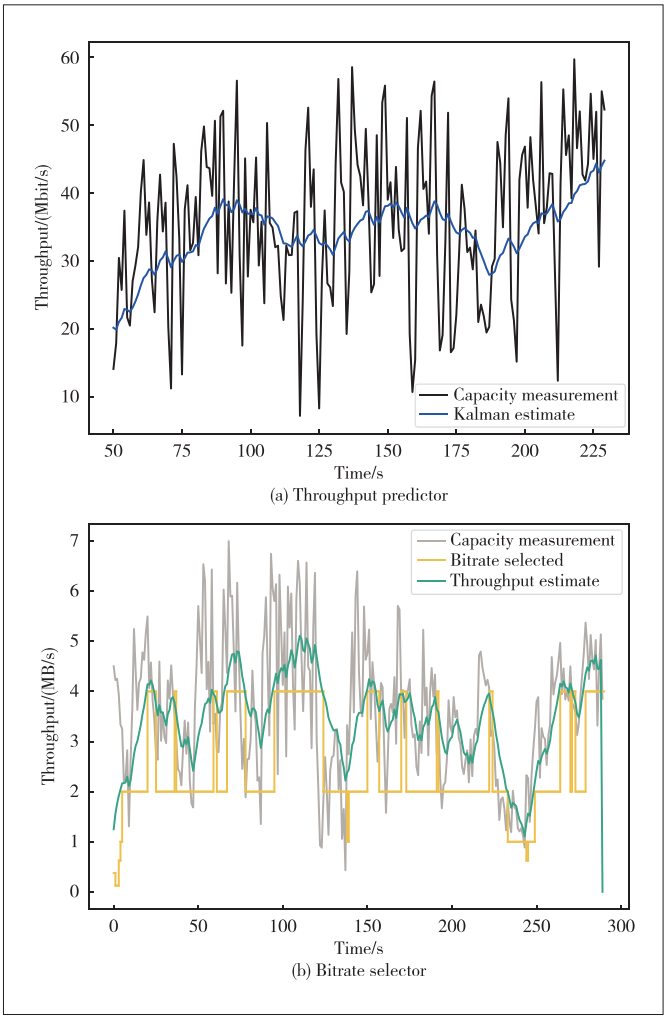
6.1 Methodology

6.1.1 Experimental Setup

Our emulated DASH system consists of a server and a video player based on Dash.js (version 3.2), an open-source implementation of the DASH standard. The client video player is a Google Chrome browser. The throughput is computed by the method in the next section in real time. Key classes of adaptive streaming-related functions are modified. First of all, we modify the media-player settings and add attributes that indicate the current chunk and tile serial number. ABR algorithms are implemented in the AbrController class, and HTTP requests for throughput measurement are collected from the Throughput History function. At the same time, we modify the buffer threshold of each player when the FOV is switched. For the tile in the viewport, the maximum buffer size is 10 s, and the safety threshold is 6 s. While the tile is outside FOV, the above two values are 4 s and 2 s, respectively. The purpose is to respond to this change faster when the viewing angle is switched. We use the Angular.js framework to unify the front-end communication of the platform, monitoring system state information such as buffer occupancy, bitrates, rebuffering time, and the predicted/actual capacity. These also are logged for the performance analysis.

6.1.2 Link Capacity Traces

To verify the effectiveness of the throughput predictor and control optimizing model on a single media player in realistic network conditions, we use link capacity traces based on the public dataset, which collects throughput measurements in 4G/LTE networks. Belgium 4G/LTE dataset records the available bandwidth while downloading a large file in and around Ghent, Belgium. Figs. 7(a) and 7(b) show the single simulator's predictor and selector, respectively, running status on a 4G/LTE trace, which can verify the algorithm accuracy on one player.



▲ **Figure 7. Single simulator running status over Belgium 4G/Long Term Evolution (LTE) dataset**

6.1.3 Video Parameters

We transform a 4K 360-degree panoramic video into six faces corresponding to a cube map for evaluation. Each video tile with 1 080 resolution is split into 123 chunks of 1 s and is encoded by VP9 codec in six bitrate versions, i.e., {0.18, 0.45, 0.91, 3.10, 4.55, 6.05} Mbit/s. The specific bitrate mapping to the same level among different video tiles varies with the video content richness; that is, a video about the sky is often simpler and has a lower bitrate than a portrait video.

6.1.4 Adaptation Algorithms

We evaluate CAMPC and the following widely adopted ABR algorithms and simple ABR rules for a 360-degree video:

• DASH. js. DYNAMIC dynamically switches between ThroughputRule and BolaRule. These two algorithms are based on rate and buffer to select bitrate.

• DASH.js.LoL+ is based on the learning adaptive bitrate algorithm Low-on-Latency (LoL), with improving adjustment of the weight for the self-organizing mapping (SOM) features and controlling the playback speed and taking into account latency and buffering levels.

• FOV is an adaptive bitrate algorithm based on the real-time viewport implemented by our experiment platform. The bandwidth allocation weight is calculated according to the angle deviation between each tile in the viewport and the center point of the FOV.

• FOVCONTENT is an adaptive bitrate algorithm based on the real-time viewport and content perception implemented by our experiment platform. It predicts the viewport based on the user's current viewport and the content richness obtained from offline training, and the average throughput within a period is used for bit rate allocation.

6.2 Choice of CAMPC Parameters

In the bandwidth predictor, we set the initial system error variance $P\left(V_{i,0}\right)$ to 7 Mbit/s and the process noise variance W to 3 Mbit/s, which denotes that the prior estimate of the network bandwidth fluctuates by 3 Mbit/s. When the initial value is set, it is necessary to ensure that the system error variance is not less than the process noise variance. A higher variance of the system error will make the prediction process more trustworthy in the throughput measurement at the initial stage, resulting in a better fitting curve. The measuring noise is updated by $Q(k) = \alpha Q(k-1) + (1-\alpha)[v(k) - \hat{c}(k|k-1)]^2, \alpha = 0.8$. The initial value of the throughput estimate $c\left(V_{i,0}\right)$ is set to 8 Mbit/s.

6.3 Real-Time Throughput Measurement

Different from the single player, which can directly measure the throughput according to the application programming interface (API) in DASH to get the throughput, multiple players share the link for synchronous transmission, with inaccuracy in the throughput obtained by any player from API. According to DASH, at the end of transmission for a chunk, the start timestamp d, the end timestamp, and the number of data transferred can be obtained by the player. Therefore, the transmission state of the video chunks, as in Fig. 8, shows a possible state.

The outermost black box represents a time slot, which is the smallest unit of our timing measurement throughput. The blue blocks in Fig. 8 indicate the downloading process of each player. The value on the blue block indicates which player is downloading. Although they request videos in sequential order $V_{i,k}, V_{i,k+1}, V_{i,k+2}, \cdots$, the order in which the players appear in the picture is random since each player is an independent download process. The blue blocks marked by the dotted line represents the download process that players' monitor cannot capture at the end of the time slot. Therefore, when calculating the throughput, the time should remove the part that has no data transmission from a slot and the total number of data should be all the data that can be sensed.

Assuming that the start time of the slot is t and the end time is $t + d$, in order to avoid the impact of the chunks that cannot be captured as much as possible, we move the start and end timestamps forward for a short period d_{back}, then the actual start time of the time slot for calculating the throughput is $t - d_{\text{back}}$, and the actual end time is $t + d - d_{\text{back}}$.

The calculator cyclically judges whether the response starts timestamp req_k and finishes timestamp fin_k in the HTTP request list satisfy $\text{req}_k < t + d - d_{\text{back}}$ and $t - d_{\text{back}} < \text{fin}_k$; if satisfied, it indicates that at least part of the download process within the time gap needs to be further judged and calculated:

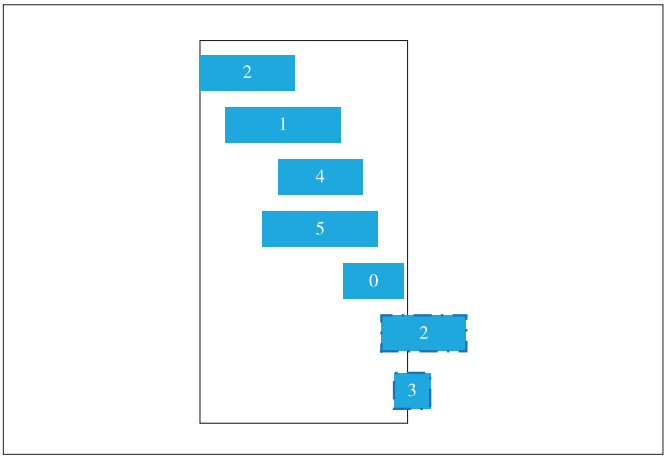
• When the start and end time of the request response is both within the timestamp, that is $t - d_{\text{back}} < \text{req}_k$ and $\text{fin}_k \leqslant t + d - d_{\text{back}}$, the total number of downloaded data D_k is directly added to the total number of downloaded data in this time slot;

• When the end time of the request response is outside the right timestamp, that is $t - d_{\text{back}} < \text{req}_k$ and $\text{fin}_k > t + d - d_{\text{back}}$, all the downloaded data are in proportion $\frac{t + d - d_{\text{back}} - \text{req}_k}{\text{fin}_k - \text{req}_k}$ to the total downloaded data in this time slot.

• When the request response start time is outside the time stamp on the left, that is $\text{req}_k < t - d_{\text{back}}$ and $\text{fin}_k \leqslant t + d - d_{\text{back}}$, add all the downloaded data D_k in proportion $\frac{\text{fin}_k - (t - d_{\text{back}})}{\text{fin}_k - \text{req}_k}$ are added to the total downloaded data in this time slot.

• When the start time and end time of the request response are outside the timestamp, that is $\text{req}_k < t - d_{\text{back}}$ and $\text{fin}_k > t + d - d_{\text{back}}$, the total number of downloaded data D_k in proportion $\frac{d}{\text{fin}_k - \text{req}_k}$ are added to the total downloaded data in this time slot.

In addition, it is necessary to avoid gaps in which no data is transmitted to the middle, beginning, and end of the slot due to buffer control rather than the current link capacity being 0. In the process, we record the current minimum request-



▲ **Figure 8. Time sequence of downloading process that may occur in multiple players**

response start timestamp req_{min}, which means there is no gap after the timestamp. If fin_k is less than req_{min}, then we subtract the gap time $req_{min} - fin_k$ from d. Finally, the throughput of the current time slot can be obtained by dividing the actual time interval by the total number of actual transmitted data.

6.4 Performance

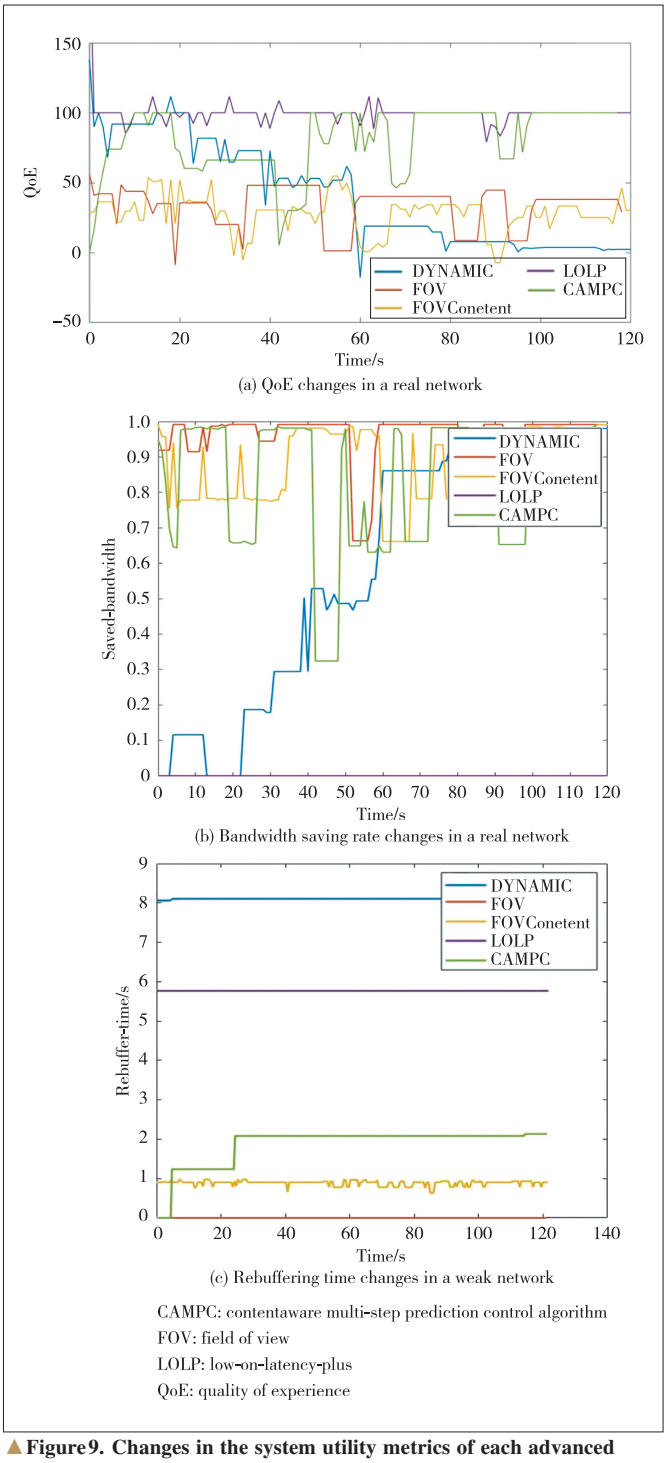
We compare the performance of ABR algorithms in a real and a weak network environment limited by the NetLimiter 4.

As shown in Fig. 9(a), the momentary fluctuation of QoE occurs when the viewport changes. Because the two rules of Dash. js treat each video player fairly, even if the viewport changes suddenly, the QoE fluctuation is minimal. For other rules, the tiles not in the FOV are often transmitted at a lower bitrate to save bandwidth, resulting in severe (30 – 50 s) QoE fluctuation when the FOV suddenly changes to a player outside the original viewport. However, the CAMPC rule can recover to the highest achievable QoE and remain stable in about 5 s, while the FOV and FOVContent rules need about 10 s to deal with this sudden change.

Fig. 9(b) shows the time-varying bandwidth saving rate compared with full video transmission. Although the CAMPC rule is slightly inferior to the LoL+ rule on QoE, it can achieve a bandwidth saving rate of 83% for tiles not in the viewport. More costs for transmissions are saved and congestion is reduced when multiple users request the same video source. No rebuffering event has occurred in the actual network environment.

In the actual network environment, the performance comparison of each ABR algorithm is shown in Table 3. The user QoE of the LoL+ rule can reach 100; the DYNAMIC rule shows that the initial bitrate can be reached in multiple tests, but the bitrate requested gradually decreases owing to the vicious circle of continuously requesting lower bitrates; the average QoE of the CAMPC rule proposed by this paper can be maintained at 80. The FOV and FOVContent rules cannot respond to the change of the user viewport in time, resulting in a sudden decrease in quality every time the user viewport changes. The bitrate is allocated according to the weight directly, leading to the case that the bandwidth within the user viewport is not made full use of, and the average QoE is low. The FOV and FOVContent rules have the highest bandwidth savings, reaching about 90%, and CAMPC can achieve 83% bandwidth savings. If both bandwidth savings and QoE are given a weight of 0.5, CAMPC can get the highest system utility of 81.9. The weight can be changed according to the importance of the cost and the QoE.

We conducted the same test in a weak network environment (the speed limit is 0.5 MB/s). Changes in the system utility metrics of each ABR rule over time show the same laws as in the natural environment, but the average QoE is lower and unstable. The performance comparison of the ABR rules in a weak network environment is shown in Table 4, where the bandwidth saving rate of each rule is about 90%. Rebuffering time changes are shown in Fig. 9(c). The FOV rule does not have rebuffering, the FOVContent rule has a rebuffering time of less than 1 s, and the CAMPC algorithm is the next, but all of these are below 2 s, which accounts for less than 1.64% of the total length of the video. The LoL+ and DYNAMIC rules have a relatively high rebuffering time, accounting for 4.73%



(a) QoE changes in a real network

(b) Bandwidth saving rate changes in a real network

(c) Rebuffering time changes in a weak network

CAMPC: contentaware multi-step prediction control algorithm
FOV: field of view
LOLP: low-on-latency-plus
QoE: quality of experience

▲**Figure 9. Changes in the system utility metrics of each advanced adaptive bitrate (ABR) rule over time**

▼ **Table 3. Performance comparison of ABR algorithms in a real network environment**

	CAMPC	DYNAMIC	LoL+	FOV	FOVContent
QoE	80.356	41.111	100.011	33.630	28.222
Saved-bandwidth	0.834 6	0.596	0	0.947	0.884
Utility	81.908	50.356	50.006	64.165	58.311

ABR: adaptive bitrate CAMPC: content-aware multi-step prediction control algorithm
FOV: field of view LoL+: Low-on-Latency-plus
QoE: quality of experience

and 6.64% of the total video length, respectively. The FOV rule has the highest system utility because, with the current rate limit of 0.5 MB/s, it happens to be enough for the player with the highest weight in FOV to request a video chunk with a quality of 6. If the network speed is lower than 0.5 MB/s, the FOV rule must have a severe rebuffering event. However, what is certain is that the FOV rule has better system utility in the range of about 0.5 MB/s. CAMPC rules are better than LoL+ and DYNAMIC rules in QoE, bandwidth saving rate, and rebuffering time. The overall utility is slightly inferior to the FOV and FOVContent rules.

▼ **Table 4. Performance comparison of ABR algorithms in a weak network environment**

	CAMPC	DYNAMIC	LoL+	FOV	FOVContent
QoE	12.051	4.690	6.565	23.526	6.904
Saved-bandwidth	0.975	0.954	0.941	0.926	0.790
Rebuffer-time	1.867	8.103	5.767	0	0.886 9
Utility	54.776	52.39	50.332	64.165	58.311

ABR: adaptive bitrate CAMPC: contentaware multi-step prediction control algorithm
FOV: field of view LoL: Low-on-Latency
QoE: quality of experience

7 Conclusions

Existing adaptive bitrate algorithms cannot provide smooth video quality for the 360-degree video in a network with high dynamic characteristics because of uncertain viewport prediction and bitrate selection. In order to achieve good QoE, the algorithm proposed in this paper considers the future multi-step network status and combines the richness of video content and the real-time user viewport to predict the future FOV, which can effectively save bandwidth resources. CAMPC uses a multi-step predictive control formulation that selects bitrate by controlling the buffer occupancy and optimizing QoE metrics over the prediction horizon. The formulation can select the bitrate level with the highest QoE and high fault tolerance. Through the above two prediction algorithms and control optimization, a content-aware 360-degree video ABR algorithm has been designed. The algorithm is implemented on the DASH video player and evaluated in reality. Experimental results show that CAMPC can save 83.5% of bandwidth resources compared with the scheme that completely transmits the tiles outside the viewport with the DASH protocol. Besides, the proposed method can improve the system utility by 62.7% and 27.6% compared with official and viewport-based rules, respectively.

References

[1] AFZAL S, CHEN J S, RAMAKRISHNAN K K. Characterization of 360-degree videos [C]//Proceedings of the Workshop on Virtual Reality and Augmented Reality Network. ACM, 2017: 1 – 6. DOI: 10.1145/3097895.3097896
[2] XIE L, XU Z M, BAN Y X, et al. 360ProbDASH: improving QoE of 360 video streaming using tile-based HTTP adaptive streaming [C]//Proceedings of the 25th ACM international conference on Multimedia. ACM, 2017: 345 – 323. DOI: 10.1145/3123266.3123291
[3] QIAN F, HAN B, XIAO Q Y, et al. Flare: practical viewport-adaptive 360-degree video streaming for mobile devices [C]//Proceedings of the 24th Annual International Conference on Mobile Computing and Networking. ACM, 2018: 99 – 114. DOI: 10.1145/3241539.3241565
[4] SONG J R, YANG F Z, ZHANG W, et al. A fast FoV-switching DASH system based on tiling mechanism for practical omnidirectional video services [J]. IEEE transactions on multimedia, 2020, 22(9): 2366 – 2381. DOI: 10.1109/TMM.2019.2957976
[5] SUN L Y, DUANMU F, LIU Y, et al. Multi-path multi-tier 360-degree video streaming in 5G networks [C]//Proceedings of the 9th ACM Multimedia Systems Conference. ACM, 2018: 162 – 173. DOI: 10.1145/3204949.3204978
[6] ZHANG Y X, GUAN Y S, BIAN K G, et al. EPASS360: QoE-aware 360-degree video streaming over mobile devices [J]. IEEE transactions on mobile computing, 2021, 20(7): 2338 – 2353. DOI: 10.1109/tmc.2020.2978187
[7] GUAN Y, ZHENG C Y, ZHANG X G, et al. Pano: optimizing 360° video streaming with a better understanding of quality perception [C]//Proceedings of the ACM Special Interest Group on Data Communication. ACM, 2019: 394 – 407. DOI: 10.1145/3341302.3342063
[8] FENG X L, SWAMINATHAN V, WEI S. Viewport prediction for live 360-degree mobile video streaming using user-content hybrid motion tracking [J]. Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies, 2019, 3(2): 1 – 22. DOI: 10.1145/3328914
[9] QIAO M L, XU M, WANG Z L, et al. Viewport-dependent saliency prediction in 360° video[J]. IEEE transactions on multimedia, 2021, 23: 748 – 760. DOI: 10.1109/TMM.2020.2987682
[10] YUAN H, ZHAO S Y, HOU J H, et al. Spatial and temporal consistency-aware dynamic adaptive streaming for 360-degree videos [J]. IEEE journal of selected topics in signal processing, 2020, 14(1): 177 – 193. DOI: 10.1109/JSTSP.2019.2957981
[11] WEI X K, ZHOU M L, KWONG S, et al. A hybrid control scheme for 360-degree dynamic adaptive video streaming over mobile devices [J]. IEEE transactions on mobile computing, 2022, 21(10): 3428 – 3442. DOI: 10.1109/TMC.2021.3058099
[12] SOBHANI A, YASSINE A, SHIRMOHAMMADI S. A video bitrate adaptation and prediction mechanism for HTTP adaptive streaming [J]. ACM transactions on multimedia computing, communications, and applications, 2017, 13(2): 1 – 25. DOI: 10.1145/3052822
[13] ZHOU C, LIN C W, ZHANG X G, et al. Buffer-based smooth rate adaptation for dynamic HTTP streaming [C]//Proceedings of 2013 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference. IEEE, 2013: 1 – 9
[14] YUAN H, HU X Q, HOU J H, et al. An ensemble rate adaptation framework for dynamic adaptive streaming over HTTP [J]. IEEE transactions on broadcasting, 2020, 66(2): 251 – 263. DOI: 10.1109/TBC.2019.2954074
[15] SPITERI K, URGAONKAR R, SITARAMAN R K. BOLA: Near-optimal bitrate adaptation for online videos [C]//The 35th Annual IEEE International Conference on Computer Communications. IEEE, 2016: 1 – 9. DOI: 10.1109/INFOCOM.2016.7524428

[16] YUAN H, FU H Y, LIU J, et al. Non-cooperative game theory based rate adaptation for dynamic video streaming over HTTP [J]. IEEE transactions on mobile computing, 2018, 17(10): 2334 – 2348. DOI: 10.1109/TMC.2018.2800749
[17] SUN Y, YIN X Q, JIANG J C, et al. CS2P: improving video bitrate selection and adaptation with data-driven throughput prediction [C]//Proceedings of the 2016 ACM SIGCOMM Conference. ACM, 2016: 272 – 285. DOI: 10.1145/2934872.2934898
[18] AKHTAR Z, NAM Y S, GOVINDAN R, et al. Oboe: auto-tuning video ABR algorithms to network conditions [C]//Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication. ACM, 2018: 44 – 58. DOI: 10.1145/3230543.3230558

Biographies

GAO Nianzhen received her bachelors' degree in computer science and technology from Sichuan University, China in 2020. She is currently working toward the PhD degree with the Research Center of 6G Mobile Communications, Wuhan National Laboratory for Optoelectronics, Huazhong University of Science and Technology, China. Her research interests include multimedia transmission and mobile edge computing.

YU Yifang received his MS degree in engineering from Xi'an Jiaotong University, China. He currently serves as the Senior Vice President of ZTE Corporation and President of the Cloud Video and Energy Product Operation Division. He has engaged in market planning and operations management in the telecommunications industry for over 20 years. His research interests include traditional telecom networks as well as the emerging fields such as cloud computing and the mobile Internet.

HUA Xinhai received his PhD degree from Nanjing University, China. He is currently the Vice President of ZTE Corporation and General Manager of Cloud Video Product Department. His research interests include cloud computing, IP-based video product technology and solutions, video business security solutions, content distribution network technology, product solutions, etc.

FENG Fangzheng received his bachelors' degree in communication engineering from Hunan University, China in 2019. He is currently working toward the PhD degree with the Research Center of 6G Mobile Communications, School of Cyber Science and Engineering, Huazhong University of Science and Technology, Hubei, China. His research interests include wireless communication and mobile multimedia transmission.

JIANG Tao (taojiang@hust.edu.cn) received his PhD degree in information and communication engineering from Huazhong University of Science and Technology, China in 2004. He is currently a Distinguished Professor with the Research Center of 6G Mobile Communications and School of Cyber Science and Engineering, Huazhong University of Science and Technology. He has authored or coauthored more than 300 technical papers in main journals and conferences, and nine books or chapters in the areas of communications and networks. He has served or is serving as an associate editor of some technical journals in communications, including the *IEEE Network*, *IEEE Transactions on Signal Processing*, *IEEE Communications Surveys and Tutorials*, *IEEE Transactions on Vehicular Technology*, and *IEEE Internet of Things Journal*, and he is an associate editor-in-chief of *China Communications*. His main research directions include wireless communication, mobile multimedia transmission, etc.

A Unified Deep Learning Method for CSI Feedback in Massive MIMO Systems

GAO Zhengguang[1], LI Lun[1], WU Hao[1],
TU Xuezhen[2], HAN Bingtao[1]

(1. State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen 518055, China;
2. The College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

DOI: 10.12142/ZTECOM.202204013

https: //kns.cnki.net/kcms/detail/34.1294.TN.20220426.0828.002.html
published online April 26, 2022

Manuscript received: 2021-11-15

Abstract: A unified deep learning (DL) based algorithm is proposed for channel state information (CSI) compression in massive multiple-input multiple-output (MIMO) systems. More importantly, the element filling strategy is investigated to address the problem of model redesigning and retraining for different antenna typologies in practical systems. The results show that the proposed DL-based algorithm achieves better performance than the enhanced Type II algorithm in Release 16 of 3GPP. The proposed element filling strategy enables one-time training of a unified model to compress and reconstruct different channel state matrices in a practical MIMO system.

Keywords: deep learning; channel state information; element filling strategy

Citation (IEEE Format): Z. G. Gao, L. Li, H. Wu, et al., "A unified deep learning method for CSI feedback in massive MIMO systems," *ZTE Communications*, vol. 20, no. 4, pp. 110 - 115, Dec. 2022. doi: 10.12142/ZTECOM.202204013.

1 Introduction

In 5G and Beyond networks, massive multiple-input multiple-output (MIMO) is considered one of the key enabling technologies to improve link capacity and energy efficiency for wireless communications[1-5]. To achieve these potential advantages, simultaneous channel state information (CSI) is required to optimize the precoding for massive MIMO systems. In frequency division duplex (FDD) MIMO systems of 4G, the downlink CSI obtained at the user equipment (UE) is sent to the base station, and vector quantization or codebook-based approaches are adopted as the compression algorithms for CSI to decrease feedback overhead[6]. However, the feedback overhead increases significantly in massive MIMO systems because the feedback quantity of the current methods increases linearly with the number of antennas. This challenge has inspired researchers to explore an effective algorithm to compress the CSI in massive MIMO systems. The technology of compressive sensing (CS) is exploited to address this issue[7-8]. Based on the uncorrelated sparse vector transformed from the correlated CSI matrix, the CS-based methods are expected to achieve an accurate performance for CSI compression. Several CS-based algorithms have been proposed in massive MIMO systems, such as the least absolute shrinkage and selection operator (LASSO) l_1-solver and approximate message passing (AMP)[9]. The advanced CS-based algorithms which include TV minimization by augmented Lagrangian and alternating direction algorithms (TVAL3) as well as block-matching and 3D filtering (BM3D)-AMP have also been proposed to improve the accuracy[10-11]. Although CS-based methods have been investigated comprehensively, it still has inherent disadvantages[11]. Firstly, the effectiveness of CS-based methods relies on the assumption that CSI matrices are sparse in some bases whereas channels are not always sparse in practical systems. And the random projection of CS-based methods cannot extract useful information from the channel structure of MIMO systems, which has negative impacts on the algorithm performance. Finally, the decoding process always requires iterative solving, therefore the decompression of the CS-based method is sub-optimal and time-consuming. In a word, the CS-based method cannot achieve high performance for the reason that the CSI matrix is not sparse enough under the large compression ratio, and the slow reconstruction of the CS-based method makes it difficult to adapt many real-time scenarios in practical systems. Recently, deep learning has been explored in signal detection and network planning[12-13]. Motivated by the rapid progress of deep learning in computer vision (CV), in particular, the successful trial of image compression and reconstruction by the autoencoder, the researcher has explored DL-based algorithms for CSI compression comprehensively.

A novel residual neural network-based model called CsiNet is proposed in Ref. [14], which shows that the performance of CsiNet outperforms existing CS-based methods significantly,

especially for low compression regions. To exploit the temporal correlations of CSI, a long-short time memory (LSTM) architecture is combined with CsiNet as CsiNet-LSTM in Ref. [15], and it shows that considering the temporal correlations benefits the accuracy of CSI reconstruction. The CsiNet is modified and redesigned as CsiNet+ in Ref. [16], which improves the performance of CSI compression. More importantly, a novel quantization layer is introduced in the DL model for end-to-end training, which meets the practical requirement of CSI feedback in massive MIMO systems. Recently two novel DL-based models called CRNet and ACRNet have been proposed for better performance in Refs. [17 – 18]. In Ref. [17], multi-resolution CRBlocks are designed in CRNet, and the warm-up aided training scheduler is implemented to achieve better performance. The result proves the effectiveness of multi-resolution CRBlocks and the novel training scheduler. In Ref. [18], a novel model called ACRNet is proposed to provide the state-of-the-art performance with network aggregation and parametric rectified linear unit (PReLU) activation. Besides, the network binarization technique is implemented to ensure the high performance and small memory cost. Most of the above works have achieved the state-of-art performance previously and outperformed CS-based methods significantly in some regions, while some problems still exist in the following aspects. Most enlightening works focus on novel designs of the DL model to improve the performance of CSI compression, but ignore the quantization of information in bit-streams for transmission in practical MIMO systems. These models should consider the quantization layer and have end-to-end training and testing to evaluate the performance of practical systems. In addition, the proposed DL-based algorithms are evaluated in the COST2100 dataset[19], which only includes data with the same shape. However, the shape of the CSI matrix changes with antenna arrangements in massive MIMO systems. Generally, misalignment problems exist between the previous model and the coming data with different shapes. To our knowledge, there are no published works discussing how to deal with this issue in practical systems. Motivated by this, a unified DL-based method for CSI feedback is proposed in massive MIMO Systems. The rest of this paper are organized as follows.

A novel DL-based network named ACRNet+ is proposed in Section 2. To improve the performance in the practical massive MIMO system, the advanced module of channel attention and spatial attention is used to enhance the ability of feature extraction. And a 3-bit uniform quantization layer is implemented in ACRNet+ for end-to-end training in Section 3, which minimizes the impact of the accuracy quantization of the model. In addition, an element filling strategy is proposed to address the incompatible problem of the trained model for the CSI matrix with a different size. Section 4 shows the experimental results that ACRNet+ provides better performance than the enhanced Type II (eType II) algorithm in the 901 dataset which focuses on outdoor scenarios with dual-polarized antennas. The element filling strategy enables the trained model to compress the diversified CSI matrices accurately without further training. Section 5 concludes the paper.

2 System Model

A simple single-cell downlink is adopted in massive MIMO systems with N_t antennas at the base station (BS) and N_r antennas at UE, where $N_t \geqslant 1$ and $N_r = 1$ in this paper. The system considers orthogonal frequency division multiplexing (OFDM) with subcarrier N_c[20], so the received signal y_n at the n-th subcarrier can be expressed as:

$$y_n = \boldsymbol{h}_n^H \boldsymbol{p}_n x_n + z_n, \tag{1}$$

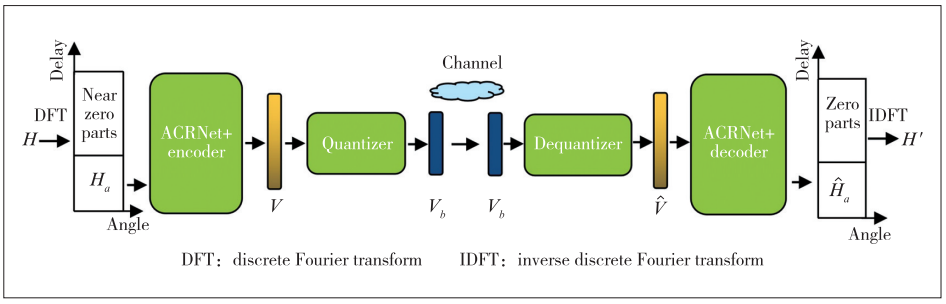
where $\boldsymbol{h}_n \in C^{N_t \times 1}$ is the downlink channel vector, and $\boldsymbol{p}_n \in C^{N_t \times 1}$ is the precoding vector based on CSI. $x_n \in C$ and $z_n \in C$ are the transmitted symbol and additive Gaussian noise for the n-th subcarrier. To obtain the advantage of channel gain in massive MIMO systems, the downlink CSI should be acquired at the BS to optimize the channel precoding. Since the downlink channel matrix $\hat{\boldsymbol{H}} = \left[\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_{N_c}\right]^H$ contains $2 \times N_c \times N_t$ elements of the float type, the direct feedback of CSI for downlink is not feasible obviously. In order to reduce the overhead of CSI feedback, a 2D discrete Fourier transform (DFT) is used to make the matrix sparse in the angular delay domain as[21]

$$\boldsymbol{H} = \boldsymbol{F}_d \hat{\boldsymbol{H}} \boldsymbol{F}_a^H, \tag{2}$$

where $\boldsymbol{F}_d$ and $\boldsymbol{F}_a^H$ are DFT matrices with the shape of $N_c \times N_c$ and $N_t \times N_t$ respectively. The obtained matrix $\boldsymbol{H}$ contains only the first N_a rows of useful elements whereas other rows of elements are near zero. Although the DFT can reduce the elements of the downlink channel matrix, the first N_a row of the transformed matrix called $\boldsymbol{H}_a$ is still too large to be sent directly through the uplink channel. According to the inaccuracy of the large compression ratio and the slowing decoding procedure of CS-based methods, a DL-based encoder and decoder are considered for CSI compression at UE and reconstruction at the BS. An auto-encoder is a neural network-based model to reconstruct the raw data through self-supervised learning. It firstly builds the main features into a lower-dimensional representation of the input data, and then the decoder tries to reconstruct the data as similarly as possible[22].

The overview of the DL-based model for uplink feedback is shown in Fig. 1. The CSI matrix $\boldsymbol{H}_a$ in the angular-delay domain is obtained from the DFT of $\hat{\boldsymbol{H}}$ and matrix truncation. The encoder of ACRNet+ compresses the input of $\boldsymbol{H}_a$ into a one-dimensional vector $\boldsymbol{v}$ with M elements. Therefore, the compressive ratio can be expressed as

$$\eta = \frac{M}{2N_a N_t}. \tag{3}$$



▲ **Figure 1. Pipeline of ACRNet+ model for channel state information (CSI) compression**

In practical systems, the bitstream is required for uplink feedback, so a 3-bit uniform quantizer is used to convert the float vector $\boldsymbol{v}$ into a binary vector $\boldsymbol{v}_b$. The above process is abstracted as

$$\boldsymbol{H} = F_q\left(F_{\text{en}}\left(\boldsymbol{H}_a, \boldsymbol{W}_{\text{en}}\right)\right), \tag{4}$$

where F_q denotes the function of quantization, F_{en} stands for the encoder of ACRNet+, and $\boldsymbol{W}_{\text{en}}$ is the trainable parameter of the encoder. After uplink transmission, the bitstream $\boldsymbol{v}_b$ is dequantized into the float vector, and then the float feature is reconstructed into $\hat{\boldsymbol{H}}_a$. The decoding process can be formulated as

$$\hat{\boldsymbol{H}}_a = F_{\text{de}}\left(F_{\text{dq}}\left(\boldsymbol{v}_b\right), \boldsymbol{W}_{\text{de}}\right), \tag{5}$$

where F_{dq} denotes the function of dequantization, F_{de} stands for the decoder of ACRNet+, and $\boldsymbol{W}_{\text{de}}$ is the trainable parameter of the decoder. After the decoding process, the estimated channel matrix for the downlink can be obtained from the inverse DFT of $\hat{\boldsymbol{H}}_a$.

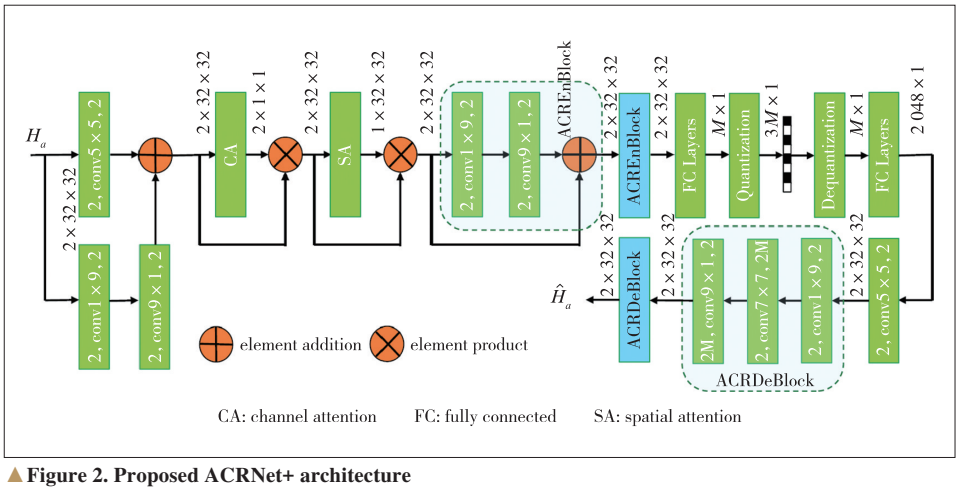
3 Description of ACRNet+

3.1 Design of ACRNet+

ACRNet is one of the most effective models in existing works, which provides the state-of-art performance for CSI compression in COST2100[18]. Based on the network aggregation technique, a novel feedback block that contains parallel convolutional groups is implemented to extract relatively independent features[23 - 24]. In addition, a learnable activation function of the parametric ReLU and an advanced training scheme are used to boost the performance of the model.

To inherit the advantages of ACRNet, ACREnBlock and ACRDeBlock are introduced in the proposed ACRNet+ . In addition, channel attention (CA) and spatial attention (SA) are implemented to extract the useful features accurately from the CSI matrices, especially for outdoor scenarios with the randomness of multi-path fading and unpredicted interferences[25]. Inspired by the design of multi-resolution networks for CSI feedback tasks in previous works[17], two independent channels with different convolution layers are built to provide more feature granularity. After the combination of the features from these two channels, CA and SA are used to make further extraction of the combined features. Different from the design of ACRNet, a quantized layer is added to convert the compressed data into bitstreams for feedback transmission on the uplink. At the BS, the bitstream is dequantized into the float features, and then the compressed vector from the dequantized layer is reconstructed into $\hat{\boldsymbol{H}}_a$ through one fully connected network and two ACRDeBlocks.

The detailed architecture of ACRNet+ is shown in Fig. 2. The image input $\boldsymbol{H}_a$ with the shape $2 \times H_a \times H_t$ is fed into two independent channels. The first channel includes a 5×5 convolution layer, and the second channel is made up of two convolution layers with a 1×9 kernel and a 9×1 kernel respectively. Then the outputs of the two channels are combined through element addition. To boost the representation power of networks, a convolutional block attention module (CBAM) is implemented to focus on important features and suppress unnecessary ones along two separate dimensions[25]. After the adaptive feature refinement by CBAM, the output of CBAM passes through the two ACREnBlocks which include a 1×9 kernel and a 9×1 kernel for further feature processing, and then the flattened feature from ACREnBlock is condensed into the vector with M elements. To meet the practical requirement for transmission of wireless communication, a 3-bit uniform quantizer is imple-



▲ **Figure 2. Proposed ACRNet+ architecture**

mented for quantization. The quantizer is embedded in neural networks as the quantization layer for end-to-end training, which can minimize the negative impacts on the model accuracy. At the BS, the bitstream is firstly recovered to the compressed vector through dequantization. Then the vector passes through a fully connected layer for element augmentation, the output is reshaped in the same dimension as the input. Finally, the reshaped feature passes one convolution layer with a 5 × 5 kernel and two ACRDeblocks which include a 1 × 9 kernel, a 7 × 7 kernel and a 9 × 1 kernel for the final reconstruction.

3.2 Generalization Scheme for CSI Compression

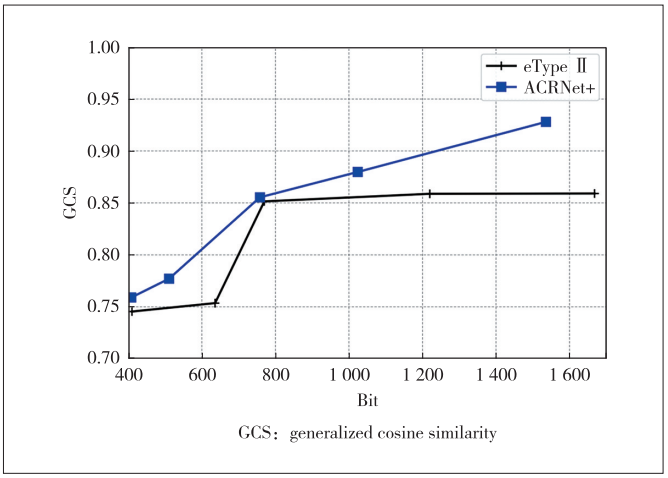
One of the main concerns for DL-based methods is the generalization problem. For data with the same shape, we can evaluate the model through the performance of cross validation and testing. DL-based methods for CSI compression have been proven effective in most previous works. However, the generalization of the DL-based model has never been discussed for data with different shapes. In practical MIMO systems, the shape of the downlink channel matrix changes with the arrangement of antennas. The misalignment problem happens in this scenario. The direct method is to get several models trained for different antenna typologies, but it requires huge computation resources for several well-trained models as well as the corresponding switching strategy. Therefore, the element filling strategy is proposed to support the training of a unified model for different scenarios covering several antenna combinations. At first, the dataset with the largest size is selected as the benchmark. Then the dataset with other shapes is filled by the constant elements with the same shape as the benchmark. Finally, a unified DL-based model is trained on the hybrid dataset covering the data from several antenna combinations in massive MIMO systems. Considering the fact that most elements in $\boldsymbol{H}_a$ are close to 0.5, the padding element is set to 0.5, which can decrease the disturbance of the padding elements for the compression and reconstruction of the actual elements.

In this paper, we consider three scenarios including 4 × 4 MIMO, 2 × 4 MIMO, and 1 × 8 MIMO with dual-polarized antennas, and the corresponding datasets are represented as data1, data2 and data3. During the training process, the real and imaginary parts of the data are represented as the third dimension, and the shapes for these datasets are 2 × 32 × 32, 2 × 16 × 32, and 2 × 16 × 32 respectively. According to the element filling strategy, we perform the padding operation to data2 and data3, which reshapes them as the size of 2 × 32 × 32. After the same shape for these scenarios is obtained, a unified model is trained on the dataset which randomly samples from data1, data2 and data3. We compare the performance of the model trained on the hybrid dataset with the model trained separately on one of the three datasets.

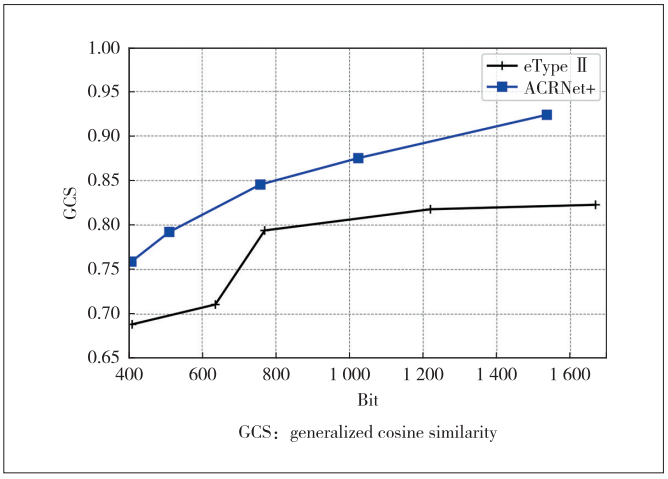
4 Experiment Results and Analysis

Most previous works are based on COST2100, which deploys a uniform linear array with 32 antennas at the BS and 1 024 subcarriers. In this paper, more complicated scenarios are considered to evaluate the effectiveness of the DL-based model. To evaluate the practical performance of ACRNet+, we first compare the performance of ACRNet+ with eType2 algorithm of Release 16 (R16) from 3GPP in two outdoor scenarios with dual-polarized antennas and two antenna topologies. The shape of the two datasets is 2 × 32 × 32. In addition, a unified model is trained on three datasets with different shapes through the element filling strategy. The performance of ACRNet+ trained on the hybrid dataset is compared with ACRNet+ trained separately on one of these datasets.

In order to evaluate the proposed model in more practical scenarios, 901data is generated according to the 3GPP Long Term Evolution (LTE) structure, in which parameters of channel models are specified in TR38: 901[26]. We compare ACRNet+ and eType2 algorithms on 901data containing two datasets, in which 16×1 MIMO and 8×2 MIMO with dual-polarized antennas are used. The generalized cosine similarity (GCS) of these two methods is presented in Figs. 3 and 4. The figures show that ACRNet+ outperforms eType II in terms of GCS when consuming similar bits. For the scenario in Fig. 3, the GCS of eType II is 0.745 4 under 410 bits. The corresponding GCS of ACRNet+ is 0.758 9 under 408 bits. It should be noted that it is difficult to completely match the number of bits for the two algorithms on the x-axis. The number of bits for eType II is 410, 636, 770, 1 220, and 1 668, and the consumed bits for ACRNet+ are 408, 511, 768, 1 024, and 1 536. We can see that the GCS of ACRNet+ is better than that of eType II although the ACRNet+ requires fewer bits. For the scenario in Fig. 4, the advantage of ACRNet+ is more obvious. The closest performance for ACRNet+ and eType II occurs when the number of bits is about 770. The corresponding GCS for eType II is about 0.793 9 where the



▲ **Figure 3. GCS of ACRNet+ and eType Ⅱ for the scenario with 1×16 multiple-input multiple-output (MIMO)**



▲ **Figure 4. GCS of ACRNet+ and eType Ⅱ for the scenario with 2×8 multiple-input multiple-output (MIMO)**

GCS of ACRNet+ under 768 bits is about 0.845 8. Finally, it can be seen from Fig. 3 that the GCSs of the algorithms are not linearly related to the consumed bits. The GCS cannot be significantly improved when the used bit is below some threshold, and the improvement is also unobvious when the consumed bit is enough for the eType II algorithm. These results provide a useful reference for the actual deployment of these algorithms.

One of the main concerns for DL-based CSI compression methods is the generalization of the model. When the topology of antennas changes, the coming data of the channel matrix are incompatible with the original DL-based model. The retraining of the model requires huge computation resources and training time. Therefore, an element filling strategy is proposed to unify the input shape. Then a unified model is trained on the datasets which cover several scenarios with different typologies. In the experiment, three datasets including 4×4 MIMO, 2×4 MIMO, and 1×8 MIMO with dual-polarized antennas are generated in outdoor scenarios, and the corresponding datasets are represented as data1, data2 and data3. The training, validation, and testing sets for each dataset contain 85 000, 5 000, and 10 000 samples. The shapes of these datasets are $2 \times 32 \times 32$, $2 \times 16 \times 32$, and $2 \times 16 \times 32$ respectively. At first, data2 and data3 are reshaped into $2 \times 32 \times 32$, where the padding element is 0.5 for all the places. We mix the reshaped datasets and randomly sample one-third of the mixed data as the training set. Therefore, the mixed training dataset also contains 85 000 samples. Finally, the performance of ACRNet+ trained on the mixed dataset is compared with the model trained on the original dataset to evaluate the effectiveness of the element filling strategy.

The results of ACRNet+ trained on the mixed dataset and the original dataset are presented in Table 1, in which ACRNetH represents the performance of the model trained on a mixed dataset and ACRNet+ stands for the model trained separately on the original dataset. We can see from the table that the performance of ACRNetH which needs to be trained once is only slightly lower than ACRNet+ which needs retraining for data with different antenna topologies. For example, the GCS of ACRNet+ under 15 times compression ratio is 0.746 2, 0.875 4 and 0.844 9, and the performance of ACRNetH that only requires one-time training reaches a similar performance as 0.722 8, 0.850 9 and 0.810 5. The results show that the proposed element filling strategy enables the unified training of the model for the dataset which contains the samples with different sizes, and the corresponding performance reaches a similar performance trained separately.

▼ **Table 1. Comparison between ACRNet+ and ACRNetH under the same compression ratio**

Dataset	Method	1/4		1/8		1/15	
		NMSE	GCS	NMSE	GCS	NMSE	GCS
Data1	ACRNet+	−7.22	0.887 9	−5.10	0.813 4	−3.865	0.746 2
	ACRNetH	−6.59	0.870 0	−4.70	0.795 8	−3.44	0.722 8
Data2	ACRNet+	−14.10	0.976 5	−9.78	0.937 5	−6.61	0.875 4
	ACRNetH	−12.38	0.966 1	−8.07	0.910 5	−5.82	0.850 9
Data3	ACRNet+	−12.62	0.969 8	−8.001	0.911 4	−5.678	0.844 9
	ACRNetH	−9.84	0.943	−6.812	0.882 5	−4.795	0.810 5

GCS: generalized cosine similarity NMSE: normalized mean squared error

One thing that should be noted is that the proposed model as well as the mentioned models in the paper addresses the CSI compression in low-speed scenarios within 3 km/h, while unknown and complex factors on the performance of the CSI feedback still exist in high-speed scenarios, which we plan to analyze in future works.

5 Conclusions

In this paper, a unified DL-based model called ACRNet+ has been proposed to compress the CSI in massive MIMO systems. The proposed model outperforms eType II algorithms in R16 of 3GPP in two outdoor scenarios. More importantly, the element filling strategy allows a unified training of the model on the dataset containing samples with different shapes, which enables the one-time training of DL-based model to address the CSI compression for different antenna typologies. The experimental results show that the performance of a unified model can reach a similar performance of the DL-based model trained separately for the dataset of a certain scenario.

Acknowledgement

Our gratitude goes to WANG Yongcheng, YANG Xikun and LUO Qingkai for the technical advices and the linguistic assistance.

References

[1] LU L, LI G Y, SWINDLEHURST A L, et al. An overview of massive MIMO: benefits and challenges [J]. IEEE journal of selected topics in signal processing,

2014, 8(5): 742 – 758. DOI: 10.1109/JSTSP.2014.2317671
[2] MARZETTA T L. Massive MIMO: an introduction [J]. Bell labs technical journal, 2015, 20: 11 – 22. DOI: 10.15325/BLTJ.2015.2407793
[3] WU H Q. Ten reflections on 5G [J]. ZTE technology journal, 2020, 26(1): 2 – 4. DOI: 10.12142/ZTECOM.202001001
[4] FANG M, DUAN X Y, HU L J. Challenges, innovations and perspectives towards 6G [J]. ZTE technology journal, 2020, 26(3): 61 – 70. DOI: 10.12142/ZTETJ.202003012
[5] WANG X Y. 5G: striving for sustainable growth amid expectations [J]. ZTE technology journal, 2020, 26(1): 64 – 66. DOI: 10.12142/ZTETJ.202001014
[6] GAO Z, DAI L L, WANG Z C, et al. Spatially common sparsity based adaptive channel estimation and feedback for FDD massive MIMO [J]. IEEE transactions on signal processing, 2015, 63(23): 6169 – 6183. DOI: 10.1109/TSP.2015.2463260
[7] KUO P H, KUNG H T, TING P G. Compressive sensing based channel feedback protocols for spatially-correlated massive antenna arrays [C]//Proceedings of 2012 IEEE Wireless Communications and Networking Conference. IEEE, 2012: 492 – 497. DOI: 10.1109/WCNC.2012.6214417
[8] LU L, LI G Y, QIAO D L, et al. Sparsity-enhancing basis for compressive sensing based channel feedback in massive MIMO systems [C]//Proceedings of 2015 IEEE Global Communications Conference. IEEE, 2015: 1 – 6. DOI: 10.1109/GLOCOM.2015.7417036
[9] DAUBECHIES I, DEFRISE M, DE MOL C. An iterative thresholding algorithm for linear inverse problems with a sparsity constraint [J]. Communications on pure and applied mathematics, 2004, 57(11): 1413 – 1457. DOI: 10.1002/cpa.20042
[10] KONG Q L, GONG R, LIU J T, et al. Investigation on reconstruction for frequency domain photoacoustic imaging via TVAL3 regularization algorithm [J]. IEEE photonics journal, 2018, 10(5): 1 – 15. DOI: 10.1109/JPHOT.2018.2869815
[11] METZLER C A, MALEKI A, BARANIUK R G. From denoising to compressed sensing [J]. IEEE transactions on information theory, 2016, 62(9): 5117 – 5144. DOI: 10.1109/TIT.2016.2556683
[12] GAO Z, YAN S, ZHANG J, et al. ANN-based multi-channel QoT-prediction over a 563.4 km field-trial testbed [J]. Journal of lightwave technology, 2020, 38 (9): 2646 – 2655
[13] GAO Z G, ZHANG J W, YAN S Y, et al. Deep reinforcement learning for BBU placement and routing in C-RAN [C]//Proceedings of Optical Fiber Communication Conference (OFC). OSA, 2019: 1 – 3. DOI: 10.1364/ofc.2019.w2a.22
[14] WEN C K, SHIH W T, JIN S. Deep learning for massive MIMO CSI feedback [J]. IEEE wireless communications letters, 2018, 7(5): 748 – 751. DOI: 10.1109/LWC.2018.2818160
[15] WANG T Q, WEN C K, JIN S, et al. Deep learning-based CSI feedback approach for time-varying massive MIMO channels [J]. IEEE wireless communications letters, 2019, 8(2): 416 – 419. DOI: 10.1109/LWC.2018.2874264
[16] LIU F, HE X C, LI C G, et al. CsiNet-plus model with truncation and noise on CSI feedback [J]. IEICE transactions on fundamentals of electronics, communications and computer sciences, 2020, E103. A(1): 376 – 381. DOI: 10.1587/transfun.2019eal2123
[17] LU Z L, WANG J T, SONG J. Multi-resolution CSI feedback with deep learning in massive MIMO system [C]//Proceedings of ICC 2020 – 2020 IEEE International Conference on Communications. IEEE, 2020: 1 – 6. DOI: 10.1109/ICC40277.2020.9149229
[18] LU Z L, ZHANG X D, HE H Y, et al. Binarized aggregated network with quantization: flexible deep learning deployment for CSI feedback in massive MIMO system [EB/OL]. [2021-10-01]. https://ieeexplore. ieee. org/abstract/document/9684243. DOI: 10.1109/TWC.2022.3141653
[19] LIU L F, OESTGES C, POUTANEN J, et al. The COST 2100 MIMO channel model [J]. IEEE wireless communications, 2012, 19(6): 92 – 99. DOI: 10.1109/mwc.2012.6393523
[20] STUBER G L, BARRY J R, MCLAUGHLIN S W, et al. Broadband MIMO-OFDM wireless communications [J]. Proceedings of the IEEE, 2004, 92(2): 271 – 294. DOI: 10.1109/JPROC.2003.821912
[21] RASHEED M H, SALIH O M, SIDDEQ M M, et al. Image compression based on 2D discrete Fourier transform and matrix minimization algorithm [EB/OL]. [2021-10-01]. https: //www. sciencedirect. com/science/article/pii/S2590005620300096
[22] WANG Y S, YAO H X, ZHAO S C. Auto-encoder based dimensionality reduction [J]. Neurocomputing, 2016, 184: 232 – 242. DOI: 10.1016/j. neucom.2015.08.104
[23] KRIZHEVSKY A, SUTSKEVER I, HINTON G E. ImageNet classification with deep convolutional neural networks [J]. Communications of the ACM, 2017, 60(6): 84 – 90. DOI: 10.1145/3065386
[24] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition [C]//Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition. IEEE, 2016: 770 – 778. DOI: 10.1109/CVPR.2016.90
[25] WOO S, PARK J, LEE J Y, et al. CBAM: convolutional block attention module [C]//Proceedings of the European Conference on Computer Vision. ECCV, 2018: 3 – 19. DOI: 10.1007/978-3-030-01234-2_1
[26] 3GPP. Study on channel model for frequencies from 0.5 to 100 GHz: TR 38.901 [S]. 2017

Biographies

GAO Zhengguang (gao.zhengguang@zte.com.cn) received his BS degree from Hubei Engineering University, China in 2013, MS degree from South China Normal University, China in 2016, and PhD degree from Beijing University of Posts and Telecommunications, China in 2020. In his doctor's degree program, he was a visiting PhD student in High Performance Networks group, University of Bristol, UK from Nov. 1, 2018 to Nov. 1, 2019. After graduation, he was selected for "LAN JIAN" program of ZTE Corporation as an algorithm researcher. His current research interests include 5G/6G communication technologies, mobile networks, and machine learning for future communications.

LI Lun received his MS degree in electronics and communication engineering from Harbin Insititute of Technology, China in 2018. He joined ZTE Corporation, China in 2018, where he is currently a technical pre-research engineer. His research interests include artificial intelligence/machine learning for wireless communications.

WU Hao received his BS degree from Beijing University of Posts and Telecommunications, China in 2010, and PhD degree from Southeast University, China in 2015, both in electrical engineering. He is now with the State Key Laboratory of Mobile Network and Mobile Multimedia Technology, ZTE Corporation, where he is a senior expert on wireless communication research and standardization. During 2011 – 2012, he was a visiting student at Columbia University, USA. Since 2016, Dr. WU has been a delegate representing ZTE Corporation in 3GPP RAN and RAN1, to which he has submitted numerous contributions on 4G and 5G technologies including MIMO, UE power saving, positioning and so on. His research interests include MIMO wireless communications, antenna array systems, and signal processing.

TU Xuezhen is currently pursuing her master's degree with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China. She received her bachelor's degree in computer science and technology from Henan University, China in 2020. Her research interest is mainly communication-efficient distributed learning.

HAN Bingtao received his BS degree from Tianjin University, China in 2001, and MS degree from Nankai University, China in 2004. He is the deputy director of the State Key Laboratory of Mobile Network and Mobile Multimedia Technology, and the leader for "Adlik" project of the LF AI & Data Foundation. Currently, he is the AI system architect of Central R&D Institute, ZTE Corporation. His current research interests include deep learning algorithms, AI systems, and network intelligence. He is the author and co-author for numerous patents and related monographs.

ZTE Communications

Table of Contents, Volume 20, 2022

Volume-Number-Page

Special Topic

Reconfigurable Intelligent Surface (RIS)

Simultaneous Wireless Information and Power Transfer: Technology and Practice

Federated Learning for IoT and Edge Computing

Wireless Communication and Its Security: Challenges and Solutions

Review

Research Paper

Volume-Number-Page

ZTE Communications Guidelines for Authors

Remit of Journal

ZTE Communications publishes original theoretical papers, research findings, and surveys on a broad range of communications topics, including communications and information system design, optical fiber and electro-optical engineering, microwave technology, radio wave propagation, antenna engineering, electromagnetics, signal and image processing, and power engineering. The journal is designed to be an integrated forum for university academics and industry researchers from around the world.

Manuscript Preparation

Manuscripts must be typed in English and submitted electronically in MS Word (or compatible) format. The word length is approximately 3 000 to 8 000, and no more than 8 figures or tables should be included. Authors are requested to submit mathematical material and graphics in an editable format.

Abstract and Keywords

Each manuscript must include an abstract of approximately 150 words written as a single paragraph. The abstract should not include mathematics or references and should not be repeated verbatim in the introduction. The abstract should be a self-contained overview of the aims, methods, experimental results, and significance of research outlined in the paper. Five carefully chosen keywords must be provided with the abstract.

References

Manuscripts must be referenced at a level that conforms to international academic standards. All references must be numbered sequentially intext and listed in corresponding order at the end of the paper. References that are not cited in-text should not be included in the reference list. References must be complete and formatted according to *ZTE Communications* Editorial Style. A minimum of 10 references should be provided. Footnotes should be avoided or kept to a minimum.

Copyright and Declaration

Authors are responsible for obtaining permission to reproduce any material for which they do not hold copyright. Permission to reproduce any part of this publication for commercial use must be obtained in advance from the editorial office of *ZTE Communications*. Authors agree that a) the manuscript is a product of research conducted by themselves and the stated co-authors; b) the manuscript has not been published elsewhere in its submitted form; c) the manuscript is not currently being considered for publication elsewhere. If the paper is an adaptation of a speech or presentation, acknowledgement of this is required within the paper. The number of co-authors should not exceed five.

Content and Structure

ZTE Communications seeks to publish original content that may build on existing literature in any field of communications. Authors should not dedicate a disproportionate amount of a paper to fundamental background, historical overviews, or chronologies that may be sufficiently dealt with by references. Authors are also requested to avoid the overuse of bullet points when structuring papers. The conclusion should include a commentary on the significance/future implications of the research as well as an overview of the material presented.

Peer Review and Editing

All manuscripts will be subject to a two-stage anonymous peer review as well as copyediting, and formatting. Authors may be asked to revise parts of a manuscript prior to publication.

Biographical Information

All authors are requested to provide a brief biography (approx. 100 words) that includes email address, educational background, career experience, research interests, awards, and publications.

Acknowledgements and Funding

A manuscript based on funded research must clearly state the program name, funding body, and grant number. Individuals who contributed to the manuscript should be acknowledged in a brief statement.

Address for Submission

http://mc03.manuscriptcentral.com/ztecom

ZTE COMMUNICATIONS
中兴通讯技术(英文版)

ZTE Communications has been indexed in the following databases:

- Abstract Journal
- Cambridge Scientific Abstracts (CSA)
- China Science and Technology Journal Database
- Chinese Journal Fulltext Databases
- Index of Copurnicus
- Ulrich's Periodicals Directory
- Wanfang Data
- WJCI 2021

ZTE COMMUNICATIONS
Vol. 20 No. 4 (Issue 81)
Quarterly
First English Issue Published in 2003

Supervised by:
Anhui Publishing Group

Sponsored by:
Time Publishing and Media Co., Ltd.
Shenzhen Guangyu Aerospace Industry Co., Ltd.

Published by:
Anhui Science & Technology Publishing House

Edited and Circulated (Home and Abroad) by:
Magazine House of ZTE Communications

Editorial Correspondence:
Add: 12F Kaixuan Building, 329 Jinzhai Road,
Hefei 230061, P. R. China
Tel: +86-551-65533356
Email: magazine@zte.com.cn
Website: http://zte.magtechjournal.com

Annual Subscription: RMB 120
Printed by:
Hefei Tiancai Color Printing Company
Publication Date: December 25, 2022

China Standard Serial Number: ISSN 1673-5188 / CN 34-1294/TN