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.

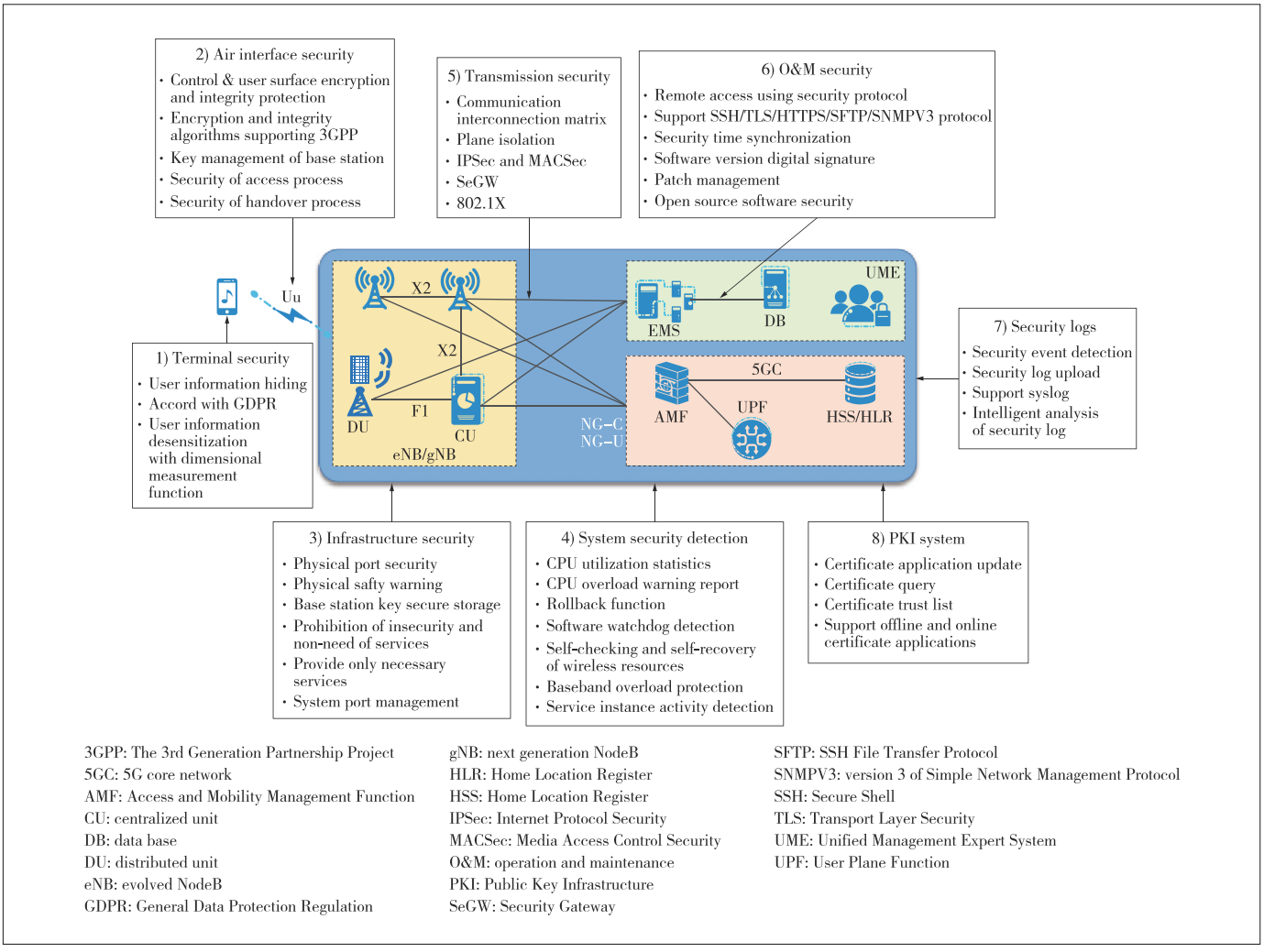
2 Key Security Technologies of 5G and 5G-Advanced

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.

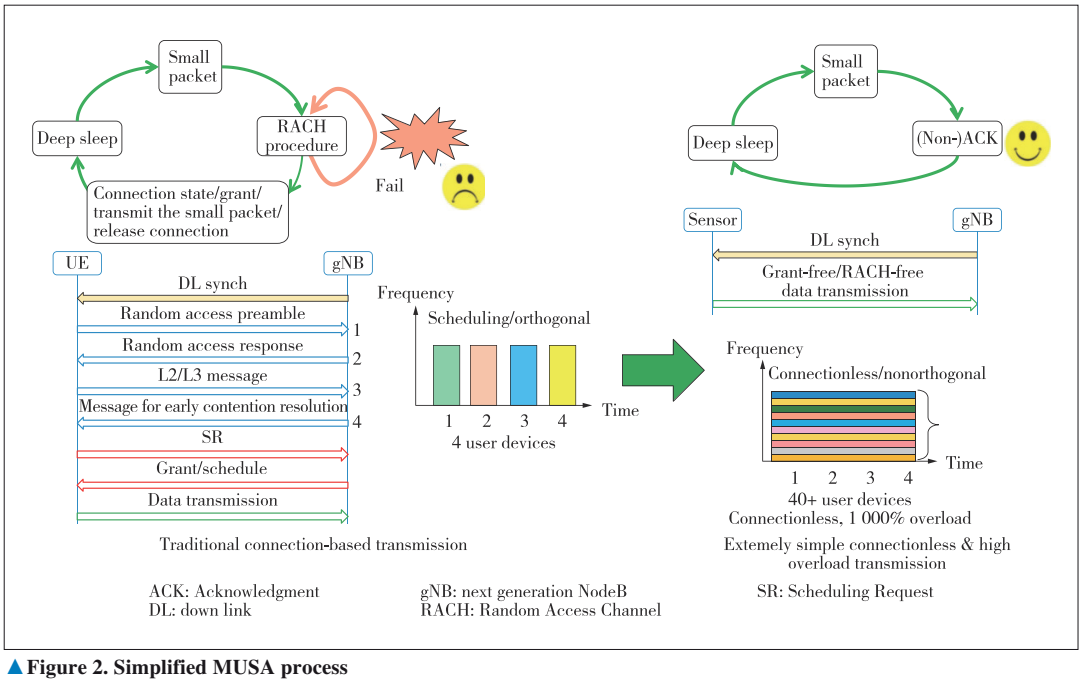
Further, with future development of the physical-layer technology, access may be initiated by using a device fingerprint message and the network may determine validity of the terminal after checking the fingerprint of the terminal device.

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).

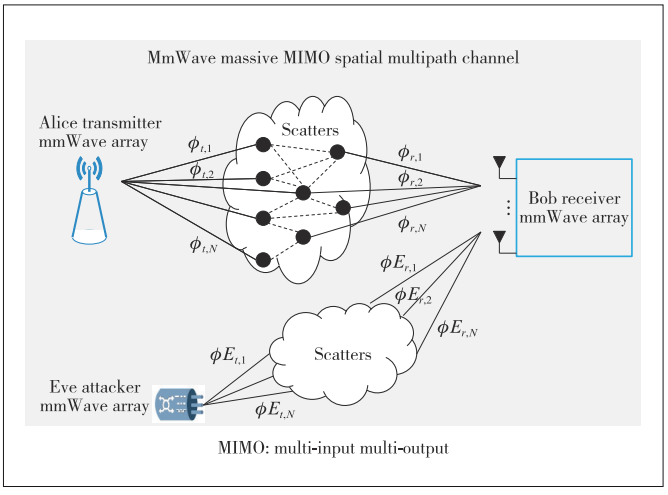
3) Sliding window detection

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

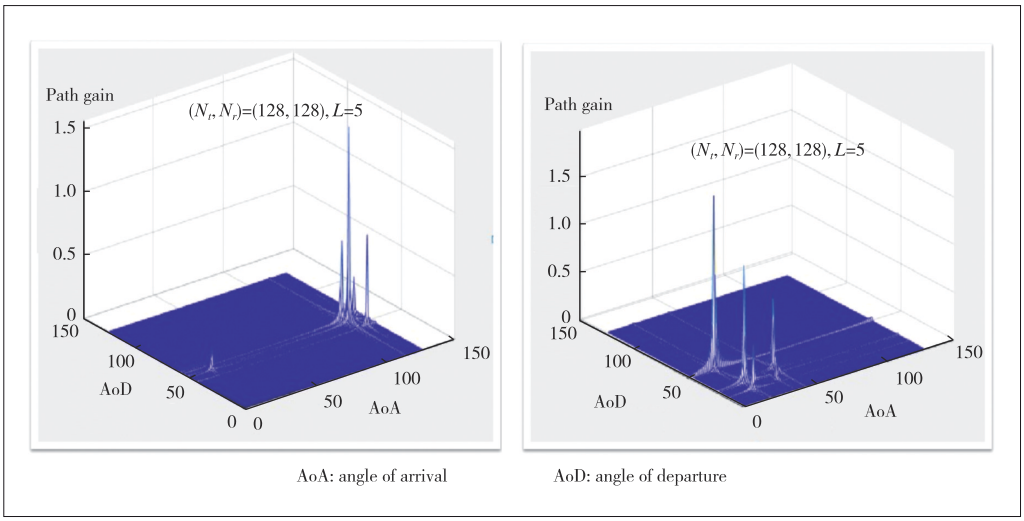
Currently, a channel model inadaptation problem exists in a high-frequency band channel fingerprint-based authentication scheme; eg., most authentication schemes do not have a channel model based on a millimeter wave frequency band, but still use a channel model in a sub-6 GHz system. Therefore, the 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.

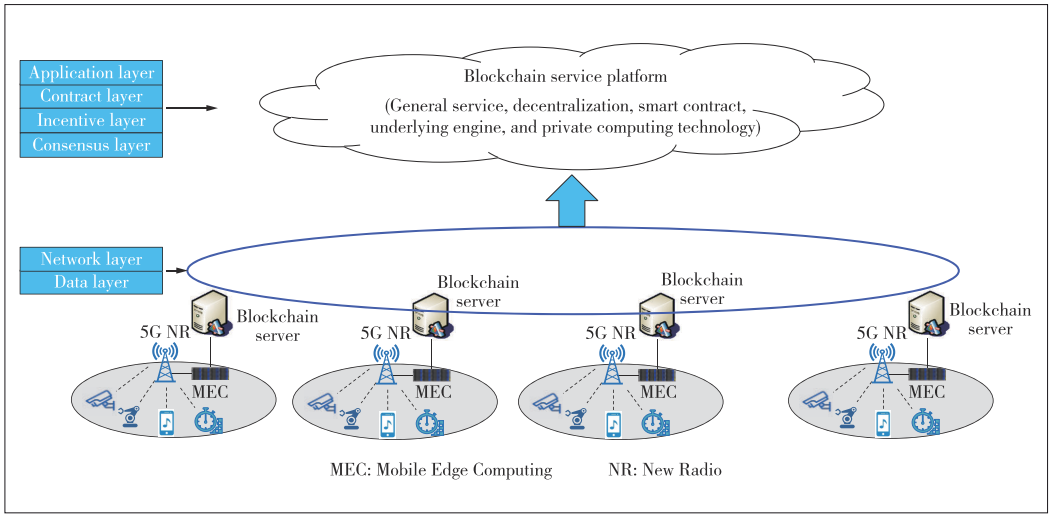
Blockchain can become a 6G intrinsic security technology or be integrated with other 6G technologies to enhance the security of 6G systems, better meeting the ToB application requirements, as shown in Fig. 5.

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.