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)

http://tech-en.zte.com.cn

March 2020, Vol. 18 No. 1

Domain Name and Identifier of Internet: Architecture & Systems

9 771673 518208 03>

The 8th Editorial Board of ZTE Communications

CONTENTS

ZTE COMMUNICATIONS March 2020 Vol. 18 No. 1 (Issue 69)

Invited Paper

Special Topic

Domain Name and Identifier of Internet: Architecture & Systems

CONTENTS

ZTE COMMUNICATIONS March 2020 Vol. 18 No. 1 (Issue 69)

Review

Serial parmeters:CN 34-1294/TN*2003*Q16*82*en*P*¥ 20.00*5000*11*2020-03

Ten Reflections on 5G

WU Hequan
(China Information Communication Technologies Group Corporation, Beijing 100083, China)

DOI: 10.12142/ZTECOM.202001001
http://kns.cnki.net/kcms/detail/34.1294.TN.20200313.1514.002.html, published online March 13, 2020

Abstract: 5G takes the concept of service-oriented architecture to replace the priority principle of network efficiency in the Internet to meet requirements of the industrial Internet and smart cities, such as high reliability and low latency. On the other hand, in order to adapt to the uncertainty of future business, 5G features the openness of services and the Internet protocols, different from the closeness of traditional telecommunication networks. Although 5G tries to have the advantages of both the Internet and telecommunication network, its realization still faces many challenges. In this paper, ten major issues concerning 5G networking and service offering are discussed.

Keywords: 5G; Software Defined Networking (SDN); Network Functions Virtualization (NFV); network slice; Service-Based Architecture (SBA); Mobile Edge Computing (MEC)

Citation (IEEE Format): H. Q. Wu, "Ten reflections on 5G," *ZTE Communications*, vol. 18, no. 1, pp. 01 – 04, Mar. 2020. doi: 10.12142/ZTECOM.202001001.

WU Hequan is an academician of Chinese Academy of Engineering (CAE). He was the vice president of CAE. Currently, he is the deputy director of the Advisory Committee for State Informatization, director of expert committee of Standardization Administration of China (SAC), director of the experts advisory committee for "Internet Plus" action plan, leader of State Internet of Things expert group, chief engineer of the major scientific and technological project of national "New Generation Broadband Wireless Mobile Communication Network," and director of Advisory Committee of Internet Society of China. He is also a senior member of IEEE. He has long been engaged in the research and development of digital networks and optical fiber communication systems; he has also taken charge of R&D projects on China's Next Generation Internet (CNGI) and 3G/4G/5G, as well as led and managed consulting projects on engineering science and technology. He won several prizes including Award of the Chinese Science and Technology Conference, the Second Prize of the National Science and Technology Progress Award, and the First Prize of Science and Technology Progress Award of Ministry of Posts and Telecommunications (MPT) of China. He has authored one book.

2019 is recognized as the first year of 5G commercialization. All the 5G commercial network operators, except the Chinese ones, have launched their 5G networks based on Non-Standalone (NSA) infrastructure, using their existing 4G core networks and new 5G base stations to provide enhanced mobile broadband capability for 5G terminals. On the other hand, China has decided to build 5G standalone (SA) core network in 2020 [1]. The SA mode can offer the capabilities of ultra-high reliability, ultra-low latency, wide-area coverage and massive connection, which NSA cannot guarantee. Besides, SA has greater efficiency of improving the mobile broadband capability than NSA. In this way, 2020 can be seen as a true beginning of 5G era.

In comparison with 4G, the 5G SA core network will be based on Service-Based Architecture (SBA) [2] to meet the service requirements of multi-service operation, low latency and high reliability, thus enabling such features as service openness, network slicing, Network Functions Virtualization (NFV), edge computing, and Internet based telecom protocols. The advent of the Internet was 50 years ago and the Internet protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP), implement data transmission based on connectionless mode and packet routing. Now, 5G has brought about a paradigm shift in mobile network architecture; its core network has connection-oriented capacity and the IP packet at Layer 3 is no longer the only forwarding element. Therefore, the communication network architecture today is undergoing profound changes never seen before after the Internet was born. We are facing many challenges to achieve the expected performance of large-scale 5G applications. In this article, we talk about ten important issues concerning 5G networking and service offering.

1) Software-Defined Networking (SDN) will play a big role in 5G networking.

SDN implements the splitting of data transmission and data control and treats the control plane as a network operating system to centrally manage different networks. With the support of Segment Routing IPv6 (SRv6), SDN also enables source routing by configuring an end-to-end route for each service flow based on big data and artificial intelligence; it then en-

codes and stores the routing information into the label stack of the IPv6 extension header of the source node and forwards the segment header to the nodes along the selected path. In this way, the intermediate nodes only need to conduct forwarding without any routing tasks, which saves the time for queuing and guarantees the low-latency forwarding in connection-oriented networks. Although SDN is expected to be a solution to real-time optimization of all kinds of service flows and nodes, multi-objective optimization of a large-scale low-latency network will bring a problem of routing conflict or divergence for SDN. This problem can be solved in two ways. One is to partition a large-scale topology and assign an SDN controller for each partition; however, inter-partition routing requires the multiple controllers to communicate service flows and network resource data with one another, leading to complex implementation of SDN. The other way is to ease the burden on SDN handling capability by forwarding part service flows in connection-oriented mode while handling the other service flows still in connectionless mode.

2) 5G changes traditional configuration of network elements.

With generic hardware (white box hardware) and software-defined networking elements, the NFV technology can flexibly implement layer-1. 5, layer-2, or layer-3 forwarding based on the specific requirements of a service flow, thus improving forwarding efficiency and dramatically reducing latency. NFV requires a network element to implement dedicated functions for different services synchronically. Once the services change, these functions will change accordingly. Therefore, it is necessary for NFV to capture accurate data of service flows and network resources in the entire network. NFV uses virtualization techniques to realize the decoupling of software and hardware and evolves toward the combination of a pool of hardware resources and microservice architecture of software applications. However, microservice has not achieved its goal of implementing network openness and interoperability yet, due to its lack of standards. Moreover, the simultaneous operation of SDN and NFV in 5G networks inevitably suffers the conflict of network resources. As for white-box network elements, a white box may have higher forwarding latency, compared with dedicated equipment; NFV performance even becomes a big challenge when white-box network elements and legacy network elements coexist in a network.

3) Network slicing is a key feature of 5G network and service.

Network slicing [5] can realize tailored Virtual Private Networks (VPN) for diversified services and use cases depending on their special requirements for such attributes as bandwidth, latency, and reliability, by implementing the orchestration of network resources in centralized network Operation and Maintenance (O&M) system. In this way, network slicing can support individualization services, especially for vertical industries. The VPN is actually not a new service in telecommunication networks, but it is built based on reservations and only offered for a very few service flows in legacy networks. In 5G system, new VPN services should be massive, real-time, and end-to-end, which makes it too idealized to set up network slices for any service demands. We should not forget the history of Asynchronous Transfer Mode (ATM) technology. If network slicing is extended from the core network to the access network, end-to-end slices will have to keep changing with the movement of users, which will certainly increase the complexity of slice management. It is also an unprecedented challenge to open the authority of organization VPN to customers to implement the provisioning of VPN finding, selecting, creating and management, as well as on-demand real-time dynamic adjustment. Furthermore, the inter-operator VPN connection requests operators to open their network resources and service data to each other, which is completely impractical. A potential solution is to set up network slices only for those services and use cases that have restrict requirements on such parameters as latency, packet loss rate, and reliability. This solution can implement the real-time creation of a VPN, free from the reservation that is mandatory for a VPN in any 4G network. Moreover, with traffic-based charging schemes, the provisioning of VPN services only to high-end customers to guarantee their Quality of Service (QoS) is unfair for low-end ones. Therefore, it is necessary to consider the design of value-oriented and QoS-based customer charging architecture.

4) SBA is an important innovation in 5G.

As an open service platform, SBA enables on-demand deployment of diversified intelligent service units, just like the use of apps on smart phones. The intelligence created by the assembly of intelligent units and flexible scheduling of network services implemented by service decoupling and modeling can respond to the unpredictability of 5G new services. Different from Intelligent Networks (IN) in the traditional telephony network architecture, the open SBA greatly enriches the sources of intelligent service units. However, SBA, with limited network resources and massive users, may also face potential conflicts between various intelligent service units, similar to the IN. The SBA opens up the closed service functions in operators' legacy networks, which also leads to new security threats. Moreover, working with SBA, the 5G mobile communication protocols are generally IP-based, which enables Internet applications to migrate to 5G system directly and further enhances its service capabilities. However, this also opens the door to the viruses and trojans on the Internet. Therefore, more effort is expected to be put into network security and data protection for 5G than that for 4G.

5) There is an inextricable link between Mobile Edge Computing (MEC) and 5G technologies.

MEC is a new paradigm for facilitating access to cloud computing capabilities, including storage and content delivery, at the edge of mobile networks, in order to enable latency sensitive services. In practice, a reasonable definition of granulari-

ty for MEC is a problem in terms of engineering. Various application terminals such as mobile terminals, robots, and intelligent connected vehicles will need to be switched across MEC hosts, which involves inter-MEC collaboration and reasonable allocation of functions in MEC and centralized clouds. This issue may lead to large overhead between MEC hosts and many interactions between MEC and centralized clouds, as well as incur delay. MEC is especially fit for those vertical business segments who want network operators to open network capabilities at the edge to them. Therefore, it is necessary to configure MEC with light cloud techniques like open source platforms and dockers for supporting third-party edge applications well. Moreover, opening MEC capabilities will inevitably make a big impact on operators' network management and data security.

6) 5G has a strict requirement for clock synchronization.

In SDN/NFV, service flows of all the network elements and big data of network resources are required to keep synchronous for absolute time alignment. A global vision in 5G system cannot be implemented without precise synchronization of different packets; a network scheduling decision based on inaccurate data may be worse. The IEEE Precision Time Protocol (PTP) 1588 is based on an assumption of the exact same delays for bidirectional propagation; however, in practical scenarios, the assumption is challenged and even the protocol itself hardly guarantees the precision of synchronization required.

7) 5G is pushing the transformation of Operations Support System (OSS).

5G system will implement real-time assignment of NFV functions to network elements, as well as the organization and lifecycle management of service-enabled network slices. In order to leverage 5G features, the OSS for 5G should enables automated orchestration of communication equipment and services based on statistics and intelligent analysis of big data from services and network resources. Real-time responses of OSS will rely on signaling control, rather than manual network management processes. A centralized OSS for the entire network facilitates overall control of network operations, but may struggle with processing capability and delay. However, if multiple OSSs are set up in different network regions, they will need data interchange and the coordination of a higher-layer central OSS.

8) Internet of Vehicles (IoV) is a new application scenario for 5G networks.

5G will be designed to guarantee low latency in both the access and core networks for the sake of IoV. Vehicles to Everything (V2X) communications are very different from personal communications. The average hops for a personal communication path are more than ten, but there are only one or two hops over a V2X path. Therefore, the advantages of NFV, network slicing and SRv6 in good control of delays in multi-hop cases are difficult to embody in the scenario of V2X communications. Moreover, legacy TCP/IP protocols cannot implement high transmission efficiency for short packets, which are the typical form of traffic in IoV. In the access network, point-to-point connection is generally used for personal communications. However, as for Vehicle-to-Vehicle (V2V) scenarios, point-to-multipoint, multipoint-to-mulitipoint, and even broadcast communication modes are used, which makes frequency arrangement more complex and latency slightly higher, because direct Device-to-Device (D2D) connectivity is hardly used and Vehicle-to-Network-to-Vehicle (V2N2V) connectivity is required. At present, many provinces in China share an internetwork node between network operators to implement their interconnection for personal communications. This is not a picture for the IoV. Because the IoV is very sensitive to latency, inter-operator V2V communications need direct interconnection in the neighborhood, in the same city at least. Therefore, it is necessary to set up local internetwork nodes in a city especially for the IoV.

9) Massive Internet of Things (IoT) is a featured application of 5G.

5G can access millions of IoT connections for every square kilometer, with an end-to-end transmission delay of less than 10 s and packet loss rate of no higher than 1%. For the sake of massive IoT terminals, group authentication schemes should be used to prevent any signaling storm. Security algorithms and protocols should also be lightweight, avoiding unwanted latency and the increase of energy consumption of the IoT terminals. Moreover, the diversified types of IoT terminals require that 5G user identity management method should adapt to the transformation from the current use of Universal Subscriber Identity Module (USIM) cards to flexible and diverse ways.

10) The industrial Internet spurs the emergence of 5G-based private networks.

Industrial digitalization should first implement the networking of production equipment of enterprises; among them, industrial robots, materials trolleys and workpieces on production lines need to be networked with wireless technologies. However, current available wireless technologies cannot meet the demands of the industrial Internet on reliability, scalability and anti-interference capability. Fortunately, the industrial Internet has become a featured application of 5G. For enterprises, 5G facilitates data transmission in either their Intranets or Wide Area Networks (WAN). Moreover, 5G operators can provide on-demand network slices for industrial enterprises, while the fact that operators' 5G networks are originally designed for the communications of public subscribers should be noted. In the Time Division Duplex (TDD) mode for operators' 5G networks, the downlink will be assigned more time slots than the uplink at the same carrier frequency for the sake of public communication services, especially video services, with downlink data much bigger than uplink data. TDD in the industrial Internet is just the opposite, with more time

slots for the uplink than that for the downlink, because sensors in the industrial Internet always send more uplink data but receive less downlink commands. When these two reverse schemes for assignment of TDD uplink and downlink time slots co-exist in the same base station, different carrier frequencies will be used to avoid mutual interference of the schemes, which will nevertheless limit the flexibility and validity of carrier frequency configuration. Moreover, large enterprises hope to build their 5G-based private networks in terms of management and security. Accordingly, the department administering radio spectrum need to allocate dedicated frequencies to the enterprises' private 5G networks.

In conclusion, constructing 5G SA networks and developing 5G SA applications can be seen as the start point of a new round of innovation for 5G technologies. As the first country to try the road of SA, China will face trial and error risk, as well as many questions worth thinking about. The road to achieving 5G innovations will be long.

References

[1] The Ministry of Industry and Information Technology. China Plans a Huge Investment in the Construction of 5G Stand-Alone Networks in 2020 [EB/OL]. (2019-09-21) [2019-12-23]. http://www.cac.gov.cn/2019-09/21/c_1570598110843638.htm
[2] The Ministry of Industry and Information Technology. 5G Mobile Telecommunication Network-General Technical Requirements of Core Network: YD/T 3615-2019 [S]. Beijing: Posts and Telecom Press, 2019
[3] ETSI. Network Functions Virtualisation (NFV); Virtual Network Functions Architecture: GS NFV-SWA 001 V1.1.1 [S]. 2014
[4] IETF. Segment Routing IPv6 for Mobile User Plane [EB/OL]. (2019-11-04) [2019-12-23]. https://datatracker.ietf.org/doc/draft-ietf-dmm-srv6-mobile-uplane
[5] 3GPP. Study on Management and Orchestration of Network Slicing for Next Generation Network (Rel-15): 3GPP TR 28.801 V15.1.0 [S]. 2018

(Translated from ZTE Technology Journal, vol. 26, no. 1)

LI Hui

Editorial：Special Topic on Domain Name and Identifier of Internet: Architecture & Systems

Guest Editor

LI Hui is a full professor of the Shenzhen Graduate School, Peking University (PKU), China. He received his B. Eng. and M. S. degrees from School of Information Engineering, Tsinghua University, China in 1986 and 1989 respectively, and Ph. D. degree from the Department of Information Engineering, The Chinese University of Hong Kong, China in 2000. He was the director of Shenzhen Key Lab of Information Theory & Future Internet Architecture and director of PKU Lab of China Environment for Network Innovations (CENI), National Major Research Infrastructure. He proposed the first co-governing future networking "Multi-Identifier System (MIN)" based on blockchain technology and has implemented its prototype on the real operators' network in the world, and the project "MIN: Co-Governing Multi-Identifier Network Architecture and Its Prototype on Operator's Network" has received the award of World Leading Internet Scientific and Technological Achievements by the 6th World Internet Conference in 2019. His research interests include network architecture, cyberspace security, distributed storage, and blockchain.

Domain name and identifier are the identity representation of each subject in the packet data network, which are the identity certificates of an organization or individual in the computer network. It is the registration and identification method of each subject, as well as the basis for network operators to charge users for service management. In fact, a country's entire collection of individual domain names and identifiers constitutes the country's virtual cyberspace, just as the global collection of domain names constitutes the global cyberspace under IP network. Domain name and identifier are in fact the objective embodiment and existence of virtual cyberspace. The so-called security of cyberspace is the security of the contents and devices of each domain name or its corresponding IP address in the space. Therefore, how to define the structure of domain name and identifier string and how to construct the allocation, registration, resolution and service management system of domain name and identifier are the most basic matters for the reliable, stable and safe operation of packet data networks. How to manage the whole lifecycle of domain name or identifier is related to the sovereignty of each country's cyberspace and is also fundamental to the security of each country's cyberspace.

The extension of the IPv4 network system swept the world at a speed that its inventors could not have anticipated, becoming the most important global infrastructure of the current information age. However, there are two major defects in the traditional IP Internet system. One is that the IP address and domain name are centrally managed by a single organization. The other is that the IP architecture does not have any guarantee scheme for network security and service quality. Decades of tinkering have proved impossible to cure.

The network itself is expanding the scale and dimension of its virtual space boundaries. The evolution of the Internet has experienced several stages, from a professional file information communication network used in scientific circles in the initial period to a consumer e-commerce network everyone could access, then to a physical interconnection network supporting automatic car driving, and finally to the value created network-industrial Internet emerging in recent years. It can be seen that network technology has indeed become the most important living and production infrastructure of human society. It is spawning hundreds of billions of domain names and identifiers for objects and data. Accordingly, its requirements on the reliability, security and service performance of the identification system are getting higher and higher.

Like the revolution of the earth around the sun, the existence of global packet data network has become an indispensable objective force in human society. We can only correct its deficiencies or defects in the course of its development or quietly replace them with new architecture without affecting the human society. This special issue is focused on the network architecture of the domain name or identifier and its system, around its evolution, security design and risk analysis model, specific industry application examples; eight papers are organized to introduce the current research trends and progress. Two of the papers discuss the gradual improvement of the traditional Domain Name Service (DNS) architecture and the architecture transformation; two papers discuss the combining of future network architecture to build industrial Internet identifier system; two papers discuss the traditional risk analysis model of IP network domain DNS and the

DOI: 10.12142/ZTECOM.202001002
http://kns.cnki.net/kcms/detail/34.1294.TN.20200324.1725.002.html, published online March 25, 2020

security design of identifier system for industrial Internet; the last two papers introduce the development of identification system for the industrial Internet and its concrete applications in different industries.

In response to the international community about the decentralization and the multilateral co-governing of Internet domain name and identifier management system, based on the proof of vote consensus algorithm of consortium blockchain, the first paper entitled "Prototype of Multi-Identifier System Based on Voting Consensus" proposes a network architecture for multiple kinds of identifiers, which is compatible with the domain name and able to be deployed over the current IP network, and has been verified on a large-scale operator's network.

Object traceability based on Radio Frequency Identification (RFID) is an important capability of the Internet of Things (IoT). GS1 Electronic Product Code (EPC) global network was a de-facto standard in RFID technology, which was developed from EPC network architecture. The inefficiency of the EPC network was caused by the distributed storage of unrelated data and the access control mechanism of discovery service. The second paper entitled "Advanced EPC Network Architecture Based on Hardware Information Service" proposes an enhanced solution to alleviate the challenges and improve the performance of the original EPC network architecture.

The host end-to-end system characterized by host IP address cannot meet the demands of the industrial Internet centered on data and services. The third paper entitled "Integrated Architecture for Networking and Industrial Internet Identity" proposes an overall framework of Information-Centric Networking (ICN)-based industrial network and Named Data Networking (NDN)-based factory extranet with Software Defined Networking (SDN). Introducing ICN into the industrial Internet facilitates the integration of industrial network and identity resolution system, flattens the overall architecture of the industrial Internet, and improves the efficiency of information retrieval, network scalability, and data security. The ubiquitous industrial Internet makes it a challenge to design a suitable identifier resolution system. The fourth paper entitled "Identifiers Management of Industrial Internet Based on Multi-Identifier Network Architecture" proposes an architecture to support multiple kinds of identifiers for the Industrial internet, including content name, identity, and location, besides the traditional IP address. The exhaustion problem of IP addresses may be solved, and the security, credibility, and availability of the industrial Internet system are enhanced with the application of multiple types of identifiers. A multi-identifier translation table is designed to establish an inter-translation scheme between multiple identifiers. An identifier addressing and routing algorithm is also presented to make it convenient to put the strategy into practice.

The security of domain name and identification system is the guarantee of reliable network operation. The fifth paper entitled "Risk Analysis of Industrial Internet Identity System" provides a detail and deep risk analysis of the current identity system represented by the domain name system and object identifier. According to the characteristics of the industrial Internet identity system, four open ecosystem planes are proposed, and a corresponding risk analysis view is established for various planes. Three defensive lines were proposed to establish the identity credit system. Security issue should be considered at the beginning of the design stage, and corresponding regulations should be setup to direct the system implementation. The sixth paper entitled "Security Risk Analysis Model for Identification and Resolution System of Industrial Internet" proposes an innovative security risk analysis model, which can help control risks at the initial stage of industrial Internet construction, provide guidance in the early design stage, and promote the healthy and sustainability of industrial identification and resolution system.

The last two papers are about the development and application of identifier system in industries. The seventh paper entitled "Construction and Application of Identifier Resolution in Automotive Industrial Internet" introduces the industrial ecosystem of the automobile industrial Internet built by Foton Motor Inc. This identifier resolution system facilitates continuous innovations, improving the design and manufacturing capabilities of the enterprise, the car ecosystem and the car life. Besides, it will not only enhance the stickiness of car customers and expand the influence and appeal of companies among users, but also promote product upgrading.

The industrial Internet technology will become more and more popular in different industries, and give birth to solution providers. The eighth paper entitled "Application of Industrial Internet Identifier in Optical Fiber Industrial Chain" is contributed by such a high-tech solution firm—Jiangsu ZTT LINK Ltd. It adapts the identifier system as a bridge to connect the information islands in the industry. It uses data to build a technology application ecolsystem based on the identifier resolution system, and develops several application objects and application scenarios of the industrial Internet identifier. As an example, its application into the optical fiber manufacturing industry has brought higher efficiency and lower cost.

The guest editor would like to thank the editorial office of *ZTE Communications* for their continuous support throughout the submission and review processes. The guest editor would also like to thank all the authors for contributing to this special issue and thank the reviewers for their timely and professional review of these papers.

Prototype of Multi-Identifier System Based on Voting Consensus

XING Kaixuan[1], LI Hui[1], YIN Feng[1], MA Huajun[1], HOU Hanxu[2], XU Huanle[2], Yunghsiang S. HAN[2], LIU Ji[1], and SUN Tao[3]

(1. Shenzhen Graduate School, Peking University, Shenzhen, Guangdong 518055, China;
2. School of Electrical Engineering and Intelligentization, Dongguan University of Technology, Dongguan, Guangdong 523808, China;
3. The Network and Information Center of Shenzhen University Town, Shenzhen, Guangdong 518055, China)

Abstract: With the rapid development of the Internet, the expansion of identifiers and data brings a huge challenge to the network system. However, the network resources such as Domain Name System (DNS) are monopolized by a single agency which brings a potential threat to cyberspace. The existing network architecture cannot fundamentally solve the problems of resource monopoly and low performance. Based on the blockchain, this paper designs and implements a new Multi-Identifier System (MIS), providing the analysis and management for different identifiers in the multi-identifier network. Our preliminary emulation results prove the correctness and efficiency of the algorithm. Besides, the prototype system of MIS has been tested on the real operators' network, realizing the function of co-governing, security supervision and data protection.

Keywords: blockchain; multi-identifier; co-governing

DOI: 10.12142/ZTECOM.202001003

http://kns.cnki.net/kcms/detail/34.1294.tn.20200318.0955.002.html, published online March 19, 2020

Manuscript received: 2019-12-16

Citation (IEEE Format): K. X. Xing, H. Li, F. Yin, et al., "Prototype of multi-identifier system based on voting consensus," *ZTE Communications*, vol. 18, no. 1, pp. 07 - 17, Mar. 2020. doi: 10.12142/ZTECOM.202001003.

1 Introduction

In nearly half a century, the Internet has experienced rapid development from simplicity to complexity. As the main carrier of cyberspace, the Internet plays a significant role in human life, social activity and even national security. However, serious problems such as resource exhaustion and poor business adaptability of the Internet network appear with the rapid development of big data and cloud computing. The semantic overload of IP address also reduces its scalability and mobility that further hinders security. In addition, under the existing system, the network resources such as Domain Name System (DNS) are monopolized by a single agency which brings a potential threat to cyberspace. Besides, malicious network users adopt a series of technical methods to hide individual IP address to escape the supervision and sanctions of the service provider. The content published by the malicious user is difficult to be discerned. These problems such as poor security and weak controllability under the traditional IP system need to be solved urgently.

To decentralize the management of the network architecture, blockchain [1] and other solutions [2] - [6] have recently been applied to build a future network realizing co-governing.

This work is supported by PCL Future Regional Network Facilities for Large-scale Experiments and Applications under Grant No. PCL2018KP001; Natural Science Foundation of China (NSFC) under Grant No. 61671001; Guangdong Province R&D Key Program under Grant No. 2019B010137001; National Keystone R&D Program of China under Grant No. 2017YFB0803204; Shenzhen Research Programs under Grant No. JSGG20170824095858416, JCYJ20190808155607340, and JCYJ20170306092030521; the Shenzhen Municipal Development and Reform Commission (Disciplinary Development Program for Data Science and Intelligent Computing).

Namecoin [7] and Blockstack [8] first applied blockchain to decentralize the management of the domain name system. However, in its underlying system based on public blockchain exists a bottleneck for its performance. To solve the problem, BENSHOOF et al. proposed an alternative solution of the DNS system based on blockchain and a distributed hash table named 3 [9], which provides solutions to current DNS vulnerabilities such as Distributed Denial of Service (DDoS) attacks. However, it risks leaking users' IP information and increases the difficulty of large-scale deployment. To mitigate the problem, the HyperPubSub system [10] uses the passive publish/subscribe receiving mode to reduce the traffic load and the delay caused by blockchain.

The above methods improve the performance of network and level of decentralization, respectively, but are unable to meet requirements [11] simultaneously. Our preliminary work proposed a new architecture: Multi-Identifier Network (MIN) [12] that constructs a network layer with parallel coexistence of multi-identifiers, including identity, content, geographic information and IP address. To solve the two major defects of the traditional network, we decentralize the identifier management by using consortium blockchain. This paper proposes a voting consensual-based multi-identifier management system Multi-Identifier System (MIS). MIS is a decentralized system composed of software and servers providing unified identifiers registration generation, classification, storage and management for identity, content, IP and other identifier spaces through the consortium blockchain Proof of Vote (PoV) [13]. Moreover, the MIS implements the digital signature to enhance security supervision and data protection.

The following chapter structures as follows. Section 2 introduces the MIN architecture. Section 3 describes the management system MIS and key technologies. Section 4 describes and analyzes the system flow of MIS, Section 5 shows the function realization and simulated verification of the prototype system, and Section 6 provides some concluding remarks and discusses ongoing and future research directions.

2 Architecture

2.1 Overview of Multi-Identifier Network

For the co-governing MIN, its decentralized management and large resolution capability enables a progressive transition from the existing network architecture to a new one.

MIN supports the coexistence of network identifiers including identity, content, geographic information and IP address. Identifiers in the network are identity-centric. All the resources are bound to the identity of their publishers. The architecture of MIN is shown in **Fig. 1**.

Fig. 2 shows the network hierarchy of MIN. It divides the whole network into hierarchical domains from top to bottom. The nodes in the top-level domain belong to the organizations of the major countries maintaining a consortium blockchain. The respective regional organizations govern the other domains. Among them, the registration and management mode of identifiers and the specific implementation details can vary. This low coupling guarantees the security of the network and enables the customization of each domain [13], [14].

The functions of a completed node in the network participate in the intra-domain management of users and the registration process of identifiers on the blockchain, as well as provide inter-translation and resolution services. In addition, there are supervisory nodes, individual users and enterprise users. Supervisory nodes are set up as the data access interfaces between the upper and lower domains. Each supervisory node has multiple identifiers.

The architecture of MIN includes a management plane and a data plane. The management plane supports traceable data signing and checking mechanism. The data plane provides the resolution for identity, content, geographic information and other identifiers. In addition, the data plane is responsible for packet forwarding and filtering. The reason for storing only the important data on-chain is to ensure efficiency, while all the information of the identifiers is stored off-chain.

2.2 Overview of Multi-Identifier System

The MIS we proposed in this paper is responsible for the generation and management of identifiers in the management plane. All user and publication resources are required to register their identifiers with the supervisory nodes. The supervisory nodes verify the identifier and reach a consensus through the consensus algorithm. It records the relevant attribution information and operation information on the blockchain to make the data in the whole network unified, tamper-resistant and traceable. All resources are required to register an identifier with a regulatory organization within the domain. Users can only access a resource in the network when its identifier has been approved by most organizations and successfully written on the blockchain. Meanwhile, the MIS uses a digital signature scheme that has the advantages of autonomy, uniqueness, security and traceability.

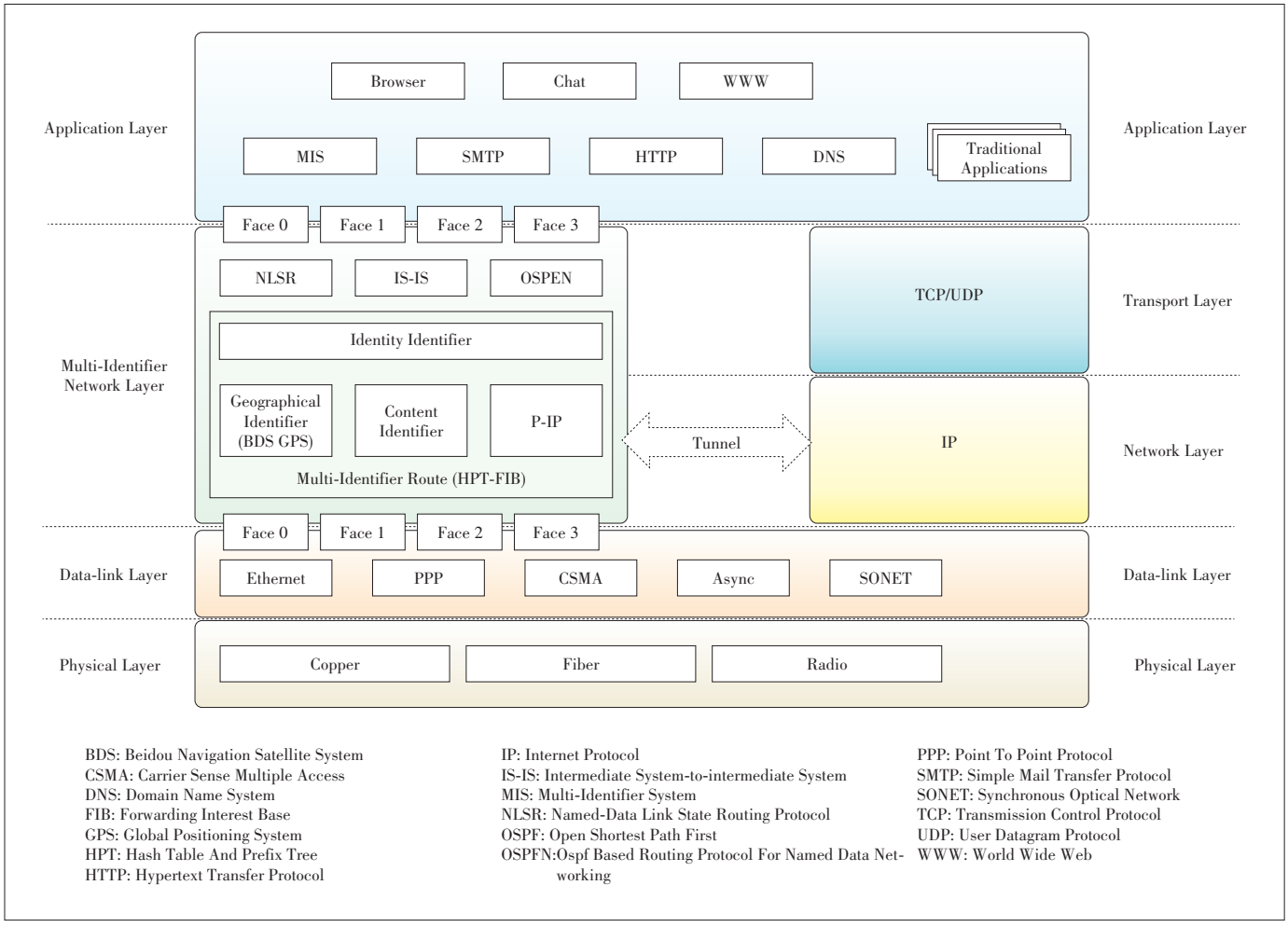
1) Autonomy.

The registration of identifiers is based on decentralized blockchain technology. The user independently defines the application for registration prefix on the premise of legal non-repetition. Besides, the registration and management rules are open, and there is no centralized control organization.

2) Uniqueness.

Real identity information such as biological information and ID number is registered to generate prefix to ensure uniqueness. Meanwhile, each user can use a prefix to identify the published resources, so that the users can identify and obtain the resource accurately.

3) Security and traceability.



▲**Figure 1. The architecture of Multi-Identifier Network.**

The prefix name must be registered and generated with real ID information to ensure that the identity of the content publisher is authentic and reliable. In addition, registration is successful only when an identity has been approved by most institutions and successfully written into the blockchain. Users who have successfully registered must use prefixes to publish content identification, and resource-publishing operations need to add user signature information. After receiving the request for publishing resources, blockchain verifies the user through signature to ensure that the resources published in the network space are safe and reliability. At the same time, the prefix name of content realizes network supervision by tracing resources to publishers.

MIS manages users' behaviors of publishing and access permission. The blockchain undeniably records illegal actions as well. Therefore, MIS keeps the cyberspace in an orderly and secure state that will direct Internet traffic to the post-IP multi-identifier network.

3 Key Technologies for MIS

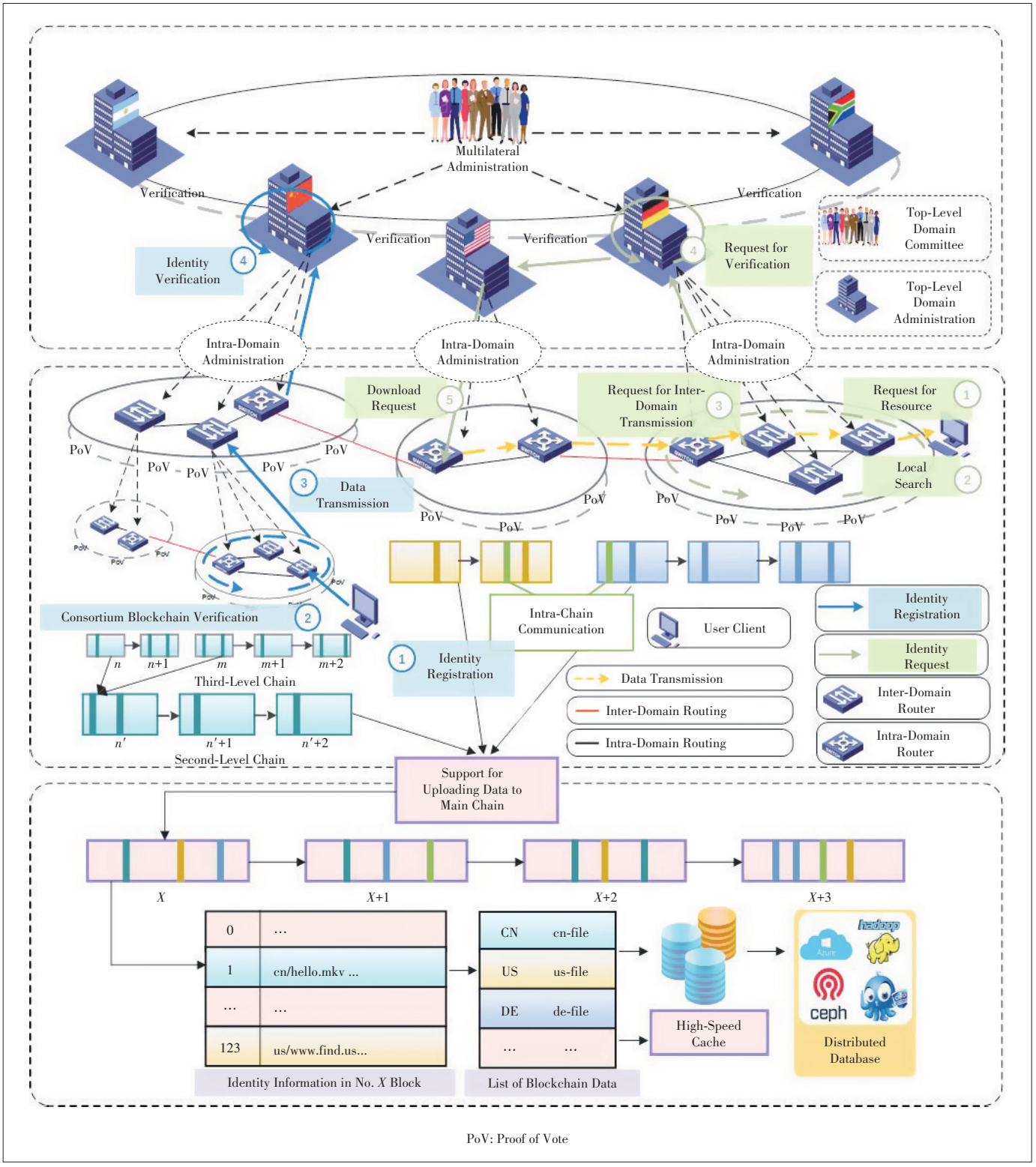
3.1 High-Performance Consensus Algorithm

The MIS system realizes the unified management of identifiers based on the improved PoV consortium blockchain consensus [13], a non-forking consensus algorithm for consortium blockchain. The core lies in the separation of voting rights and butler rights. The butler nodes work in a joint effort to conduct decentralized arbitration according to the votes of the commissioner nodes.

The PoV consensus divides the blockchain nodes into four characters: the commissioner, butler, butler candidate, and ordinary user. Each node has its own public-private key pair and digital certificate based on its identity and account number.

1) Commissioner.

The commissioners come from different regions or institutions maintaining a consortium blockchain together. Commissioners have the right to recommend, vote and evaluate the but-



▲**Figure 2. Multi-Identifier Network management architecture and operation flow.**

lers. They also have the obligation to verify and forward blocks and transactions. A block generated in the blockchain network will be sent to all commissioners for verification. When a block receives at least 51% of the votes, the block will be marked as valid and be added to the blockchain. The result of the voting can represent the will of all the commissioners.

2) Butler.

The butler is responsible for generating blocks in the current consensus round. The number of butlers is limited. A butler gathers transaction information from the network, packs them into a block, and signs the block. At the end of the term, the commissioner votes on the butler candidate to produce the next butler nodes. Besides, a node can be a commissioner and a butler at the same time.

3) Butler candidate.

As the number of butlers is limited, a butler comes from butler candidates by election and all commissioners vote candidates. If a candidate is lost in the election, he can stay online and wait for the next election

4) Ordinary user.

Ordinary users are responsible for processing block distribution and message forwarding if not being authorized. They can join or exit the network anytime without being authorized and their behaviors can be arbitrary.

There are two types of message voting in PoV for the transactions of identifiers and election: verification vote and confidence vote.

1) Vote for block generation.

The butler processes transactions to generate a block then sends it to all commissioners. A commissioner will encrypt the block header and return the signature to the butler if it agrees to produce the block.

2) Vote for confidence.

In the last duty cycle of the term, the commissioner sends signed voting transactions to the butler. After collecting and counting the ballot tickets, the butler generates a special block with election results and related records. Then the butler sends this block to all the commissioners for validation

3.2 Privacy Protection and Identity Management Solution

There are effective solutions to privacy protection in blockchain, but it is unable to achieve effective management of the participating nodes' identity and tracking of their behaviors. This is unacceptable in the MIS where there is a need to manage the behavior of participants.

The MIS provides privacy protection by applying identity management.

Nodes in the domain can be divided into three characters: the ordinary node, butler node and commissioner node according to their different missions. One node can concurrently act as more than one characters (**Fig. 3**). The ordinary nodes in green color have the right-to-know and the right-to-propose but cannot participate in the consensus process. The butler nodes own the rights to the generate blocks. The commissioner nodes have the right to verify the block; they can recommend, verify and evaluate the butler node and participate in consensus on the upper level. The commissioner nodes of the lower domain also act as a character in the upper domain.

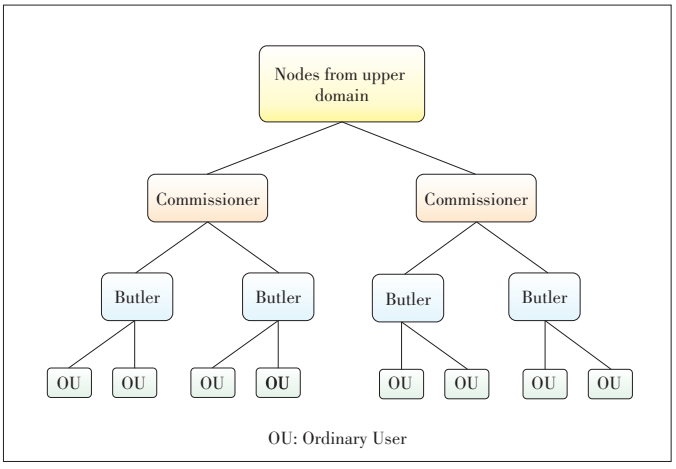
A hierarchical group/ring signature mechanism is used in the MIS due to the different node division. The node signatures in the network form a tree structure, and each parent node regards a group of subordinate nodes as its leaf nodes. The superior signature is generated by the combination of the subordinate signatures. The superior signature contains all the subordinate signature information. The verification of the superior signature also includes the verification of the tree with the signature as the root. Similar to normal group/ring signature requirements, no third party can trace the identity of the signer who has produced the signature with obtained signature and verified the public key. In addition, the security of the hierarchical group signature scheme requires that the group administrator can only trace the signer's leaf nodes' identity, while he/she cannot open the signatures generated by other groups' members. The group administrator of the parent node can quickly locate the problem group and identify the corresponding malicious users by establishing a group relationship between nodes of different levels and characters.

The following specific signature process is shown in **Fig. 4**.

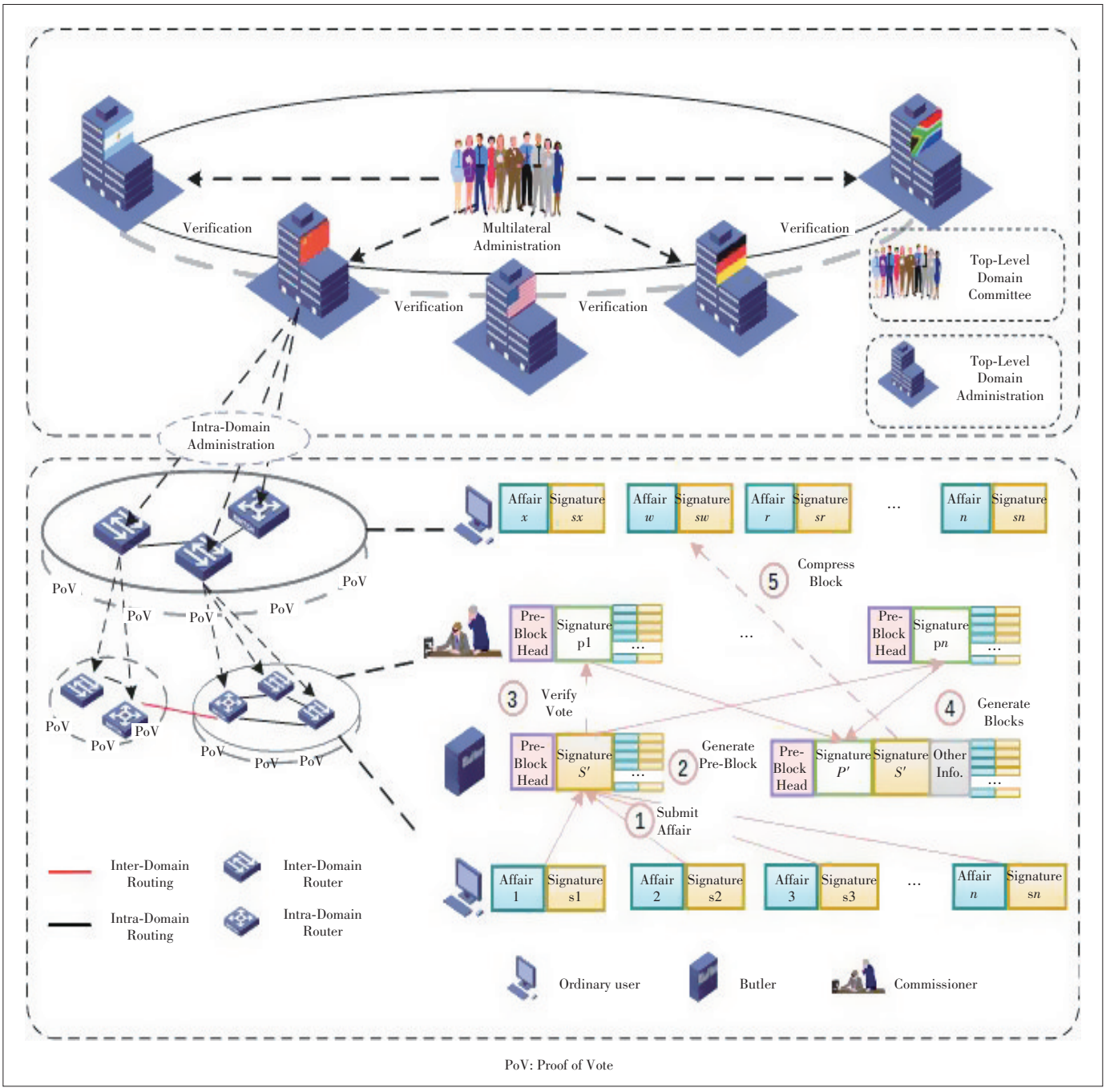
1) An ordinary node in the underlying domain produces a transaction and a signature S. It also receives intra-domain transactions, verifies the correctness of the transaction content and signature, and forwards the transaction to other nodes in the domain if correct. The butler nodes listen on intra-domain transactions and place valid transactions into the transaction pool.

2) The butler nodes periodically take some transactions out of the transaction pool and then encapsulates them into pre-blocks. The pre-blocks group with the ordinary nodes it belonged to generate a new parent group signature S'. S' and the pre-block are sent to all the commissioner nodes and other butler nodes in the domain. Once receiving the new parent group signature S' and the pre-block, the other butler nodes save them.

3) After the commissioner node receives the pre-block, they verify the transaction and butler signature in the pre-block. If it agrees to the generation of this block, it sends back its relat-



▲**Figure 3. Relationship among characters.**



▲**Figure 4. The specific signature processes.**

able ring signature P and timestamp to the butler node.

4) Before the deadline of generating a block, if the number of the commissioners' signatures and time stamps that the butler has received is more than the default value, the butler will generate a new superior ring signature and add it to the head of the pre-block to generate a block. This block will be broadcasted to all domains with block body and signature S'. Otherwise, if the number is no more than the default value or timeout, there will be no block generated in this consensus cycle. The default value can be set in different scenarios.

5) After receiving the block, the commissioner node verifies its signature S' and P', and then removes the transaction contained in the valid block from the transaction pool. If the commissioner nodes are not in the top-level domain, extract the block as a transaction, generate a new superior group signature S'' according to the attached butler signature S', and submit the transaction as an ordinary node of the previous domain. The other superior nodes continue to verify the signa-

ture. Only if the block is in the top-level domain and the number of commissioner nodes is greater than the default value, it will enter the legal state and have the final confirmation.

According to the characteristics of the hierarchical signature scheme, the MIS uses different data structures for block and pre-block (**Tables 1** and **2**).

The multi-identifier management and privacy protection mechanism based on digital signature is the key technology to ensure the security and reliability of the transaction of the consortium chain.

4 Implementation of MIS

1) User registration.

Every blockchain node in the MIS runs a service thread that is used to process requests sent by clients and provide corresponding services. **Fig. 5** describes the full process of user registration including request reception, verification and user registration information saving on the blockchain. User registration involves the communication between clients and blockchain nodes by embedding the user registration into the consensus of blockchain. The commission nodes verify and reach consensus so as to achieve the co-governing function.

The main function of the user client is to generate a pair of public and private keys for the user according to his/her identity. The two keys will be bound and then uploaded to the blockchain. At the same time, the user who publishes the resource will apply for a content name prefix when registering, thus realizing the binding of content identifier and public key. The users who have successfully registered can publish resources using the content name prefix produced through registration. The resource publishing needs to add the user private key information.

When a new user registers for using the network, MIS will require the user to submit the information such as prefix and real identity shown in **Table 3**. According to different security requirements, MIS can dynamically adjust the biometric information recognition strategy. For now, the prototype achieves the function for collecting fingerprint, facial and human iris information.

In particular, the prefix information follows the naming rules for hierarchical network domains. In addition, the system creates a table as shown in **Table 4** to store the successfully registered user information on the blockchain.

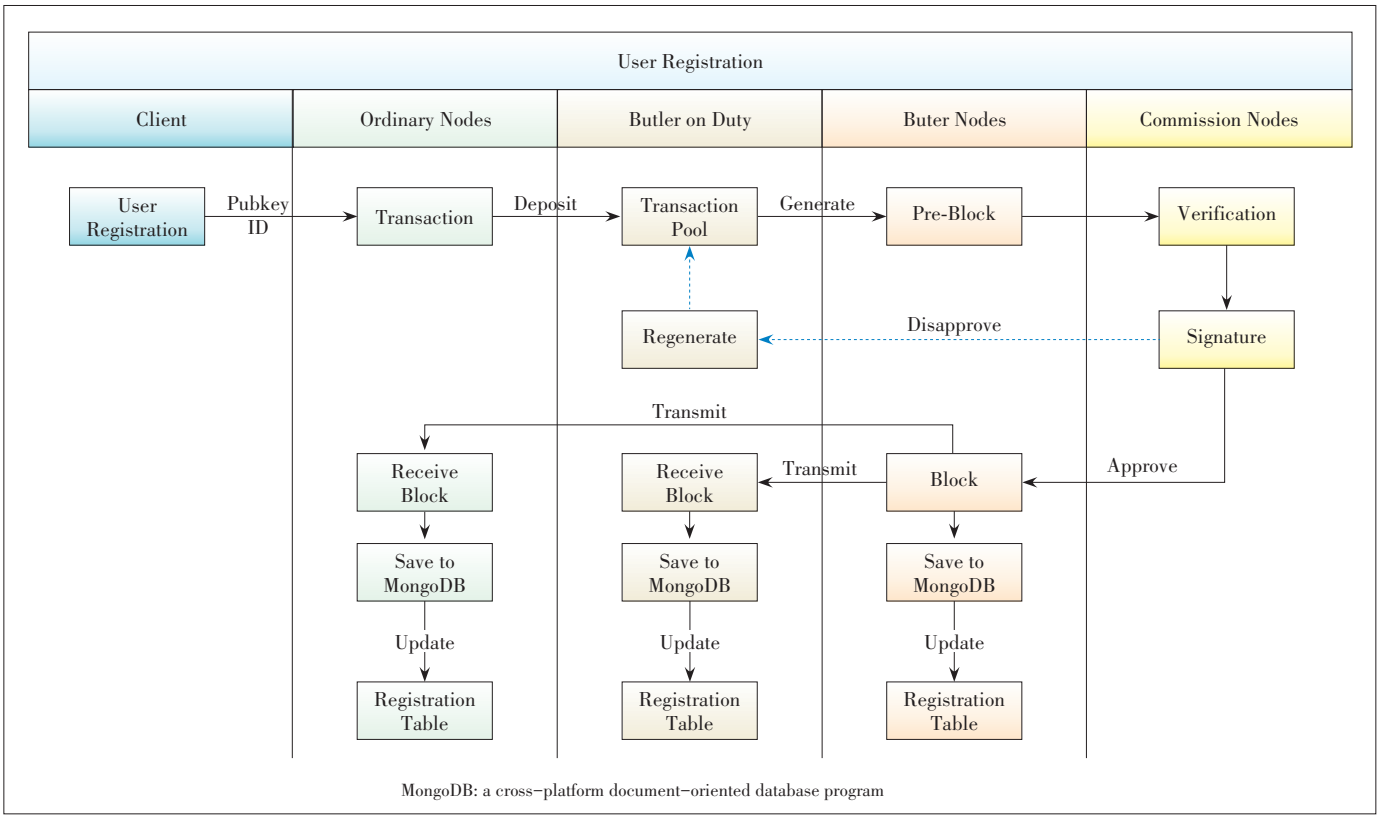
MIS generates a certificate for users once it receives and saves such an application. Then user identity and prefix binding process are completed. All the resources published by, for example, Jason will be located in /Jason. The certificate con-

▼Table 1. Data structure for block

Block		
Final-Header		**Body**
Pre-Header	Contain all property of Pre-Header	$\{tx\}=\begin{Bmatrix}tx_0,\\tx_1,\\\cdots,\\tx_i\end{Bmatrix}$
pre_header_ring_sign $\{\langle C\_time, C\_sign\rangle\}$	The Commissioner node returns the superior ring signature *C_time* is processor timestamp *C_sign* is the commissioner signature of *Pre-header* and *C_time*	
R	Random function obtained using the RandomNum algorithm that determines the butler number for the next block.	
M	The times of cycle to generate a block	
Time	Time of current block	

▼Table 2. Data structure for pre-block

Pre-Block		
Pre-Header		**Body**
Hash	Unique ID of block, Hash the SHA-256	$\{tx\}=\begin{Bmatrix}tx_0,\\tx_1,\\\cdots,\\tx_i\end{Bmatrix}$
Pre-Header	Hash Value of previous block	
Height (h)	The height of current block	
Height_LastSpecial (hs)	The height of special block next to the current block Especially when $h = hs$, the block is a special block Special block generated every B_w Usually $h - hs \leqslant B_w$	
M	The times of cycle to generate a block	
Puk (addr)	Encapsulate the public key of the butler of the current block; used to prove the accounting attribution of the current block	
Merkle_Root	Used to verify primitiveness and authenticity of all transactions	
…	Custom properties section	



▲Figure 5. User registration flow.

tains the user information and will be located under /Jason/cer. Other users who request for /Jason resources will first verify the certification under the /Jason/cer to check whether legal or not. Besides, the user information determines the access permission so as to achieve specific management functions underlying different scenarios.

2) User inquiry.

The user inquiry process consists of receiving the client's query user request, querying the user information from the user information table and returning it to the client. MIS system supports two types of queries: querying the corresponding user information through the user public key and querying all user information.

3) Resource publishing.

The content in the network also follows the rules of prefix names. **Fig. 6** shows the full process of resource publishing. When a user applies to publish content on the network, the published resource will be signed and submitted to the blockchain node for the consensus process. Specifically, the blockchain node that receives the request encapsulates the request in an ordinary transaction, and then several nodes verify and vote on this transaction. If the consensus is agreed, the inter-translated information will be stored in the table shown in **Table 5**.

4) Resource inquiry.

The resource inquiry function receives the client's identifier query request. The request inquires about the real address

▼Table 3. An example of the user application table

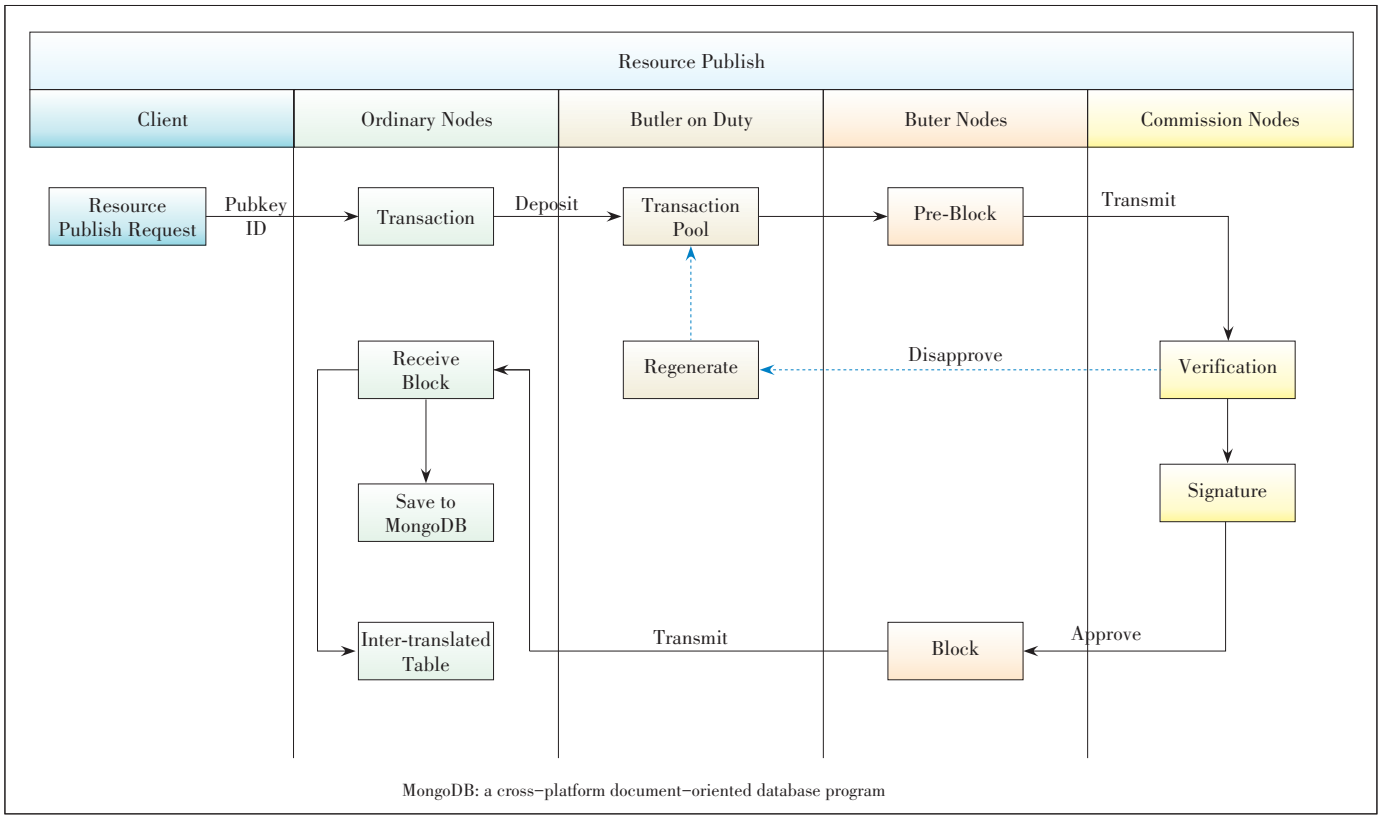
Registration Prefix	/Jason
Name	Jason
Valid ID	E77669818
Public key	54cd12s4d6g9mj
Biometric information	fs283n2n812b59u0sk42
Phone	9876070

▼Table 4. User information table

Key	Value	Description
Pub_KEY	String	Pub key of user
Prefix	String	Identifier prefix
Level	Int	User permission level
Real_msg	String	Real ID
Timestamp	Double	Time

▼Table 5. Content in inter-translation table

Key	Value	Description
Identifier	String	Resource
RealAdd	String	Real Address
Pub_KEY	String	Public Key
Hash	String	Hash Value
Timestamp	Double	Time stamp



▲**Figure 6. Resource publication flow.**

corresponding to the inter-translation information table. Similar to the user inquiry, MIS supports two types of queries: querying data by content identity and querying data by the resource publisher's public key.

5 Evaluation

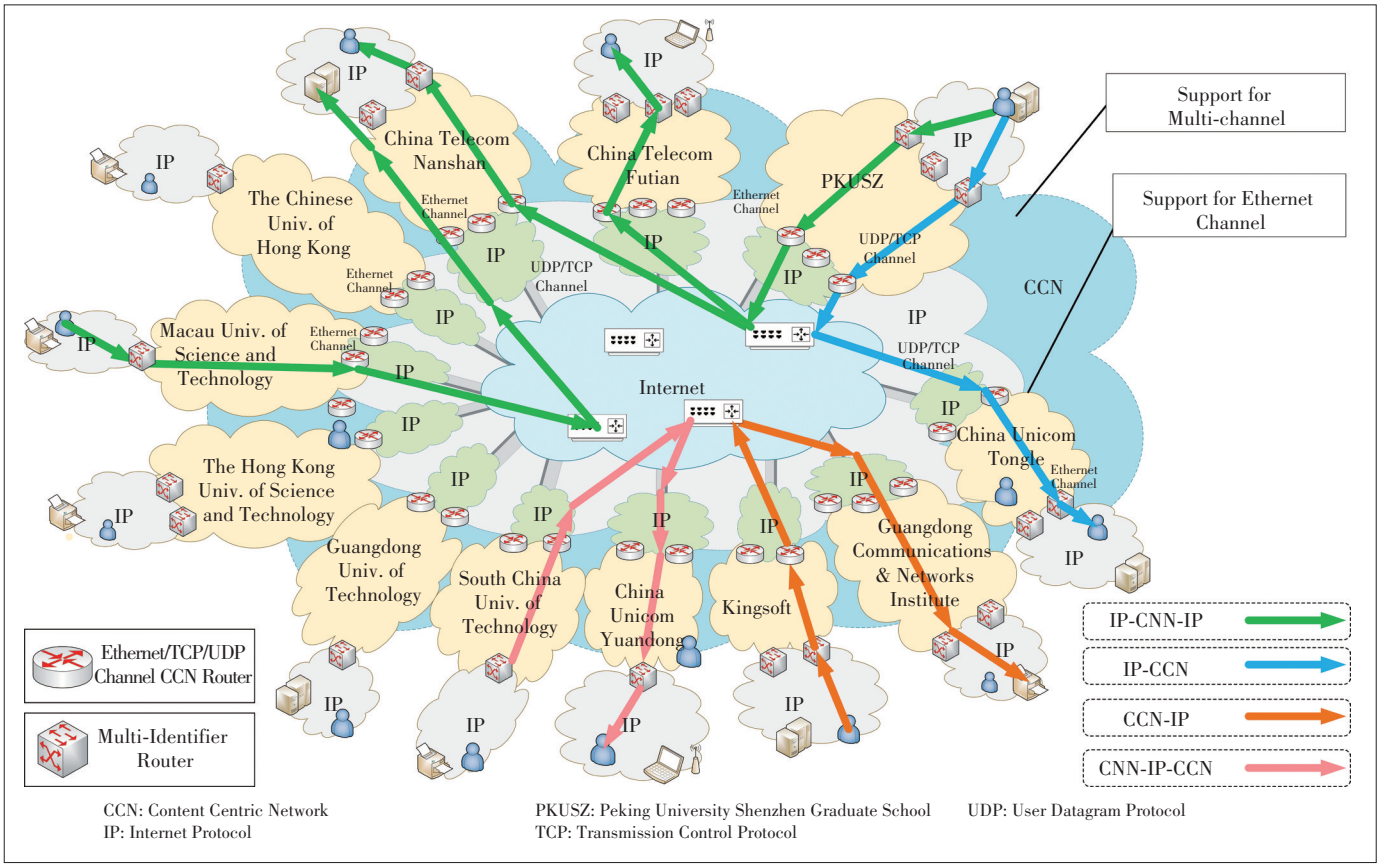
We develop a prototype system for MIS and deploy it on a real carrier-level operators' network consisting of the Chinese mainland and China's Hong Kong and Macao special administrative regions, as shown in **Fig. 7**. The system has realized the binding mechanism of user content and private key signature, as well as the blockchain function module and application function module. The system contains the user client and administrator client.

The main function of the user client is to generate a pair of public and private keys for the user and upload the user ID and public key to the blockchain so that the user ID is bound to the public key. Details are shown in **Fig. 8**. At the same time, the users who publish resources will apply for a content name prefix when registering, achieving the binding of content identifier and public key. The users who have successfully registered can publish content using the content name prefix applied during registration. The resource publishing operation needs to add the user's private key signature information. After the blockchain receives the request to publish the resource, it verifies the user rights through the signature. The signature also binds the user identity to the published content identifier, so as used for the inter-translation of the identity when routing.

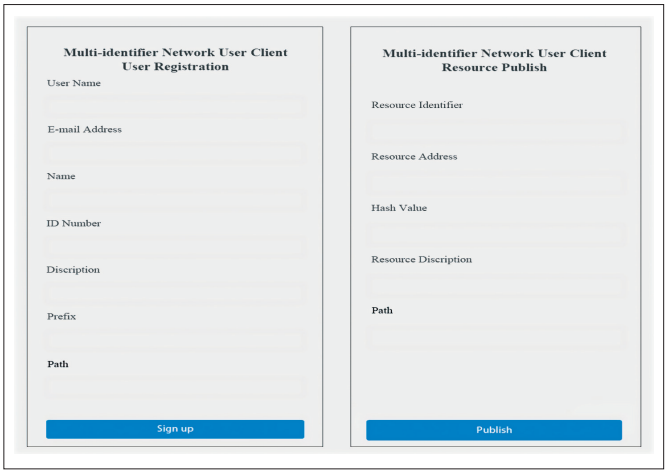
The main function of the administrator client of blockchain includes the real-time display of the running state of nodes, querying of blockchain data and configuration of blockchain nodes. Blockchain nodes store the identifier data, the user information stored in the form of transactions in each block. Each registration and publication generate a consensus for the whole network. The consensus is reflected in the number of transactions in the administrator interface that is shown in **Fig. 9**.

We deployed PoV and Practical Byzantine Fault Tolerance (PBFT) in a distributed environment and measured their throughput Transaction Per Second (TPS) separately. The experimental environment included five servers connected to the same router, each with 128 Gigabytes of memory and an Intel Xeon Silver 4116 processor. The PoV butler node was set to generate six PoV blocks, including five common blocks and one special block, within one service cycle. The theoretical calculation and experimental test results are shown in **Table 6**.

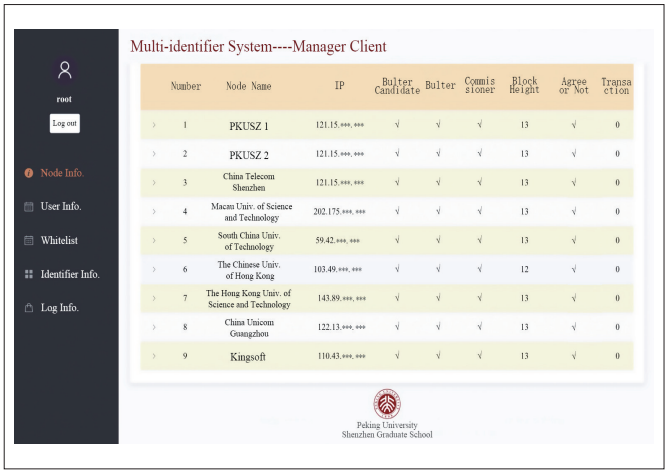
The results show that the performance trends of the two algorithms are consistent with the theoretical values. When the number of nodes is more than 100, the TPS of PoV declines slowly, and the rate of decline is slower than PBFT. Com-



▲Figure 7. The proposed prototype system for multi-identifier System.



▲Figure 8. Interfaces of user registration and resource publishing.



▲Figure 9. Status information of blockchain.

pared with the traditional PBFT algorithm, PoV has better scalability. This is because the PoV consensus two-phase commit communication complexity is only $O(n)$, which is only affected by the number of commission nodes. In terms of performance, the PoV consensus only needs one block to achieve tamper-proof transaction confirmation, with better performance and lower energy consumption than the public chain.

6 Conclusions

A future network should be decentralized, secure and compatible with the existing IP-based network. In this paper, we propose a multi-identifier system that constructs a network layer with a parallel coexistence of multiple identifiers, including identity, content, geographic information, and IP address. MIS provides the generation, management, and resolution ser-

▼Table 6. Comparison between PBFT and PoV

The Number of Nodes		10	50	100	150	200	250
PoV	Theoretical Results	11 669	2 277	1 105	715	521	406
	Experiment Results	8 408	1 686	848	552	381	314
	Uniformization	0.7205	0.7404	0.7674	0.772	0.7312	0.77
PBFT	Theoretical Results	11 457	1 427	330	116	52	27
	Experiment Results	8 305	1 083	257	84	40	20
	Uniformization	0.7249	0.7589	0.7788	0.7241	0.7692	0.7407
Ratio	Theoretical Results	1.02	1.6	3.35	6.16	10.02	15.04
	Experiment Results	1.01	1.56	3.3	6.57	9.52	15.7

PBFT: Practical Byzantine Fault Toleranc
PoV: Proof of Vote

vices of identifiers and uses consortium blockchain to enable decentralized management. MIS also implements data privacy protection. The test results based on the prototype system show that the network has excellent performance and can support real-world applications after further development.

References

[1] NAKAMOTO S, BITCOIN A. A Peer-to-Peer Electronic Cash System [EB/OL]. (2008) [2019-12-25]. https://bitcoin. org/bitcoin.pdf
[2] CACHIN C. Architecture of the Hyperledger Blockchain Fabric [C]//Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Chicago, USA, 2016, 310: 4
[3] CASTRO M, LISKOV B. Practical Byzantine Fault Tolerance [C]//OSDI. New Orleans, USA, 1999: 173 – 186
[4] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol [C]//Proc. Annual International Cryptology Conference. Cham, Switzerland: Springer International Publishing, 2017: 357 – 388. DOI:10.1007/978-3-319-63688-7_12
[5] KING S, NADAL S. PPcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake [EB/OL]. (2012-08-19) [2019-12-26]. https://decred.org/research/king2012.pdf
[6] SCHWARTZ D, YOUNGS N, BRITTO A. The Ripple Protocol Consensus Algorithm [J]. Ripple Labs Inc White Paper, 2014: 1 – 8
[7] LOIBL A, NAAB J. Namecoin. Namecoin. Info [EB/OL]. (2014) [2019-12-26]. https://Namecoin.info
[8] ALI M, NELSON J, SHEA R, et al. Blockstack: A Global Naming and Storage System Secured by Blockchains [C]//Annual Technical Conference. Denver, USA, 2016: 181 – 194
[9] BENSHOOF B, ROSEN A, BOURGEOIS A G, et al. Distributed Decentralized Domain Name Service [C]//IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). Chicago, USA: IEEE, 2016: 1279 – 1287.DOI:10.1109/ipdpsw.2016.109
[10] ZUPAN N, ZHANG K W, JACOBSEN H A. Hyperpubsub: a Decentralized, Permissioned, Publish/Subscribe Service Using Blockchains [C]//Proc. 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos. New York, USA: ACM, 2017: 15 – 16.DOI: 10.1145/3155016.3155018
[11] WU H Q. Reflections on the Reform of Network Architecture [J]. ZTE Technology Journal, 2019, 25(01): 2 – 4. DOI: 10.12142/ZTETJ.201901001
[12] LI H, WU J, XING K, et al. The Prototype and Testing Report of Multilateral and Multi-mode Identification Domain Management System [J]. Scientia Sinica Informationis, 2019, 49(09): 1186 – 1204. DOI: 10.1360/N112019-00070
[13] LI H, LI K, CHEN Y, et al. Determining Consensus in a Decentralized Domain Name System: US Patent App. 15/997,710 [P]. 2018
[14] LI H, WANG X, LIN Z, et al. Systems and Methods for Managing Top-Level Domain Names Using Consortium Blockchain: US10178069B2 [P]. 2019

Biographies

XING Kaixuan is a postgraduate student of Shenzhen Graduate School, Peking University, China. His research interests include new architectures and new generations of information communication technology.

LI Hui (lih64@pkusz.edu.cn) received the B.Eng. and M.S. degrees in information engineering from Tsinghua University, China in 1986 and 1989, and Ph.D. degree in information engineering from The Chinese University of Hong Kong, China in 2000. He is currently a professor with Peking University, China. His research interests include future network architecture, cyberspace security, and blockchain technology.

YIN Feng is a postgraduate student of Shenzhen Graduate School, Peking University, China. His research interests include blockchain technology and network security.

MA Huajun is a postgraduate student of Shenzhen Graduate School, Peking University, China. His research interests include network security and distributed system technology.

HOU Hanxu received the B.Eng. degree in information security from Xidian University, China in 2010 and Ph.D. degrees in information engineering from The Chinese University of Hong Kong, China in 2015 and from the School of Electronic and Computer Engineering, Peking University, China. He is now an assistant professor with the School of Electrical Engineering & Intelligentization, Dongguan University of Technology, China. His research interests include erasure coding and coding for distributed storage systems.

XU Huanle received the B.Sc. (Eng.) degree from the Department of Information Engineering, Shanghai Jiao Tong University, China in 2012 and Ph.D. degree from the Department of Information Engineering, The Chinese University of Hong Kong, China in 2016. His primary research interests focus on job scheduling and resource allocation in cloud computing, decentralized social net-works, parallel graph algorithms and machine learning. He is also interested in designing wonderful algorithms for real applications and practical systems using mathematical tools.

Yunghsiang S. HAN received his Ph.D. degree from the School of Computer and Information Science, Syracuse University, USA in 1993. Now he is with School of Electrical Engineering & Intelligentization, Dongguan University of Technology, China. He has also been a chair professor at Taipei University, China since February 2015. His research interests are in error-control coding, wireless networks, and security. Dr. HAN was a winner of the 1994 Syracuse University Doctoral Prize and a Fellow of IEEE. One of his papers won the prestigious 2013 ACM CCS Test-of-Time Award in cybersecurity.

LIU Ji is the director of the Information Office at Shenzhen Graduate School, Peking University. His research interest is new network architecture.

SUN Tao is the director of The Network Information Center of Shenzhen University Town. His research interests include blockchain and cyberspace security.

Advanced EPC Network Architecture Based on Hardware Information Service

HAN Tianyu, ZHU Siyu, XIE Bin, and TIAN Juan

(China Academy of Information and Communications Technology, Beijing 100191, China)

Abstract: Object traceability based on Radio Frequency Identification (RFID) is an important capability of the Internet of Things (IoT). GS1 EPCglobal, a de-facto standard in RFID technology, develops Electronic Product Code (EPC) network architecture, which mainly includes EPC Information Service (EPCIS), Object Name Service (ONS), and Discovery Service (DS). This architecture is used to capture and share standardized events representing various aspects on EPC object. However, the EPC network architecture also faces challenges; for example, the separate management of unrelated event data and master data may increase time consumption when an application extracts valuable information by combing them. A Hardware-Based Information Service (HIS) device is raised in this paper, which is installed on the specific EPC tagged object directly and this could alleviate the problem above. The HIS could store the event data and master data related to the EPC identifier centrally and the application could gain the basic information based on the data stored in the HIS without utilizing ONS, DS and EPCIS.

Keywords: EPCIS; lifecycle information; hardware information service

DOI: 10.12142/ZTECOM.202001004

http://kns.cnki.net/kcms/detail/34.1294.TN.20200316.1731.010.html, published online March 17, 2020

Manuscript received: 2019-12-01

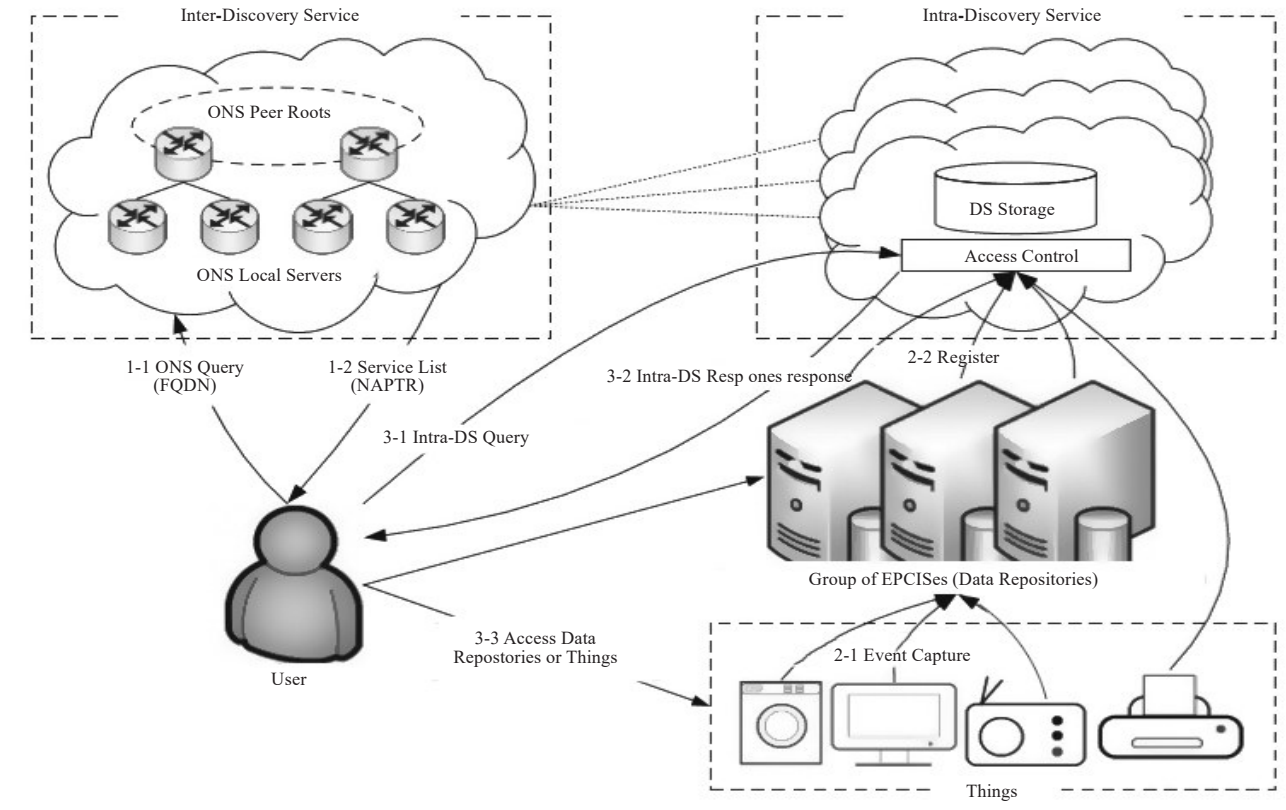
Citation (IEEE Format): T. Y. Han, S. Y. Zhu, B. Xie, et al., "Advanced EPC network architecture based on hardware information service," *ZTE Communications*, vol. 18, no. 1, pp. 18–23, Mar. 2020. doi: 10.12142/ZTECOM.202001004.

1 Introduction

The Electronic Product Code (EPC) network system is based on the Radio Frequency Identification (RFID) and Internet architecture. It assigns a globally unique encoding to each physical object. EPC technology system is considered as a scientific and authoritative identification system. EPC encodings are mainly aimed at improving the reliability and efficiency of supply chains. They are widely used in some open circumstances, for example, the smart agriculture and logistic. The EPC network system basically includes EPC identifier, EPC Information Service (EPCIS), Object Name Service (ONS), and Discovery Service (DS).

Fig. 1 shows one of the most widely used EPC network system [1]. In response to Fully Qualified Domain Name (FQDN) typed ONS query, ONS Returns Naming Authority Pointer (NAPTR) typed service list for the given object. Here, FQDN and NAPTR belong to the standard massage formats of Domain Name System (DNS). By adding end-point of DS as one of the service elements in ONS, user can access DS which actually locates the desired data repositories (Steps 1-1 and 1-2 in Fig. 1). DS has two data flows: write and read flows. The

This work was supported by the 2018 Industrial Internet Innovation and Development Project —— Industrial Internet Identification Resolution System: National Top-Level Node Construction Project (Phase I).



▲**Figure 1. Overview of discovery service.**

write flow occurs when the event is captured from things and the spatial-temporal data extracted from the event is registered to DS (Steps 2-1 and 2-2 in Fig. 1). The spatiotemporal data includes time and logical location of repositories for indirect access things' data through data repositories. It may also include physical location and logical location of things for finding the physical location and direct accessing things. There an access control mechanism is necessary to ensure the safety and privacy of the data in these steps. The read flow occurs when the users search the logical locations of desired repositories or things (Steps 3-1, 3-2, and 3-3 in Fig. 1). Similar with the write flow, before querying the main storage service, authority check is established. After the authority is verified, the users would receive a list of EPCIS logical addresses related to the query and the users could access each of the EPCIS repositories respectively to extract the information needed.

Based on the commonly used event-oriented EPC network structure, we address several possible problems as follows [2]:

1) EPCIS separately manages event data (i. e. , aggregation event, transaction event, etc.) and master data (i. e. , static information over the whole life of objects) so that the accessing application needs to combine them to obtain all the information on an object with additional cost.

2) The accessing application needs to search all the event types over again until there is no additional event found and extract target information from the reconstructed data since the accessing application may not know what event type is used for and what object is transformed from or transformed to the queried object in advance.

3) Under an event-oriented approach, each event can include a business context on one or more objects so that it may make EPCIS inefficient when an access control mechanism must be enforced on the selected objects. For example, the owner of a ranch may want to share business contexts on the cow only with the slaughterhouse owner. However, to enforce this kind of instance-level access control, a query interface of EPCIS becomes too complicated to filter them appropriately.

This paper proposes a Hardware-Based Information Service (HIS) device, which is mainly installed on some intelligent equipment or machines. The main idea of HIS is that it could centrally store the basic lifecycle information, which is used to be stored in the distributed EPCIS servers. Therefore, the cli-

ent only needs to simply search the HIS to obtain the complete traceability information of the item. There are two application scenarios of HIS. One is to interact with EPCIS and the other is to communicate with other HISs. Communicating with EPCIS is to fit to the existing EPC networks for centrally storing the distributed data in EPCIS servers. Exchanging information among HISes is to record the events that occur between EPC objects. Thus, the detector in the HIS will identify the devices in the scene firstly in order to determine the mode of data interaction. Next, the event processor will process the data received from HIS or EPCIS and store it in the memory. Finally, users can access the data in HIS in a flexible way.

Although HIS can only store the basic information about EPC items, users can directly obtain the complete lifecycle data, so that they can make further targeted query according to the information provided by the HIS, instead of iteratively querying for the information utilizing discovery service. Meanwhile, with the use of HIS, the number of query to the EPC system could be reduced dramatically. Thus, the work load of the EPC network can be significantly alleviated.

It should be noticed that the implementation of HIS is based on the EPC network, which is no need to be modified to fit HIS. Although the HIS can gain the data of the item easily, the EPC network can still be used for further searching if the user is interested in the master data that is not stored in the HIS. It takes less time to access the master data because the user could use ONS to find the location of the related EPCIS without applying discovery service.

2 Related Work

For several years, many works for alleviating the problems mentioned above have been conducted. Semantic web technologies lead to the development of EPCIS variants. Linked EPCIS [3] – [5] presents an ontological model of EPCIS events to improve supply chain visibility. However, Linked EPCIS is not compatible with the standard capture interface and does not provide scalability for a large amount of event data. Unlike the event-oriented persistent approach of Linked EPCIS, EPC Graph is a graph-oriented persistent approach [1], [6]. EPC Graph establishes efficient and privacy-enhanced traceability by representing the EPCIS document as properties and relationships in/among objects and locations. However, this solution is not compatible with the EPCIS accessing application because it does not provide a standard query interface.

Some works have focused on how DS is efficient designed [7], [8]. Bridge DS, the most early presented architecture design, suggests eight different DS architectures. Among them, four efficient architectures are selected considering how fast the response latency is and easily the secured resource is protected. Some works focus on the performance issues to find one of distributed DSes. For this, most of them apply peer-to-peer (P2P) technology to DS, Especially Distributed Hash Table (DHT) [9] – [11]. DHT offers high robustness, single failure avoidance, and load distribution. However, the previous works do not seriously deal with the intra-DS aspect. Any deterioration in the intra-DS may cause great performance degradation of entire DS. Additionally, security issues are also important for protecting secured resources in DS.

3 Hardware Information Service Device

3.1 Architecture of HIS

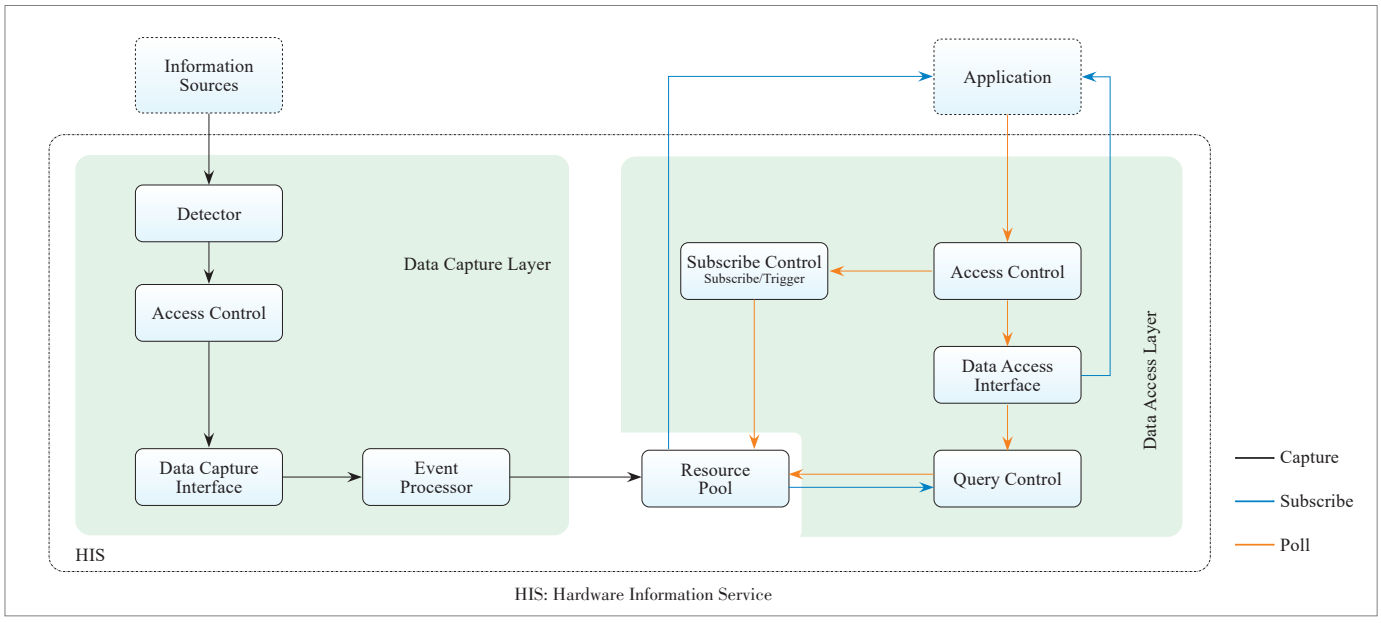
To improve the performance of the current EPC network system, we propose a HIS device, which is installed on the EPC-tagged item itself. The HIS of an item stores all the basic data (event data and master data) related to the EPC identifier and the device could be any small equipment like the Universal Serial Bus (USB) disk that we daily use.

Items installed with HIS need to meet certain conditions. HIS is mainly used in self-powered devices, which can search for their own energy supply; for example, the self-driving car that can intelligently find its own charging pile, or the robot that can generate electricity by utilizing other kinds of energy. Self-powered devices usually have mobility and intelligence. When self-powered equipment is running, people usually do not know its location or what happened to it. In this way, a certain device is needed to record their behavior. However, the things that are not self-powered such as foods and drugs do not need equipping with HIS because the limit amount of dynamic data generated by this kind of things could be processed by the existing EPC network system easily and the most queries related to them ask for the static data without distributed processing involved, which makes the response relatively faster.

As illustrated in **Fig. 2**, HIS could be separated into three parts according to their functions: the data capture layer, resource pool, and data access layer. The data capture layer is used to capture data (event and master data) and store it into the resource pool. The data access layer is implemented to publish and access data.

3.2 Procedure of Implementing HIS

Algorithm 1 shows the specific operation process of the data capture layer. The detector is used to detect the interactive device in the scene and broadcast permission and device type related information. The access control is implemented to get the device type and the state code of the device detected. The state code is introduced because of the safety and privacy concerns. The data capture interface is utilized to receive standardized both dynamic and static data from the device connected. After that, the event processor is needed to handle the data properly. Actions like data cleaning, sorting the events by the EventTime, and filtering unreasonable data should be taken in order to capture the valuable information and store it in the resource pool, which could be regarded as the memory of HIS.



▲**Figure 2. The structure of HIS.**

Algorithm 1. Data Capture Layer.

```
1: procedure CaptureData
2:     // Capture the data from EPCIS or HIS
3:     EPC: the identifier of the object
4:     L: the broadcast massage received
5:     U: the data stored in the HIS
6:     while ture do
7:         // broadcast the permission information and the de-
           vice type
8:         Broadcast;
9:         if device detected then // privacy protection
10:            state_code, type = permission_check(L);
11:            if state_code is 2 then
12:                connection established;
13:                send(U);
14:            else if state_code is 1 then
15:                if type is EPCIS: then
16:                    Interact_EPCIS(EPC);
17:                end if
18:                if type is HIS: then
19:                    Interact_HIS;
20:                end if
21:            else
22:                connection rejected;
23:            end if
24:        end if
25:    end while
26: end procedure
27: procedure Interact_EPCIS(EPC)
28:     R1: the date related to the EPC stored in the EPCIS
29:      connection established;
30:     R1 = query(EPC);
31:     U = store(R1);
32:     // data cleaning, sorting by the EvenTime, etc.
33:     process(U);
34: end procedure
35: procedure Interact_HIS
36:     R2: the data generated by the EPC object itself
37:     connection established;
38:     R2 = generater;
39:     U = store(R2);
40:     process (U);
41: end procedure
```

In the data access layer, there are many types of HIS requests, which could be similar with the requests of EPCIS [12]. Users can obtain the data from the repository immediately through the poll method. Meanwhile, event data can be delivered to a specific destination periodically (i. e. scheduled subscription) or if a specific condition meets at the time of capture (i. e. trigger subscription) via the subscribe method. The former subscription is useful for automating event delivers while the later one is suitable for developing real-time monitoring applications. Both of the subscription methods store their configurations in the resource pool. The access control is introduced to protect the privacy and enhance the safety of the system. Subscribe control and query control are required to manage subscribe and poll methods respectively.

3.3 Application Scenarios of HIS

There are two main application scenarios. One is between HIS and EPCIS and the other is between HISes.

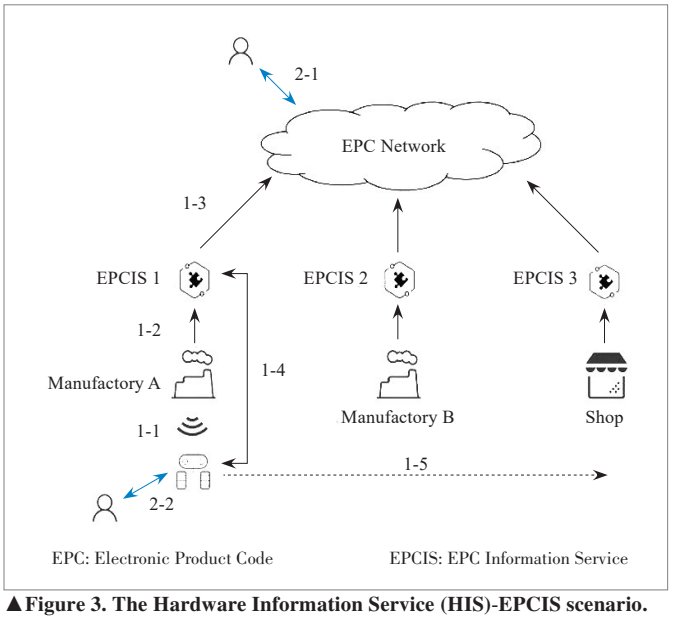
For the former scenario (**Fig. 3**), in the data capture phase, when a self-powered item enters the scene, the factory will generate corresponding data and send it to the EPCIS of the factory (Steps 1-1 and 1-2 in Fig. 3). The EPCIS of the factory is registered to the EPC network system in advance, so that the data of the manufactory could be found by the EPC network (Step 1-3 in Fig. 3). When EPCIS obtains data, it will synchronize it to the HIS (Step 1-4 in Fig. 3), so that the complete lifecycle could be maintained in HIS. The processes above would be repeated in the lifecycle of the item when entering the similar scenes (Step 1-5 in Fig. 3). In the data access phase, users can obtain data through the EPC network (Step 2-1 in Fig. 3) or access to HIS directly (Step 2-2 in Fig. 3).

For the later scenario (**Fig. 4**), self-powered devices generate the data themselves and interact with each other through HIS.

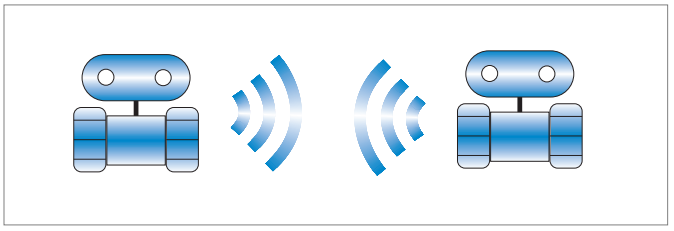
3.4 Evaluation of HIS

In order to compare the difference between the time required for the EPC network query method and the HIS query, we abstractly divided the time into t1 – t8. As shown in **Fig. 5**, the query method of the EPC network consists of all the time phases: t1 is the time phase of the discovery server receiving the request to retrieve the network address of the EPCIS servers related; t2 is the time period when the ONS searches the discovery service related to the EPC object or the network address of the manufacturer's EPCIS server; t3 and t4 are the time periods for the EPCIS server of the manufacturers and the participators to retrieve the relevant data respectively; t5 is the time period for transmitting the data retrieved to the discovery server; t6 is the time period for transmitting the data retrieved by the EPCIS of manufacturers to the user; t7 is the time period for transmitting the data aggregated in the discovery server to the user; t8 is the time period for the user to reconstruct the returned data and extract meaningful information. For HIS, since the basic information of the article is already stored, it only needs to query the master data of interest by utilizing ONS. **Table 1** shows the query time between the EPCIS and the HIS. It can be seen that the query efficiency of HIS will be relatively high.

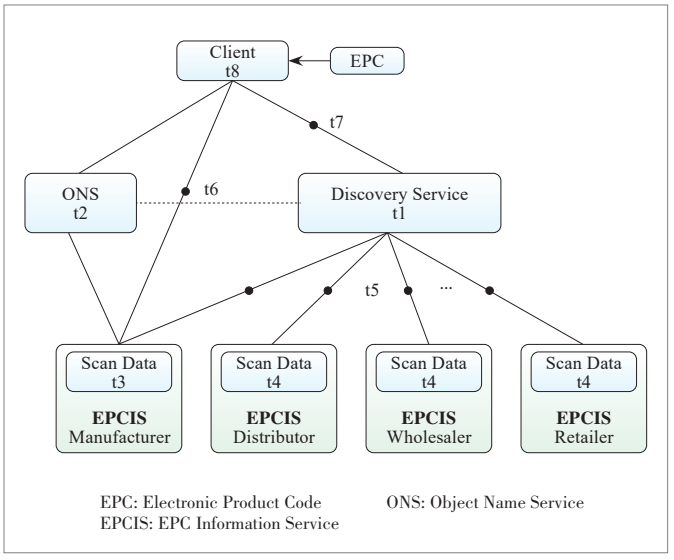
HIS have multiple advantages. Firstly, HIS stores all the basic data related to an item. In this way, people can gain the target information easier and faster than the tradition approach because no discovery service query is needed and the accessing application can easily indicate the relationship between the events. Secondly, because the client could access HIS directly, the load of the EPC network can be reduced significantly. Finally, HIS is designed for the future usage. The hardware can be installed on the robots, self-driving cars, drones and so on for monitoring, predicting and describing. In addition, users can access the information regardless of time, place and environment.



▲**Figure 3. The Hardware Information Service (HIS)-EPCIS scenario.**



▲**Figure 4. The Hardware Information Service (HIS)-HIS scenario.**



▲**Figure 5. The EPC network query process.**

▼**Table 1. The query time required for the EPC network and HIS**

Method	t1	t2	t3	t4	t5	t6	t7	t8
EPC network	●	●	●	●	●	●	●	●
HIS		●	●			●		

EPC: Electronic Product Code HIS: Hardware Information Service

4 Conclusions

In this paper, the potential issues of the currently widely used EPC network are evaluated. The issues include the inefficiency of the EPC network led by the distributed storage of the unrelated data and the access control mechanism of discovery service. Thus, the hardware information service is proposed to alleviate the challenges and improve the performance of the system. The basic idea of HIS is that it centrally stores the basic lifecycle information of the attached object and the user accesses it directly without involving discovery service, which may decrease the response time and alleviate the work load of EPC network. The device is specifically designed for the self-powered equipment. It has two different modes of data interaction: One is to exchange information with EPCISs in the existing network and the other is to communicate with other objects equipped with HIS. Both of the methods are used to capture the data from where it generated. Though HIS may improve the performance of system, the cost of implementing such mechanism is relatively high and the safety and robustness of EPC network still remain unsolved. For the further work, we will construct more realistic experiment environments by deploying IoT devices and getting real-data from them. Additionally, we will research on the searching performance improvement of the EPC network.

References

[1] KWON K, KIM D, KIM D. Oliot-Discovery Service: Dealing with Performance and Security Issues from Intra-DS Aspect for IoT [C]//IEEE Global Communications Conference (GLOBECOM), Washington DC, USA, 2016. DOI: 10.1109/glocom.2016.7842037
[2] BYUN J, KIM D. EPC Graph Information Service [M]//Lecture Notes in Computer Science. Cham, Switzerland: Springer International Publishing, 2015: 232 – 246.DOI: 10.1007/978-3-319-26190-4_16
[3] SOLANKI M, BREWSTER C. Representing Supply Chain Events on the Web of Data [C]//Detection, Representation, and Exploitation of Events in the Semantic Web, Workshop in Conjunction with the 12th International Semantic Web Conference. Sydney, Australia, 2013: 18 – 29
[4] SOLANKI M, BREWSTER C. EPCIS Event-Based Traceability in Pharmaceutical Supply Chains via Automated Generation of Linked Pedigrees [M]//The Semantic Web – ISWC 2014. Cham: Springer International Publishing, 2014: 82 – 97.DOI: 10.1007/978-3-319-11964-9_6
[5] SOLANKI M, BREWSTER C. Modelling and Linking Transformations in EPCIS Governing Supply Chain Business Processes [M]//Lecture Notes in Business Information Processing. Cham, Switzerland: Springer International Publishing, 2014: 46 – 57.DOI: 10.1007/978-3-319-10491-1_5
[6] BYUN J, WOO S, KIM D. Efficient and Privacy-Enhanced Object Traceability Based on Unified and Linked EPCIS Events [J]. Computers in Industry, 2017, 89: 35 – 49. DOI: 10.1016/j.compind.2017.04.001
[7] EVDOKIMOV S, FABIAN B, KUNZ S, et al. Comparison of Discovery Service Architectures for the Internet of Things [C]//IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. Newport Beach, USA, 2010. DOI: 10.1109/sutc.2010.22
[8] BRIDGE. High Level Design for Discovery Services [EB/OL]. (2007-08-31) [2019-11-15]. http://www.bridge-project.eu
[9] LORENZ M, MUELLER J, SCHAPRANOW M P, et al. A Distributed EPC Discovery Service Based on Peer-to-Peer Technology [C]//7th European Workshop on Smart Objects: Systems, Technologies and Applications; RFID SysTech 2011.Dresden, Germany, 2011: 1 – 7
[10] LIU P, KONG N, TIAN Y, et al. A Distributed EPC Discovery Service Based on Peer-to-Peer Technology [C]//IEEE International Conference on Internet of Things (iThings). Taipei, China, 2014
[11] MANZANARES-LOPEZ P, MUÑOZ-GEA J P, MALGOSA-SANAHUJA J, et al. An Efficient Distributed Discovery Service for EPCglobal Network in Nested Package Scenarios [J]. Journal of Network and Computer Applications, 2011, 34(3): 925 – 937. DOI: 10.1016/j.jnca.2010.04.018
[12] BYUN J, WOO S, TOLCHA Y, et al. Oliot EPCIS: Engineering a Web Information System Complying with EPC Information Services Standard towards the Internet of Things [J]. Computers in Industry, 2018, 94: 82 – 97. DOI: 10.1016/j.compind.2017.10.004

Biographies

HAN Tianyu received the B.E. degree in automation from Beijing Jiaotong University, China in 2016, and the M.S. degree from the School of Computer Science, University of New South Wales, Australia, in 2019. He works at the industrial Internet and Internet of Things Institute, the China Academy of Information and Communications Technology. His research interests include the areas of industrial Internet and Internet of Things, especially the data model and data sharing mechanism.

ZHU Siyu received her Ph.D. degree in signal and information processing from the Chinese Academy of Sciences, China. She now works at the industrial Internet and Internet of Things Institute, the China Academy of Information and Communications Technology. Research areas include industrial Internet Identifier Resolution, Blockchain and Internet of Things.

XIE Bin received the B.E. degree in automation from Beijing Forestry University, China in 2012, and M.S. degree in control theory and control engineering from Beihang University, China in 2019. She is currently a research engineer of the Institute of industrial Internet of Things, the China Academy of Information and Communications Technology. Her research interests include industrial Internet data models and data sharing mechanism for the industrial Internet of Things.

TIAN Juan (tianjuan@caict.ac.cn) received the B.E. degree in electronic information engineering from Chengdu University of Information Technology, China in 2005, and M.S. degree in signal and information processing from Chengdu University of Information Technology in 2008. She is currently a research director of technical research development of the Institute of industrial Internet of Things, the China Academy of Information and Communications Technology. Her research interest includes the area of the industrial Internet with focuses on data acquisition and automatic identification technology, and network communication technology.

Integrated Architecture for Networking and Industrial Internet Identity

LU Hua[1], LI Xiaolu[2,3], XIE Renchao[2,3], and FENG Wei[4]

(1. Guangdong Communications & Networks Institute, Guangzhou, Guangdong 510700, China;
2. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;
3. Purple Mountain Laboratories, Nanjing, Jiangsu 211111, China;
4. Department of Information and Software Services, Ministry of Industry and Information Technology of People's Republic of China, Beijing 100846, China)

Abstract: Several excellent works have been done on the industrial Internet; however, some problems are still ahead, such as reliable security, heterogeneous compatibility, and system efficiency. Information-Centric Networking (ICN), an emerging paradigm for the future Internet, is expected to address the challenges of the industrial Internet to some extent. An integrated architecture for industrial network and identity resolution in the industrial Internet is proposed in this paper. A framework is also designed for the ICN-based industrial Network And Named Data Networking (NDN) based factory extranet with Software-Defined Networking (SDN). Moreover, an identity resolution architecture in the industrial Internet is proposed based on ICN paradigms with separate resolution nodes or with merging resolution and routing.

Keywords: ICN; NDN; industrial network; industrial Internet identity

DOI: 10.12142/ZTECOM.202001005

http://kns.cnki.net/kcms/detail/34.1294.TN.20200317.1624.005.html, published online March 18, 2020

Manuscript received: 2019-12-08

Citation (IEEE Format): H. Lu, X. L. Li, R. C. Xie, et al., "Integrated architecture for networking and industrial internet identity," *ZTE Communications*, vol. 18, no. 1, pp. 24 – 35, Mar. 2020. doi: 10.12142/ZTECOM.202001005.

1 Introduction

Recent advances in the integration of the Internet and the industry have attracted great attention. The industrial Internet [1] is a new industrial economic system that incorporates industrial production, advanced production technologies, internet information technologies, and other new technologies. The industrial Internet supports ubiquitous connection, flexible supply, and efficient allocation of manufacturing resources to satisfy the demands of manufacturing industry, such as digitalization, networking, and intelligence. As a result, it reorganizes and optimizes the modes of industrial production, manufacturing, production organization, and service.

The industrial Internet includes industrial network, industrial platform, industrial security, and industrial internet identity. Although some excellent works have been done on these four aspects of the industrial Internet, a few major problems are still ahead, such as reliable security, heterogeneous compatibility, and system efficiency. In terms of security, network failures may have catastrophic consequences. Industrial networks communicate between sensors, actuators, and control centers, which needs ultra-high reliability. Encryption and other cryptographic techniques are often considered as a silver bullet to ensure security in the industrial Internet. A reliable data protection capability is essential for the industrial Internet; however, IP-based sender-driven end-to-end communi-

This work was supported in part by National Key Research & Development Project (Grant No. 2019YFB1804400) and the MIIT of China 2019 (Innovative Identification and Resolution System for Industrial Internet of Things).
LU Hua and LI Xiaolu contributed equally to this work and are co-first authors of the article.

cations have fundamental security defects, introducing host-centric security mechanisms. In terms of heterogeneous compatibility, due to the lack of unified standards in industrial internet identity, manifold identity systems constitute the present situation of multi-system heterogeneity. Heterogeneous compatibility has become one of the main challenges to be addressed in the industrial Internet. In terms of system efficiency, the current industrial Internet system separates networking and identity resolution. The multi-layer architecture is not conducive to efficient information interaction and represents a large portion of infrastructure costs. A more flatting industrial Internet architecture is necessary to reduce the information loss in different system levels.

Information-Centric Networking (ICN) [2], an emerging paradigm for the future Internet, is expected to address the challenges of the industrial Internet to some extent. The key idea of the ICN is to replace the traditional host-based networking primitives with novel name-based ones. In the ICN, a content requester does not need to maintain the knowledge of specific hosts (that act as a content provider), and all networking operations are driven by content names without any references to host locators. ICN strictly names data packets according to its contents instead of its locations, which natively promotes content-based security mechanisms. Content naming also introduces name-based routing protocols, which can route paths according to content names directly. ICN provides an opportunity to integrate networking and identity resolution for the industrial Internet.

In this paper, we first propose an integrated architecture for industrial network and identity resolution in the industrial Internet. We present the framework designs of ICN-based industrial network architecture and Named Data Networking (NDN)-based factory extranet with Software-Defined Networking (SDN). We also address an identity resolution architecture in the industrial Internet based on ICN paradigms with separate resolution nodes or with merging resolution and routing.

The remainder of this paper is organized as follows. In Section 2, we comprehensively review the industrial Internet and ICN. In Section 3, we present an integrated architecture for industrial network and industrial internet identity. We conclude this paper in Section 4.

2 Overview of Industrial Internet and Information-Centric Networking

2.1 Industrial Internet

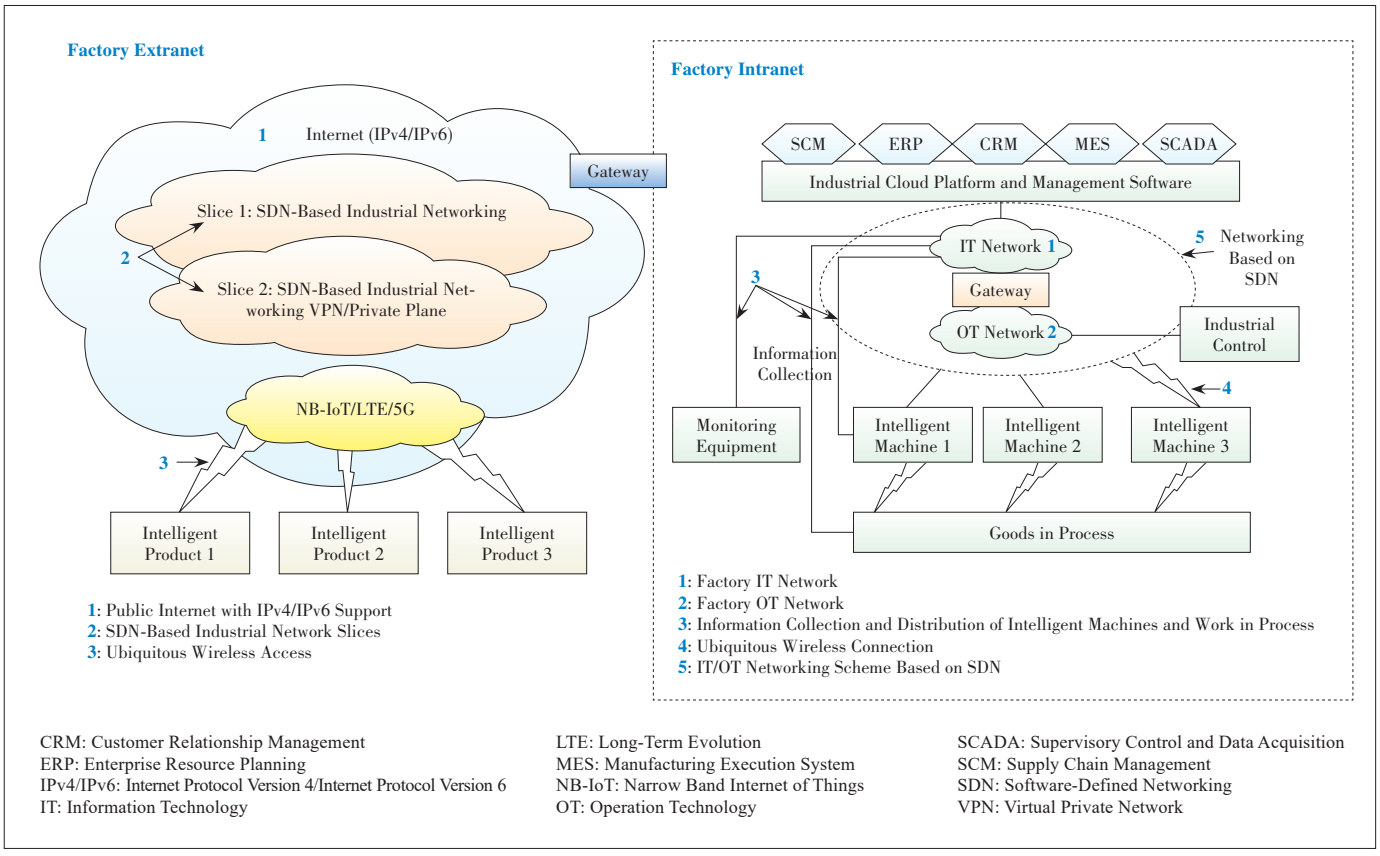
The industrial Internet is a service system based on mass data collection, convergence, and analysis for the demand of manufacturing industry, such as digitalization, networking, and intelligence. It is an industrial cloud network that supports ubiquitous connection, flexible supply, and efficient allocation of manufacturing resources. The ultimate goal of the industrial Internet is to realize enterprise intelligence, so as to build the powers of manufacturing and network. industrial Internet architecture consists of four main aspects: industrial network, industrial platform, industrial security, and industrial internet identity. Among them, we will introduce the industrial network and the industrial internet identity in detail.

2.1.1 Industrial Network

The industrial network is an important foundation to realize the layout of the industrial Internet. It integrates the industrial production processes, the information communication technologies, and the basic elements of intelligent manufacturing systems. The industrial network interconnects people, machines, control systems, and information systems together. Its core is to connect the entire industrial system, break information isolation, and ensure the barrier-free data transmission between different devices and systems, thus forming an intelligent system. **Fig. 1** shows the overall architecture of the industrial network. We can divide the industrial network into a factory intranet and a factory extranet according to the deployment position. The factory intranet is deployed in factories and connects people, products, intelligent machines, industrial control and information systems. The factory extranet connects the enterprise, intelligent products, users, and service platforms, aiming at supporting various activities in a product lifecycle.

The factory intranet, according to the carried data, can be divided into Information Technology (IT) network and Operation Technology (OT) network. The IT network connects the information systems in enterprises, interconnecting with the control systems. The OT network interconnects the production control systems (including Distributed Control System (DCS), Fieldbus Control System (FCS), and Programmable Logic Controller (PLC)) and the machines (mainly servers on the device and sensors). The current factory intranet faces several obstacles, including the coexistence of multiple protocols and multiple transmission modes, the existing 5G technology unable to meet the requirements of wireless communication in the factory, the heterogeneous hierarchical access to enterprise data, the ossified network architecture, and the lack of customized services. In order to cope with the above issues, manifold solutions have been researched among the industry, academic, and standardization organizations.

In industry, China Academy of Information and Communications Technology (CAICT) and Huawei have jointly proposed MulteFire, 5G, and SDN/NFV solutions to transforming and constructing the factory intranet. China United Network Communications Co. , Ltd. has applied industrial Passive Optical Network (PON) technology at the perception layer to provide wired network coverage for production line equipment and achieved wired and wireless integrated network coverage in the workshop through the wireless network bearer. ADLINK Technology has explored a future wireless factory



▲**Figure 1. The overall architecture of the industrial network.**

model by using agile 5G industrial wireless technology.

In academia, GOGOLEV et al. [3] studied the integration scheme of industrial field equipment and embedded object linking and embedding OLE for Process Controls (OPC) Unified Architecture (UA) on Time Sensitive Networking (TSN). MANNWEILER et al. [4] outlined the favorable deployment scenario of 5G/TSN systems integrated under the industry 4. 0 environment. NSAIBI et al. [5] proposed a solution to integrating TSN into the automation network and demonstrated its improvement and enhancement of delay performance in industrial Ethernet.

In standardization organizations, the Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), and other standardization organizations are committed to the transformation of the factory intranet. In order to solve the problem of hierarchical and heterogeneous access to industrial data, the OPC Foundation proposed a unified OPC architecture in 2008 to solve the problem of heterogeneous data connection. In order to meet the deterministic delay, the IEEE 802. 1 working group has formulated and developed TSN-related standards, aiming to establish a "universal" time-sensitive mechanism for the Ethernet protocols [6], [7]. The IETF has developed the related standards for Deterministic Networking (DetNet) [8], which provides reliable network-layer transmissions by providing data transmission with a certain range of delay, packet loss, and delay jitter.

The factory extranet connects users, data centers, factories, and upstream/downstream enterprises to facilitate enterprise cooperation, operation decision-making, and rapid deployment. The current factory extranet faces with such problems as the large granularity of network services and stiff adjustment, the inability of enterprises to provide edge computing power, and network security. In order to cope with these problems, many solutions have been researched among the industry, academic, and standardization organizations.

In industry, China Mobile and Huawei have introduced Software-Defined Wide Area Network (SD-WAN) controller into the factory extranet to separate the control and forwarding functions of network equipment, so as to build a Wide Area Network (WAN) with open business, flexible programming, and easy operation and maintenance for enterprise users. By building SD-WAN, Huawei could quickly distribute connection services and provide management in the cloud, making it more convenient for enterprise users to define new services and conduct network management. China United Network Communications Co. , Ltd. has proposed an integrated application project of 5G industrial Internet automotive extranet transformation.

In academia, CHAUDHARY et al. [9] designed a multi-attribute secure communication model for the industrial Internet with SDN. LI et al. [10] proposed an adaptive transmission architecture for the industrial Internet based on SDN and edge computing and provided a coarse-grained transmission algorithm. To meet the processing requirements of enterprises for big data, the edge computing technology was used to provide enterprises with edge computing capacity and edge caching capacity in [11] and [12], so as to support industrial Internet applications and realize production monitoring, data processing, automatic decision-making, and automatic and rapid response to user demands.

In standardization organizations, the industrial Internet has become the focus of 3GPP R16. 5G network slices are constructed to meet different business operations. 5G edge computing accelerates the integration of industrial IT and OT networks, improves the performance of the industrial Internet such as high reliability and low delay, provides better security and user privacy, and optimizes resource sharing and user experience. The current standardization of 3GPP industrial Internet architecture mainly includes three aspects: new network architecture, enhanced network functions, and new networking mode [13] – [15].

2.1.2 Industrial Internet Identity

Identity resolution is a key hub to connect industrial elements and realize industrial data interchange, which is responsible for providing identification registration, management, analysis, and other services. The identity resolution system includes two parts: identity coding and identity resolution. The identity code is used as the "ID card" to identify the unique device; the identity resolution utilizes identification to uniquely locate and address the device. Currently, there are many identity resolution systems, such as Electronic Product Code (EPC) global [16], Object Identifiers (OID) [17], Handle [18], and UID [19].

We can divide the existing identity resolution systems into two categories, namely, the evolution schemes and the clean-slate schemes. The evolution schemes are still based on the Domain Name System (DNS) system, which overlay a set of identity services on top of the DNS technology and store the identity ID and the mapping associated with it. At present, OID, Ecode, and Global Standards One (GS1) belong to the evolution schemes. These schemes are conducive to deployment, but at the same time, they are secondary platforms grafted on DNS. All lookups need to go through DNS, which resulting in low resolution efficiency and heavy reliance on the operation of DNS system. In addition, some researchers believe that the expansion of DNS system should be more cautious due to the importance of DNS system.

The clean-slate schemes, such as Handle and UID, utilize fresh identity resolution technologies which are different from DNS. Specifically, Handle system is a popular identity resolution solution, which has gradually become the essential infrastructure promoting the fusion of the Internet, data, and artificial intelligence. Handle system has broad prospect and is able to effectively integrate information islands and implement cross-border information sharing, which is an indispensable technology to the future development. These identity resolution technologies are independent of the DNS system and are more suitable for industrial internet scenarios, but at the same time, the clean-slate identity resolution infrastructures need to be deployed, which are expensive and take a long time.

Identity resolution in the industrial Internet faces severe challenges in efficiency, heterogeneous compatibility, and security. The identity resolution system obtains the information addresses of objects (such as IP addresses) based on identification, and then the network routes information requests to the devices storing the information. The whole process of obtaining data needs to be completed by the cooperation with identity resolution system and the network routing system, which is complex and redundant to some extent, resulting in low efficiency of content retrieval. In addition, the data security needs to be considered in both systems, resulting in the difficulty of ensuring the whole system security. There are many heterogeneous identity resolution systems, causing conflicts between them. Without the compatibility of heterogeneous identities, it will be difficult to realize the interconnection between industrial Internet applications.

2.2 Information-Centric Networking

The ICN replaces the traditional address-centered network communication model with information naming centric ones to realize efficient information retrieval. The idea of ICN was first proposed by NELSON in 1979. Several countries around the world have started a series of ICN-related projects. We review the ICN from the following perspectives, including typical projects, naming mechanisms, and important features.

2.2.1 Typical Projects

The American academic community takes the lead in launching research projects on content-oriented network architectures, including Content-Centric Networking (CCN), NDN [20], Data-Oriented Network Architecture (DONA) [21], etc. The European Union has launched research projects on Network of Information NetInf, Publish-Subscribe Internet Technologies (PURSUIT)/Publish-Subscribe Internet Routing Paradigm (PSIRP), Point, etc. We will introduce DONA and NDN.

1) DONA.

DONA, launched in 2006 and lasting for two years, is a data-oriented network architecture proposed by the Radiation (RAD) Laboratory at the University of California, Berkeley. The project comes up with a self-validating name and adds the capability of advanced caching. The architecture design also takes naming, name resolution, security, and routing into consideration. It expounds the basic functions, such as server se-

lection, mobility, multihoming, multicast, and session initialization. In the extended applications, DONA realizes content distribution, delay tolerant networks, access rules, and middleware. The name resolution mechanism of DONA is similar to DNS but not exactly the same. DONA designs a flat naming mechanism based on URL construction, which realizes the registration, publication, and acquisition of content. Furthermore, naming is used to solve the problems of persistence and reliability. The new self-verification approach simplifies the security model; and the name resolution method finding the path by name solves the validity problem. At present, the project has been completed, but its research results have laid the foundation for the subsequent designs of various ICN architectures.

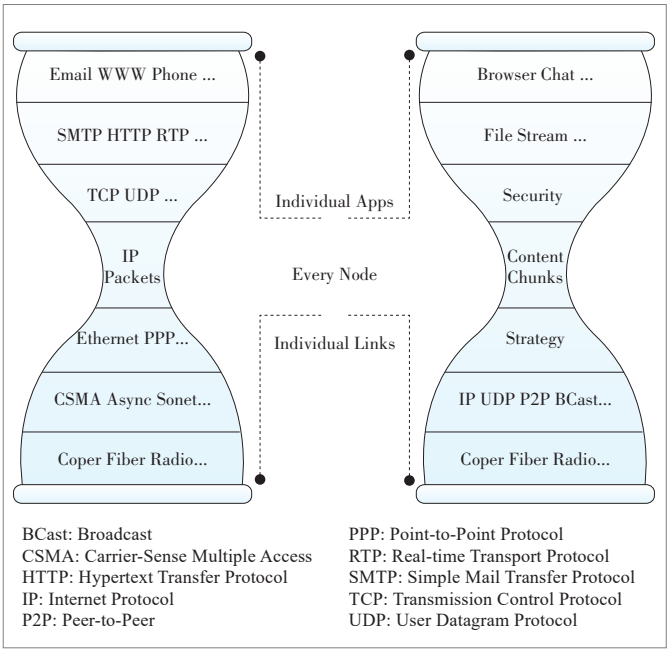
2) NDN.

In 2009, JACOBSON of the PARC Research Center proposed CCN and launched the CCNx project. The NDN is an engineering project based on the idea of CCN. It was one of the research projects on the future Internet architecture announced by the Natural Science Foundation of the United States in August 2010. NDN tries to change the current host-based point-to-point communication architecture and realize the transformation to a new network architecture centered on named data. NDN shifts its focus from "the where" to "the what", which focuses on the content that users and applications are interested on. NDN decouples the content from the protected hosts and directly protects the content, so as to expand the communication mechanisms fundamentally. With the name-based routing, NDN references the hourglass model of current IP network. As shown in **Fig. 2**, it places the content block instead of IP in the waist part and constructs the basic safety module by signature for all named data.

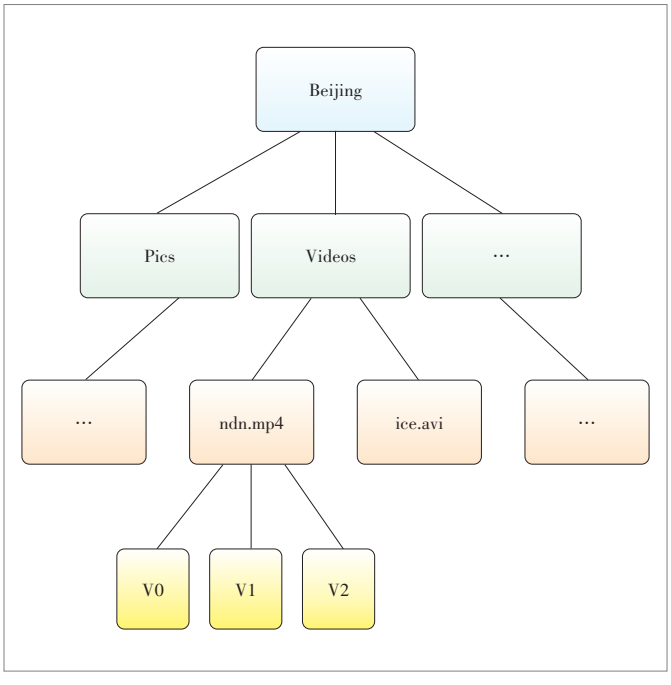
2.2.2 Naming Mechanisms

The naming mechanisms of ICN fall into two categories: hierarchical naming and flat naming. The typical representative of hierarchical naming is NDN, which is similar to URL with "/" as the separator. With hierarchical naming, network nodes can receive, recognize, and forward the received content based on longest prefix matching. At the same time, hierarchical naming is adopted to facilitate clustering of network nodes, which can merge similar items and facilitate search. For example, as shown in **Fig. 3**, to find /Beijing/videos/ndn.mp4/v1, NDN will first lookup /Beijing, since the data naming with the /Beijing prefix has been gathered together. The aggregation ability enables NDN to process massive data. It solves a part of the burden caused by naming, that is, the amount of content in the whole network is much larger than that of hosts, which makes the scale of content-oriented addressing larger than that of host-oriented ones. Nevertheless, hierarchical naming is generally less secure.

The typical representative of flat naming is DONA, which has the form of a *P*:*L*. *P* is the hash value of public key of the content provider; *L* is name tag, describing the content details, and the granularity of *L* can be control by the user. In addition, DONA supports naming formats of *P*: *, which can be used to verify that the prefix is used, and of *:*L*, which can be used to describe *L* contents or services provided by any content service provider. The naming of hash strings without semantics guarantees good stability and uniqueness, but at the



▲**Figure 2. Named data networking hourglass architecture with content chunks.**



▲**Figure 3. Named data networking hierarchical naming example.**

same time brings inconvenience in understanding and memory, and the name will change after the encryption algorithm is upgraded.

2.2.3 Important Features

ICN separates content from its location by virtue of its name-based routing, which greatly facilitates the transmission and forwarding of information. Therefore, ICN provides an efficient platform for content distribution. Compared with the traditional IP networks, its core features and advantages are as follows:

1) Content naming.

NDN directly names the content, decouples the content and location information, and realizes name-based routing. On the other hand, since the address space of content naming is infinite, it can effectively solve the problem of IP address exhaustion in terms of a large number of terminals in the IoT environment.

2) In-network caching.

Due to the decoupling of content from specific geographical locations brought by content naming, it is feasible to cache content copies in the network. The spatial resources of in-network caching can be used to exchange time benefits, reducing content response time and saving bandwidth.

3) Mobility support.

ICN is a content-enabled request/response model, which eliminates the need to establish and maintain connections. Therefore, ICN is more suitable for mobility scenarios. When the request packet passes through the ICN router, the router will automatically record the track of the demand packet and return the data packet to the user according to the track. When the user moves, a new trajectory will be generated again, so there is no need to maintain the location information of the user in the network. Supporting the mobility of hosts solves the problem of efficiently transmitting mass information. Compared with end-to-end IP communications, ICN's connectionless communication provides a better foundation for seamless switching of mobility, and at the same time, in-network caching benefits for reducing content response latency.

4) Network layer security.

ICN has taken security into consideration during its design. By directly protecting the content itself, the security mechanism of ICN is more robust than that of IP. In traditional IP networks, security depends on whether the host is trusted. If the host is not trusted, the information stored on the host is considered untrusted. However, the security of information is not necessarily related to the host where the information is stored. ICN directly implements security measures on information, so that the granularity of security policy can be coarse or fine.

As a result, ICN adopts information naming instead of the traditional address-centered network communication model, so as to solve some inherent problems in IP networks and meet users' demand for massive information access. Introducing ICN to the Industry Internet can solve the problem of separating industrial network and industrial identity resolution. We design an integrated architecture for industrial network and identity resolution in the industrial Internet, to flat the overall industrial internet architecture, improve information retrieval efficiency, increase network scalability, and improve data security in the industrial Internet.

3 An Integrated Architecture for Industrial Network and Industrial Internet Identity

In this section, we describe the proposed integrated architecture for industrial network and industrial internet identity. The details of this architecture are described as follows.

3.1 ICN-Based Industrial Network Design

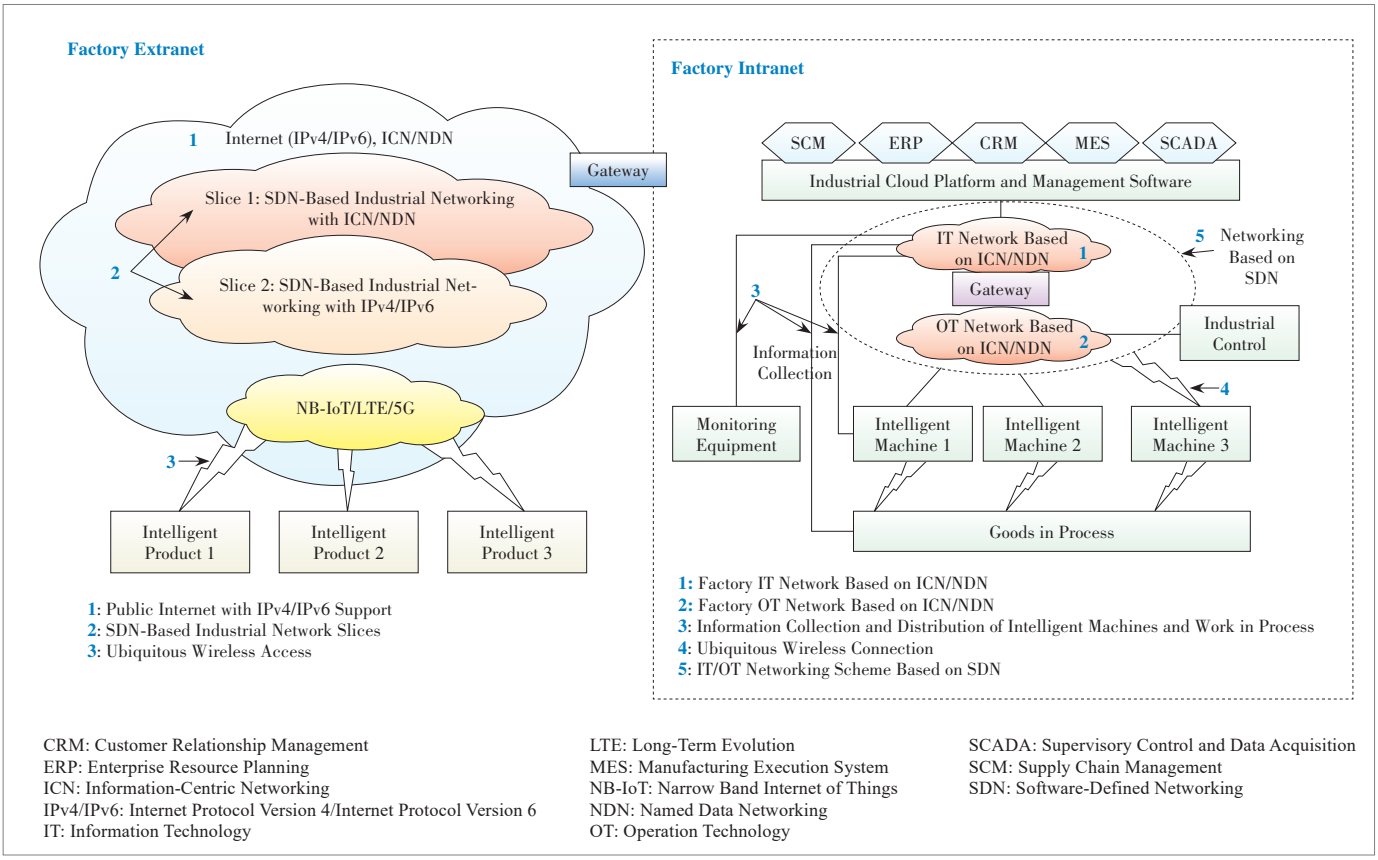
In order to meet the development of industrial network services, the networks need to guarantee efficient data transmission, flexible mobile access, convenient and differentiated demand, and industrial data security. It is urgent to introduce new network technologies to solve the problems including low utilization of network resources, redundancy and complexity of protocol, patchy security mechanism, and inflexible mobile access.

The data-centered ICN provides a solution to solve the above problems to some extent. ICN provides efficient content distribution, mobility support, and security support, bringing new opportunities for the development of industrial networks. In order to realize the deployment of ICN/NDN technology in the industrial network, we propose an overall framework design and a specific NDN-based factory extranet design with SDN.

3.1.1 Framework Design

The overall framework design of ICN-based industrial network is shown in **Fig. 4**. Both factory intranet and factory extranet are ICN enabled. Moreover, we utilize SDN to manage and orchestrate both factory extranet and factory intranet, which resides in the threefold aspects. Fist, SDN can manage and orchestrate the high-dimensional and high-volume resources, especially the caching/computing/networking resources in ICN and large amounts of machines and equipment in the industrial Internet. Second, SDN can separate the control plane (routing protocol) from the forwarding devices to release more resources for processing and forwarding, so as to improve the network performance. Finally, SDN can provide network programmability to implement fresh information-centric schemes conveniently. As a result, it is convincing to implement the ICN-based industrial Internet in a software-defined architecture.

We take the factory extranet as an example. The factory ex-

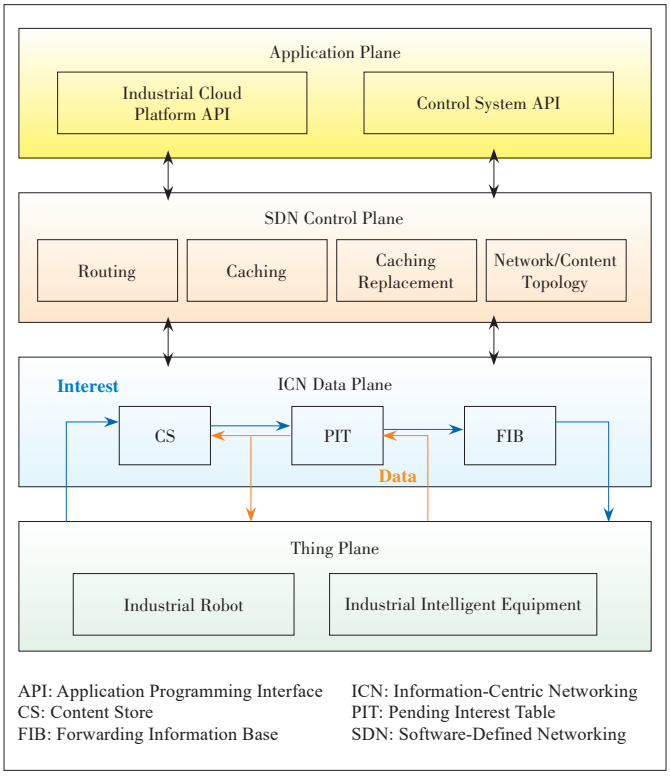


▲**Figure 4. A framework design of ICN-based industrial network.**

tranet includes three main components. First, the public Internet supports the coexistence of IPv4/IPv6 and ICN/NDN. Due to the explosive growth of the number of industrial Internet terminals, the network based on IP addresses is unable to meet the needs of the industrial Internet. Therefore, ICN/NDN network mechanism is introduced to directly name the network content itself to solve problems such as insufficient IP addresses and difficult mobility support. Second, the network slices based on 5G or other network technologies are supported. Industrial networks can include multi-slice implementation of multi-protocol network configuration, such as SDN based IPv4/IPv6 industrial Internet slices and SDN based ICN/NDN industrial Internet slices. Third, ubiquitous wireless access is introduced. NB-IoT, LTE enhancement, 5G and other technologies are utilized to realize wireless access to various smart products.

3.1.2 NDN-Based Factory Extranet with SDN

Taking the representative NDN as an example, the specific deployment design of NDN-based factory extranet with SDN is shown in **Fig. 5**. Based on the characteristics of separating control and forwarding in SDN, we divide the NDN-based factory extranet architecture with SDN into four layers: the application plane, SDN control plane, ICN data plane, and thing



▲**Figure 5. The NDN-based factory extranet design with SDN.**

plane.

1) Application plane.

The application plane is responsible for interacting with the industrial internet cloud platform and control system and formulating network strategies which are implemented by the control plane. The application plane provides API interfaces to interact with the external environment and implements specific network functions by formulating network policies (such as load balancing, traffic scheduling, and resource allocation) to meet network performance requirements in different scenarios.

2) SDN control plane.

The SDN control plane is responsible for the centralized control of the data plane devices. The SDN control plane holds the global topology of network nodes and contents within the network, uses the routing strategy to calculate the path, and installs the FIB table to the data plane devices. At the same time, the control plane grasps the caching strategies and caching replacement strategies, so as to carry out content caching under different requirements. The SDN control plane interacts with the application plane, providing the application plane with the underlying network information (e. g. , network traffic) and implementing the upper application's control instructions on the data plane devices.

3) ICN data plane.

The ICN data plane, under the centralized control of the control plane, is responsible for packet forwarding and caching to quickly respond to content requests from the thing plane. Taking the NDN paradigm as an example, the content requests can be cached locally or routed through Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB) tables in the form of Interest packets. The Data packages directly use the PIT table to return the content request nodes along the reverse paths of Interest packets, and at the same time, the local cache strategies are utilized to cache the content into CS. This process completes the content request and response.

4) Thing plane.

The thing plane implements all devices accessing to the industrial Internet, such as industrial robots, industrial intelligent devices, and sensors. These devices act as network terminals, playing the role of content sources (collecting content) and/or content requesters for efficient content distribution and acquisition through the ICN data plane.

3.2 ICN-Based Identity Resolution in The Industrial Internet

Identity resolution in the industrial Internet needs to query the server addresses, which store product information using product identity, or directly query product information and related services. ICN/NDN is applied to the industrial Internet for identity resolution. We use content naming as the identification of products, components, and equipment. The name resolution mechanism in ICN is used as the identity resolution scheme in the industrial Internet. ICN paradigms include the ICN architectures that implement name resolution and routing as independent functions (such as DONA, PURSUIT, SAIL, COMET, and MobilityFirst) and the ICN architectures that merge name resolution and routing functions (such as CCN and NDN) [22].

For the former paradigm, name resolution servers (called by different names) are organized hierarchically, and consumers and producers contact such servers to publish and subscribe to content in various ways. Consumers obtain the locations of publishers from name resolution servers and send their content requests to those locations to get the required content or services. Enabling the updates of name-to-address mapping is a non-trivial problem using hierarchical structures, spanning trees, or DHT-based organizations of servers.

For the later paradigm, NDN and CCNx merge name resolution and routing functions; in this way, routers are the facto name resolvers by establishing routes to name prefixes on a hop-by-hop basis. A major advantage of doing this is that it eliminates the complexity of designing and maintaining a network of name-resolution servers that replace the DNS. This merging of functionalities is supported by: 1) a name-based routing protocol operating in the control plane, which updates the entries in FIBs listing the next hops to known name prefixes, and 2) forwarding interests based on the Longest Prefix Match (LPM) between the Content Object (CO) name in the interest and a name prefix listed in the FIBs.

We design from these two types as follows.

3.2.1 Identity Resolution Based on ICN with Separate Resolution Nodes

Name resolution in DONA is provided by specialized servers called Resolution Handlers (RHs).

There is at least one logical RH at each Autonomous Systems (AS). The multi-level identity resolution system in the industrial Internet can adopt DONA's multi-level RH architecture, including four levels: root node, national top-level node, secondary identity resolution node, and enterprise identity resolution node. When the identity resolution system in the industrial Internet is deployed by ICN with separate resolution nodes, the current network technology can still be used at the network layer and below, or ICN can be directly deployed at the network layer. When ICN is directly deployed in the industrial network layer, it can be used as both routing and identity resolution system, so as to realize the integrated design of identity resolution and routing.

As shown in **Fig. 6** the content provider needs to send the registration information to the identity resolution system to complete the registration (Fig. 6, step 1). The user queries the identity resolution system for the content provider that can provide the required content object. The identity resolution system finds the most appropriate content provider based on

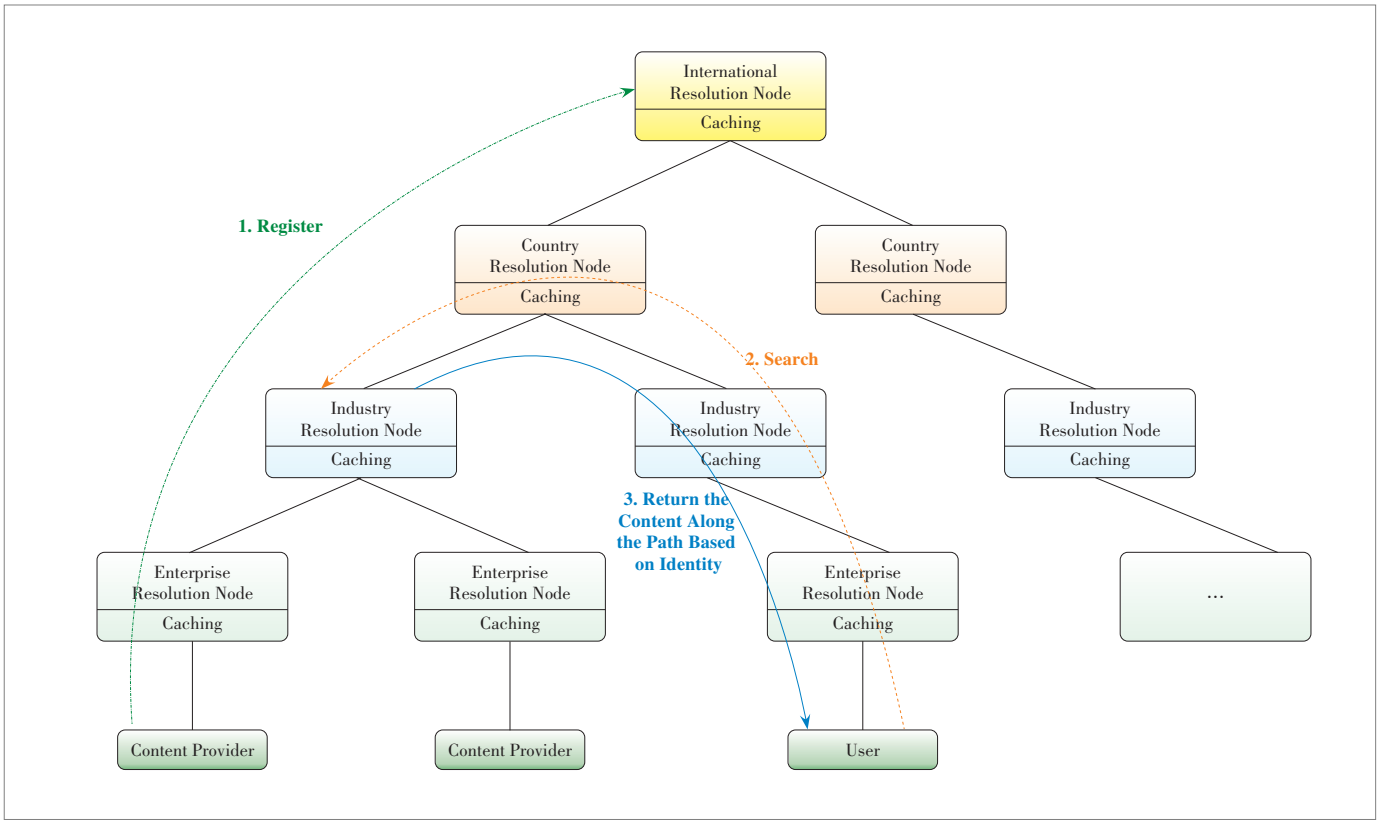
the content identity name, which may be the registered content provider or the cache on the resolution node (Fig. 6, step 2). The content object is returned directly to the user along the reverse path (Fig. 6, step 3).

3.2.2 Identity Resolution Based on ICN with Merging Resolution and Routing

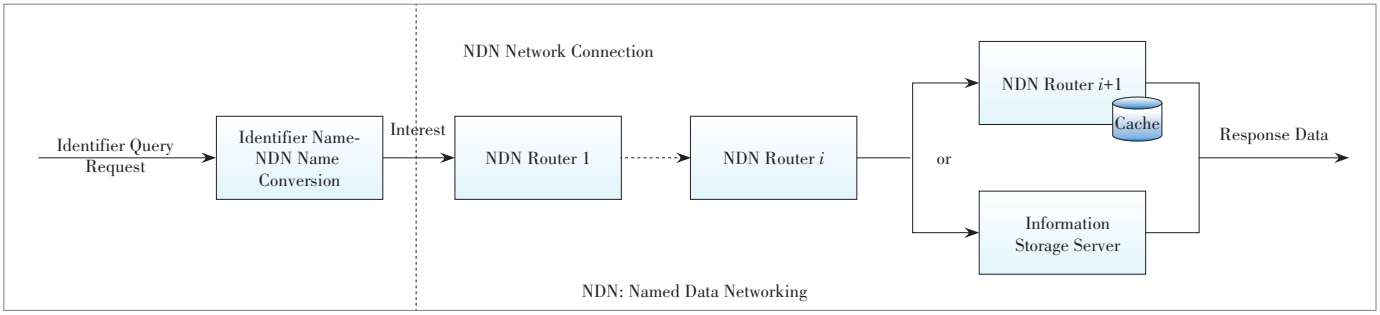
The NDN paradigm can directly merge the name resolution and routing. Specifically, NDN implements content name-based routing and forwarding based on name-based routing protocols without the need for a DNS server to query the server location. This characteristic of the NDN network provides an effective solution to integrate network routing and identity resolution. The merging architecture is shown in **Fig. 7**.

As shown in Fig. 7, the identifier name-NDN name conversion module is responsible for converting the queried identifier name into the naming format of NDN, that is, to obtain the NDN identifier name, so that the identifier query request can be forwarded in NDN. The NDN router is responsible for forwarding the interest packets and data packets, and stores the passing data packets into the local cache. The information storage server stores the identifier name, corresponding NDN identifier name, and its information.

The identifier query request first needs to be constructed as an interest packet conforming to the NDN naming format before accessing the NDN network, so that the interest packet



▲**Figure 6. Identity resolution and routing architecture based on data-oriented network architecture.**



▲**Figure 7. Architecture of merging identity resolution and routing based on NDN.**

can be forwarded in NDN. Until the NDN identifier name is found in the NDN router cache or the information storage server, the corresponding information data packet is returned to the identification query request node along the reverse path of the interest packet to complete the information query response.

The designs of the identifier name-NDN name conversion module and information storage server are as follows.

1) The identifier name-NDN name conversion module.

In order to integrate identity resolution and NDN networks, it is imperative to unify NDN naming and identifier names. Since NDN naming is hierarchical, and the existing identifier names include different parts; besides, both NDN naming and identifier names are variable-length naming, so NDN naming is very suitable for compatibility with a variety of identifier names.

Specifically, since each part of the NDN hierarchical naming is separated by "/", while the delimiters of different identifier names are different, the identifier name-NDN name conversion module is responsible for unifying the various delimiters of identifier names as "/". Besides, the NDN identifier name also uses the identification mechanism as the prefix to avoid conflicts between different identification systems. At the same time, it enhances the aggregation of the NDN identifier name and improves query efficiency. We have to note that the identifier name-NDN name conversion module is executed before the request packet accesses the NDN network, such as end devices.

We use OID as an example to describe the conversion process. The OID mechanism has OID numeric value, OID alphanumeric value, and OID Internationalized Resource Identifier (OID-IRI). For numeric values, different levels are separated by ". ", such as {2. 17. 2. 3} which is converted to NDN identifier name as /OID/2/17/2/3. For alphanumeric values, it is exemplified by {joint-iso-itu-t (2) registration-procedures (17) document-types (2) binary (3)}, which is converted to NDN identifier name as /OID/joint-iso-itu-t (2)/registration-procedures (17)/document-types (2)/binary (3). For OID-IRI, the example is /Joint-ISO-ITU-T/Registration-Procedures/Document Types/Binary, which is converted to NDN identifier name as /OID/Joint-ISO-ITU-T/Registration-Procedures/Document Types/Binary.

2) The information storage server.

Since the identifier name is uniformly converted by the identifier name-NDN name conversion module before accessing the NDN network, the registration of the identifier name in the information storage server should also include the converted NDN identifier name. Each record in the information storage server contains the identifier name, NDN identifier name, and information content.

Fig. 8 shows the following workflow of the process of registration as well as the identifier query request and response in the proposed merging architecture.

1) Register and publish in the information storage server.

a) Register: When a new identifier name and its corresponding information content are to be registered and stored in the information storage server, the identifier names of all entries in the information storage server are searched for the identifier name to be registered. If it exists, it means that the identifier name already exists in the information storage server, thus updating the information content. If it does not exist, a new entry is added to the information storage server to record this identifier name and its information content. The NDN identifier name is also recorded, which is obtained according to the conversion rule in the identifier name-NDN name conversion module. Due to applying the same conversion rules, the NDN identifier name stored in the server is consistent with the NDN identifier name converted when the identifier query request is made. The registration entry of product 1 is shown in Fig. 8.

b) Publish: The information storage server publishes the locally stored NDN identifier name, so that the NDN network can perform routing and forwarding according to the NDN identifier name.

2) End device 1 requests an identifier query.

a) End device 1 gets the identifier name {2. 17. 2. 3} of product 1 and converts it to the NDN identifier name /OID/2/17/2 by local identifier name-NDN name conversion model. And then, it constructs an interest packet sending to the NDN network.

b) When the NDN router receives this interest, it processes and forwards the interest according to the standard NDN node processing model [20]. That is, it looks up in the local cache. If the corresponding data exists, it will return the data packet immediately; otherwise, it forwards this interest based on PIT and FIB.

c) The interest packet reaches the information storage server through R1 and R2. The information storage server searches the NDN identifier name. If it exists, the information storage server returns the data packet (/OID/2/17/2/3); otherwise, it discards the interest.

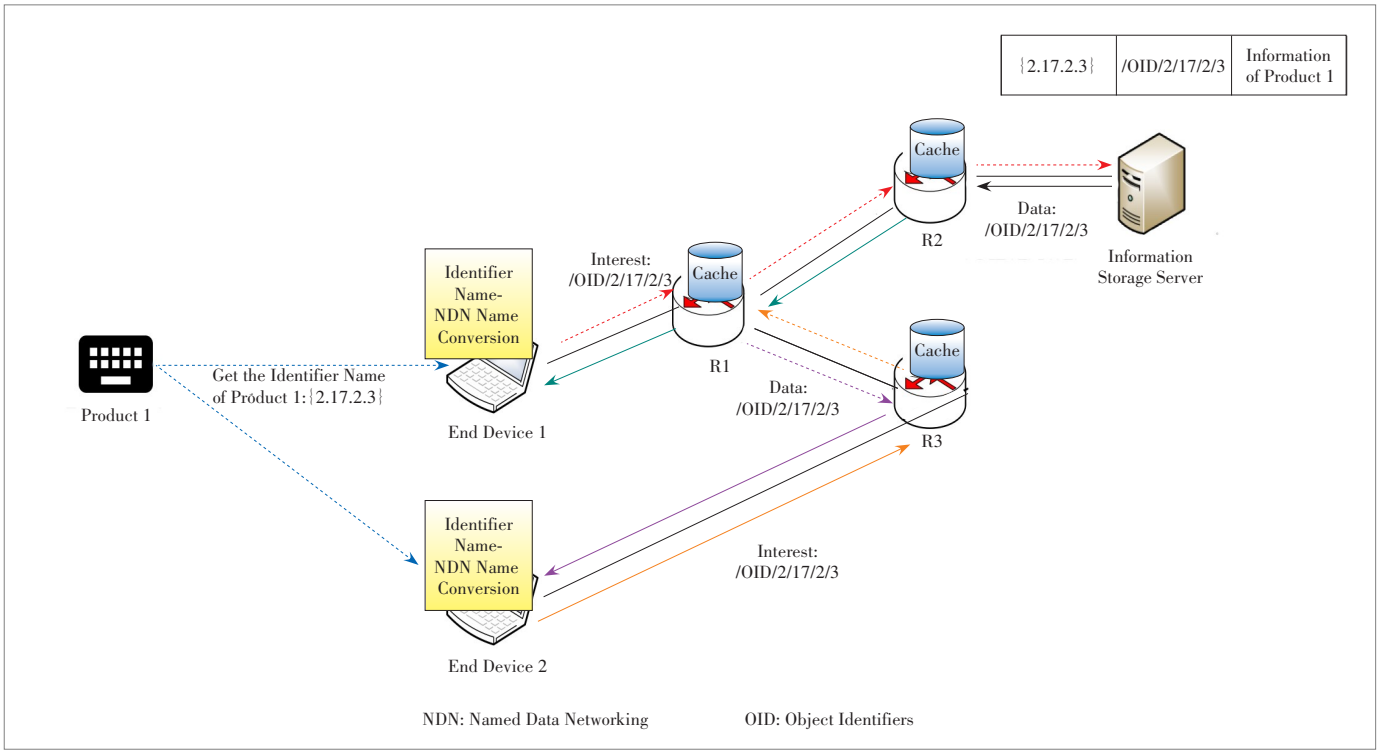
d) When the NDN router receives this data packet, it returns the data packet to end device 1 along the reverse way of interest according to the standard NDN node processing model [20], and caches this data packet according to the local caching strategies. The cached entry in the local cache contains /OID/2/17/2 and the information of product 1.

3) End device 2 requests the same identifier query.

a) End device 2 also requests to query the information of this product. It obtains the identifier name of product 1, and converts it to the NDN identifier name. It constructs an interest packet and sends the interest to the NDN network.

b) When this interest arrives at R1 via R3, because this product information is already stored in the local cache of R1, R1 can directly return the data packet (/OID/2/17/2/3).

c) The data packet is returned from R1 to end device 2 via R3, thus completing the identifier query request.



▲**Figure 8. The workflow of the merging architecture.**

4 Conclusions

In this paper, we overviewed the industrial network, industrial Internet identity, and ICN. We presented an integrated architecture for industrial network and industrial Internet identity. We proposed the overall framework of ICN-based industrial network and NDN-based factory extranet with SDN. We also addressed the architecture of identity resolution in the industrial Internet based on ICN with separate resolution nodes or with merging resolution and routing. By introducing ICN into the industrial Internet, we realized the integration of industrial network and identity resolution system, flattening the overall architecture of the industrial Internet, improving the efficiency of information retrieval, network scalability, and data security.

References

[1] DUAN S H, GAO W, WANG J P. A Novel Network Control Architecture for Large Scale Machine in Industrial Internet [C]//IEEE International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI). Beijing, China, 2015: 229 – 232.DOI: 10.1109/iiki.2015.56
[2] XYLOMENOS G, VERVERIDIS C N, SIRIS V A, et al. A Survey of Information-Centric Networking Research [J]. IEEE Communications Surveys & Tutorials, 2014, 16(2): 1024 – 1049. DOI: 10.1109/surv.2013.070813.00063
[3] GOGOLEV A, MENDOZA F, BRAUN R. TSN-Enabled OPC UA in Field Devices [C]//IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA). Turin, Italy, 2018: 297 – 303. DOI: 10.1109/etfa.2018.8502597
[4] MANNWEILER C, GAJIC B, ROST P, et al. Reliable and Deterministic Mobile Communications for Industry 4.0: Key Challenges and Solutions for the Integration of the 3GPP 5G System with IEEE [C]//Mobile Communication-Technologies and Applications; 24. ITG-Symposium. Osnabrueck, Germany, 2019: 1 – 6
[5] NSAIBI S, LEURS L, SCHOTTEN H D. Formal and Simulation-Based Timing Analysis of Industrial-Ethernet Sercos III over TSN [C]//IEEE/ACM 21st International Symposium on Distributed Simulation and Real Time Applications (DS-RT). Rome, Italy, 2017: 83 – 90. DOI: 10.1109/distra.2017.8167670
[6] BRUCKNER D, BLAIR R, PSTANICA M, et al. OPC UA TSN-A New Solution for Industrial Communication [R]. B&R Industrial Automation, 2018
[7] AL-GUMAEI K, SCHUBA K, FRIESEN A, et al. A Survey of Internet of Things and Big Data Integrated Solutions for Industrie 4.0 [C]//IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA). Turin, Italy, 2018: 1417 – 1424. DOI: 10.1109/etfa.2018.8502484
[8] IETF. Deterministic Networking Architecture: RFC 8655 [S]. 2019
[9] CHAUDHARY R, AUJLA G S, GARG S, et al. SDN-Enabled Multi-Attribute-Based Secure Communication for Smart Grid in IIoT Environment [J]. IEEE Transactions on Industrial Informatics, 2018, 14(6): 2629 – 2640. DOI: 10.1109/tii.2018.2789442
[10] LI X M, LI D, WAN J F, et al. Adaptive Transmission Optimization in SDN-Based Industrial Internet of Things with Edge Computing [J]. IEEE Internet of Things Journal, 2018, 5(3): 1351 – 1360. DOI: 10.1109/jiot.2018.2797187
[11] DATTA S K, BONNET C. MEC and IoT Based Automatic Agent Reconfiguration in Industry 4.0 [C]//IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). Indore, India, 2018: 1 – 5. DOI: 10.1109/ants.2018.8710126
[12] UGWUANYI E E, GHOSH S, IQBAL M, et al. Reliable Resource Provisioning Using Bankers' Deadlock Avoidance Algorithm in MEC for Industrial IoT [J]. IEEE Access, 2018, 6: 43327 – 43335. DOI: 10.1109/access.2018.2857726
[13] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Communication for Automation in Vertical

Domains: TR 22.804 [S]. 2017
[14] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for Cyber-Physical Control Applications in Vertical Domains: TR22.104 [S]. 2019
[15] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Security for 5GS Enhanced Support of Vertical and LAN Services: TR 33.819 [S]. 2020
[16] BROCK D L. The Electronic Product Code (EPC) [R]. Cambridge, United States: Auto-ID Center White Paper MIT-AUTOID-WH-002, 2001
[17] Orange SA. Object Identifier (OID) Repository [EB/OL]. (2020-01-05). http://www.oid-info.com
[18] IETF. Handle System Overview: RFC 3650 [S]. 2003
[19] MAEDA M. System and Method for Initially Configuring and Booting a Device Using a Device Identifier: U.S. Patent No. 7293168 [P]. 2007-11-06
[20] ZHANG L X, AFANASYEV A, BURKE J, et al. Named Data Networking [J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66 – 73. DOI: 10.1145/2656877.2656887
[21] KOPONEN T, CHAWLA M, CHUN B G, et al. A Data-Oriented (and Beyond) Network Architecture [J]. ACM SIGCOMM Computer Communication Review, 2007, 37(4): 181. DOI: 10.1145/1282427.1282402
[22] GARCIA-LUNA-ACEVES J J, MIRZAZAD-BARIJOUGH M, HEMMATI E. Content-Centric Networking at Internet Scale through the Integration of Name Resolution and Routing [C]//3rd ACM Conference on Information-Centric Networking (ACM - ICN' 16). Kyoto, Japan, 2016: 83 – 92. DOI: 10.1145/2984356.2984359

Biographies

LU Hua received his master's degree in information and communication from Jeonbuk National University, Republic of Korea. He is the director of the Network Technology Innovation Center of Guangdong Communication & Network Institute, China. He worked with ZTE Corporation and was engaged in the research and development of wireless base stations, core networks, bearer networks, virtualization and other system products. He has 15-year experience of research and development of industrialization in baseband channel codec, voice codec, router, and virtualization. His research interests include new network architecture, software-defined networking, P4 programmable, and virtualization.

LI Xiaolu (lixiaolu@bupt.edu.cn) received her B.S. degree in telecommunication engineering from Beijing University of Posts and Telecommunications (BUPT), China in 2017. She is currently working toward her Ph.D. degree at the State Key Laboratory of Networking and Switching Technology, BUPT. Now she is visiting Carleton University, Canada as a visiting Ph.D. student. Her current research interests include future network architecture design, information centric networking, software defined networking, edge intelligence, and the industrial Internet.

XIE Renchao received his Ph.D. degree from the School of Information and Communication Engineering, BUPT in 2012. From July 2012 to September 2014, he worked as a postdoctoral researcher at China Unicom. From November 2010 to November 2011, he visited Carleton University as a visiting scholar. He is currently an associate professor with BUPT. His current research interests include future network architecture design, information centric networking, 5G networks, and the industrial Internet. He has published more than 30 journal and conference papers. He served on the Technical Program Committees (TPCs) of Chinacom 2016 and 2012 IEEE Vehicular Technology Conference (VTC)-Spring. He has also served for several journals and conferences as a reviewer, including IEEE Transactions on Communications, ACM/Springer Wireless Networks, the EURASIP Journal on Wireless Communications and Networking, Wireless Communications and Mobile Computing (Wiley), IEEE Communications Letters, 2011 IEEE GLOBECOM, and so on.

FENG Wei is a visiting scholar of University of Cambridge, United Kingdom. He is working at the Department of Information Technology Application and Software Services, Ministry of Industry and Information Technology of People's Republic of China. His research interest is the industrial Internet of Things.

Identifier Management of Industrial Internet Based on Multi-Identifier Network Architecture

WANG Yunmin[1,2], LI Hui[1,2], XING Kaixuan[1], HOU Hanxu[3], Yunghsiang S. HAN[3], LIU Ji[1], and SUN Tao[4]

(1. Shenzhen Graduate School, Peking University, Shenzhen, Guangdong 518055, China;
2. Pengcheng Laboratory, Shenzhen, Guangdong 518000, China;
3. School of Electrical Engineering and Intelligentization, Dongguan University of Technology, Dongguan, Guangdong 523808, China;
4. The Network and Information Center of Shenzhen University Town, Shenzhen, Guangdong 518055, China)

Abstract: The industrial Internet realizes intelligent control and optimized operation of the industrial system through network interconnection. The industrial Internet identifier is the core element to accomplish this task. The traditional industrial Internet identifier resolution technologies depend excessively on IP networks, and cannot meet the requirements of ubiquitous resource-restraint Internet of Things (IoT) devices. An industrial Internet identifier resolution management strategy based on multi-identifier network architecture is proposed in this paper, which supports content names, identities, locations, apart from the traditional IP address. The application of multiple types of identifiers not only solves the problem of IP addresses exhaustion, but also enhances the security, credibility, and availability of the industrial Internet identification resolution system. An inter-translation scheme between multiple identifiers is designed to support multiple identifiers and the standard ones. We present an addressing and routing algorithm for identifier resolution to make it convenient to put our strategy into practice.

Keywords: identifier resolution; industrial Internet; inter-translation; multiple identifier; routing and addressing

DOI: 10.12142/ZTECOM.202001006

http://kns.cnki.net/kcms/detail/34.1294.TN.20200316.1732.012.html, published online March 17, 2020

Manuscript received: 2019-12-09

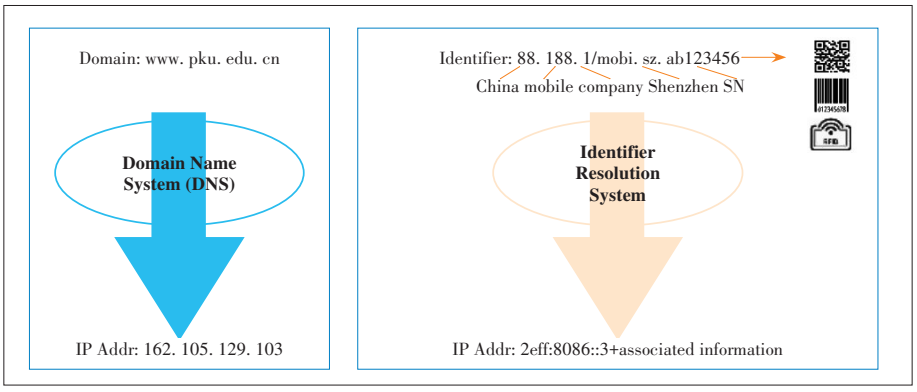
Citation (IEEE Format): Y. M. Wang, H. Li, K. X. Xing, et al., "Identifier management of industrial internet based on multi-identifier network architecture," *ZTE Communications*, vol. 18, no. 1, pp. 36 - 43, Mar. 2020. doi: 10.12142/ZTECOM.202001006.

1 Introduction

The industrial Internet is an intelligent closed loop driven by data and integrated by Information Technology (IT) and Operational Technology (OT). The identifiers of the industrial Internet will spread the hosts in the traditional Internet to resources such as goods, information, machines, and services, and extend the IP addresses to a heterogeneous, off-site, and refined information set [1]. The identifier resolution system consists of an identifier coding system and a resolution system [2]. The identifier code is the identity card of the machine or the goods, and the resolution system uses the identifiers to locate and query the machine or the goods uniquely. Identifier resolution is the premise of the supply chain system, the production system, the complete lifecycle management, and the intelligent service. Identifier resolution provides a technical support on unified network layer for cross-industry/inter-disciplinary industrial Internet platforms and enables intelligent association of heterogeneous devices

This work is supported in part by PCL Future Regional Network Facilities for Large-scale Experiments and Applications under Grant NO. PCL2018KP001, by Guangdong R&D Key Program under Grant No. GD2016B030305005, by National Natural Science Foundation of China (NSFC) under Grant No. 61671001, by National Key R&D Program of China under Grant No. 2017YFB0803204 and by Shenzhen Research Programs under Grant Nos. JSGG20170824095858416, JCYJ20190808155607340, and JCYJ20170306092030521. This work is also supported by the Shenzhen Municipal Development and Reform Commission (Disciplinary Development Program for Data Science and Intelligent Computing).

and services from different vendors. Similar to the Domain Name System (DNS) in the traditional Internet, the industrial Internet identifier resolution system is the gateway to the entire industrial Internet, as shown in **Fig. 1**. Besides, it is the basis for the interconnection of the whole industrial Internet.



▲**Figure 1. An Industrial Internet identifier.**

The identifier resolution system is an essential part of the industrial Internet architecture, and also a nerve hub supporting the interconnection of the industrial Internet [3]. Flexible identifier differentiation and information management of the entire network resources are achieved by assigning each product, component, machine, or device or digital intellectual property copyright a unique "identity card". Industrial Internet identifier resolution refers to the unique positioning and relevant information query of machines, goods, and digital knowledge products. At the same time, the global supply chain system and enterprise production system can be accurately connected.

IP protocol is the backbone protocol of contemporary Internet connection. In the meantime, various universal industrial Internet identifier resolution systems, such as Handle [4], Object Identifier (OID) [5], Ubiquitous ID (UID) [6], and Global Standard 1 (GS1) [7], are also designed and running upon the IP architecture [8]. However, the industrial Internet often contains many resource-constrained devices, which have smaller memory, limited computing power, and energy. Sensors and actuators often raise communication requirements in industrial applications that are critical for business and safety. Besides, the design concept of the IP model is based on a host-to-host communication mode, which will become a bottleneck to deal with high traffic and high bandwidth environment.

Moreover, regarding the particular application scenarios, identifier authentication, Quality of Service (QoS) assurance, and the network efficiency are not supported by the current Transmission Control Protocol / Internet Protocol (TCP/IP) protocol stack. In the future, the integration of terrestrial Internet and satellite-based space Internet is a possible technical requirement of the industrial Internet [9].

This paper proposes an Internet identifier resolution management system based on the multi-identifier network architecture. It eliminates the malpractice and hidden dangers of excessive concentration on IP network management and control. The main contributions of this paper are listed as follows:

1) We propose a hierarchical network architecture with manageable and controllable trust and privacy protection that supports multiple identifier routing and addressing. The core of this network is that the network inherently supports multiple network identities for simultaneous routing and addressing, and assists users to access the new network system in multiple ways seamlessly. The identity of the user is integrated with the content published on the network, which can ensure the regular operation and management of the network. At the same time, the hierarchical signature scheme with high security and low complexity is introduced to ensure that the network data content cannot be tampered and stolen, which dramatically improves the security, credibility, and availability of the whole network.

2) We present the inter-translation schemes for multiple identifiers in order to solve the problem that multiple network identifiers and multiple standard identifiers inevitably coexist.

3) An addressing algorithm is designed to speed up the lookup process of the identifier's name, which makes our proposal more convenient to be put into practice.

The remainder of this paper is outlined as follows. Section 2 provides background and related work. We describe in detail the design essentials of the autonomously controllable multiple identifier systems for the industrial Internet in Section 3. Inter-translation of multiple network identities is presented in Section 4, and addressing algorithms for large scale identifier space are proposed in Section 5. Section 6 concludes the paper.

2 Related Work and Background

2.1 National Industrial Internet Identifier Resolution System

The national industrial Internet identifier resolution system of China is designed with three levels: international root nodes, national top nodes, and secondary nodes, besides recursive resolution nodes along with all these levels, as shown in **Fig. 2**. By the end of 2018, five national top-level nodes of identifier resolution in Beijing, Shanghai, Guangzhou, Wuhan, and Chongqing were put into operation, fully supporting various identifier systems. By the end of 2019, 47 secondary nodes had been set up, and the number of identifier registrations has reached 915 million, with 785 pertinent enterprises [10].

The national top-level nodes act as the foundation, which continuously improve the system functions and capabilities

based on the established plan and gradually build the network infrastructure of the identifier and resolution system of open integration, unified management, interconnection, security, and reliability. The secondary nodes are the graspers, a number of which have been playing their roles in pioneering new approaches [11]. They are built to promote the integrated innovation application of industrial Internet identifier resolution. Lastly, industrial applications are the purpose of identifier resolution. It can encourage the application demonstration in many industries such as aviation and machinery vehicles, and gradually build the identifier resolution industry ecology.

2.2 Named Data Networking

Named Data Networking (NDN), a content-based future network architecture, was proposed ten years ago [12], [13]. NDN replaces host-addressed IP packets with named data as a new narrow waist of the hourglass protocol stack. Each data object has a hierarchy name that is used as a unique identifier in the application context that publishes and consumes the data. In order to request a data object, an interest is sent with a prefix of the data name. The NDN forwarder forwards the interest packet towards the location where the data may be located. Each forwarder along the path records the interest and its incoming interface in the local Pending Interest Table (PIT). When a matched packet is found either in the forwarder's cache or from the original producer, the packet will be returned to the requester along the reverse path recorded in the PITs of the nodes. A copy of the data packet will be stored in their local caches after forwarding to satisfy the future requirements for the same data request. The data packet has an encrypted signature generated by its producer, together with the name of the signing key, which allows data consumers to verify the provenance of the received data regardless of its source. Compared with the traditional IP network, it is more suitable for the demand of industrial Internet content and has the potential to solve the problems and challenges of the industrial Internet on the network layer. Specifically, for the industrial Internet, NDN is superior to IP in security, mobility, scalability, and quality of service [14].

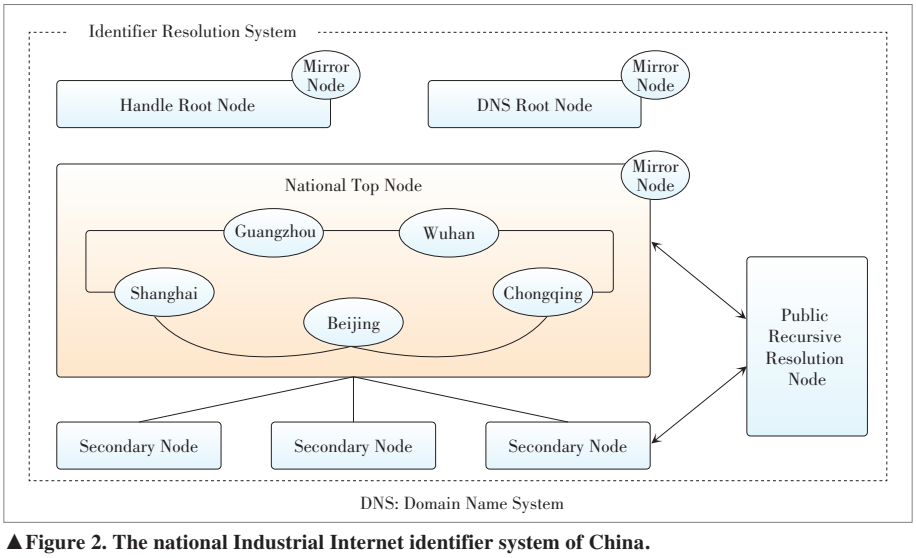
However, NDN only supports the content network identifier, so the solution for constructing an industrial Internet identifier based on NDN also has significant drawbacks in its unbound name length and publish-subscribe data acquisition model. NOUR et al. propose a hybrid name scheme for heterogeneous devices [15] and recent advances in how to exploit NDN for IoT scenarios are surveyed in [16].

Therefore, it is urgent to construct a multi-identifier future network model in which identifier serves as the content center. The data exchange between nodes is based on identity, content, service, ground space location, besides the IP address of the endpoint. Content-centric networks increase efficiency for content delivery, especially when the content is stored in multiple nodes, and content providers or content requesters are in the process of moving.

3 Autonomously Controllable Multi-Identifier Architecture for Industrial Internet

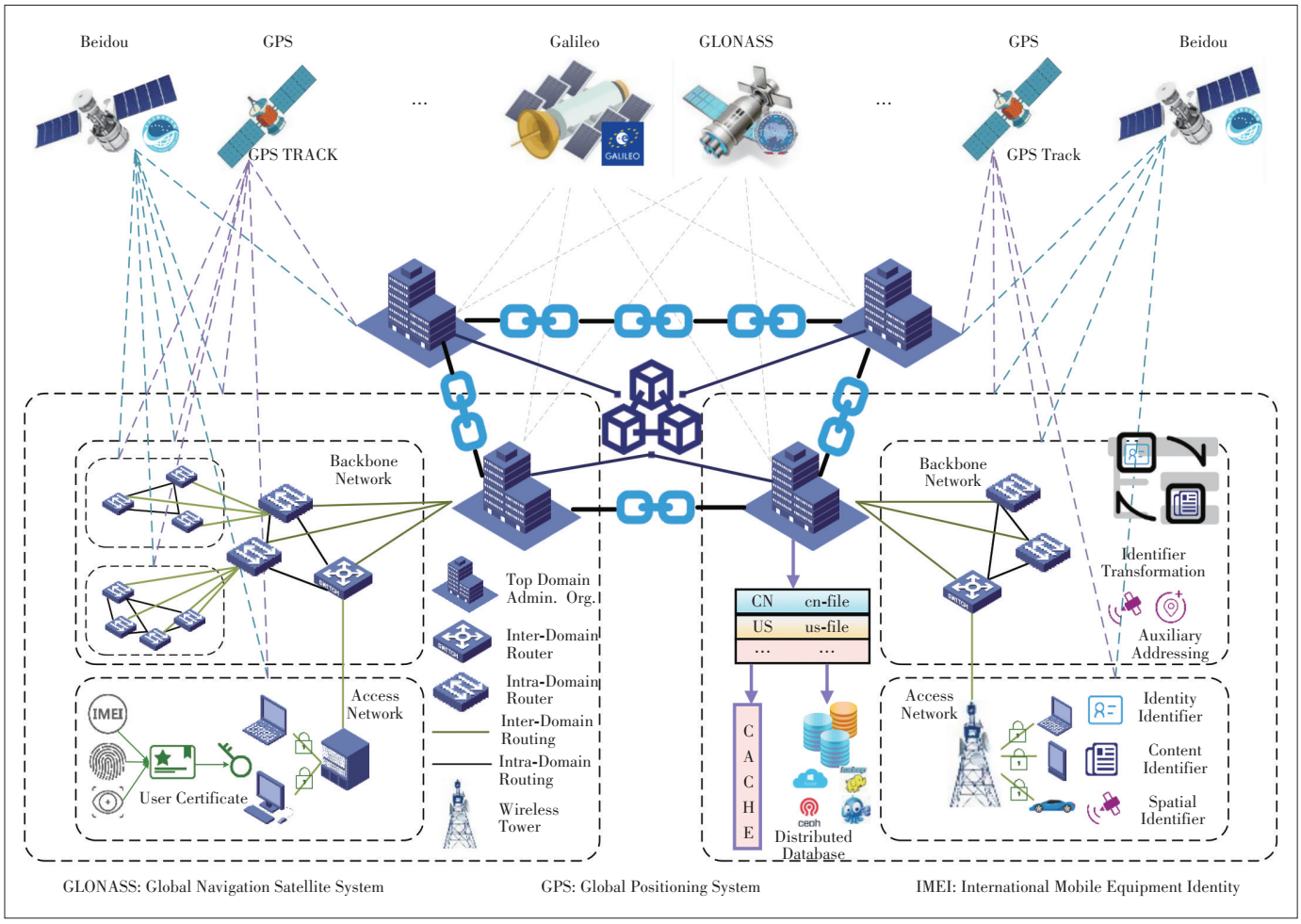
3.1 Multiple Identifier Management

This proposal dispenses the dependence of the traditional industrial Internet and IP networks, based on a multi-identifier future network architecture. The system breaks through the current dilemma of IP single identifier and centralized management. It constructs an industrial Internet identifier service platform based on the voting-based consortium blockchain [17], and supports network addressing and routing with multiple identifiers and parallel coexistence, including identity, content, service, location, and IP address, as shown in **Fig. 3**. The dilemma of unilateral monopoly is broken in the centralized management of domain names of the IP system [18].



▲**Figure 2. The national Industrial Internet identifier system of China.**

1) Name. Name is a hierarchical string that is used to identify each resource in the network. In order to support the addressing process of content name directly, the multi-identifier network nodes have a forwarding information table with a name as the key to record the corresponding forwarding port information. The data transmission is performed in a user-driven manner: the content requester puts the content name into an interest message and sends it to the network; the routing node records the arrival port of this interest message in the PIT and queries the Forwarding Information Table (FIB) [19]; The mes-



▲**Figure 3. Multi-identifier future network architecture.**

sage is forwarded until it reaches a holder of the content; by querying the pending interest table, the packet containing the requested content will be traced back to the requester along the arrival path of the interest message; the name-oriented addressing process will decouple the data itself from the specific location of the data, which provides more flexibility to the network system.

2) Identity. The identity is used to identify a user locally or globally. The favorite identity identifiers include the public key, the user's ID, the International Mobile Equipment Identity (IMEI) code of the mobile phone, the email address, and other various identities, besides biometrics information such as the face, fingerprint, pupil, and voice. The behaviors of users on the network, including the issuance and access to network resources, will be subject to the specific authority determined by their identity, and each behavior can be traced back to the identity information of the user.

3) Location. The location information can not only represent the geographical location in the real sense, but also represent the virtual location in the abstract space, such as the mathematical coordinates acquired by the nodes after mapping the network into the geometric space. The addressing process for spatially geographical location is that the multi-identifier network nodes calculate the geometric distance between each neighbor and the destination, and the smallest one is greedily selected as the forwarding object. And global navigation satellite system (GNSS), such as Galileo in EU, Beidou in China, Global Positioning System (GPS) in USA, Global Navigation Satellite System (GLONASS) in Russia are supported in our system, as shown in Fig. 3.

3.2 Identifier Registration and Request

The network supports routing and addressing with multiple types of identifiers, including the identity identifier, content identifier, spatial location identifier, and IP address identifier. The content identifiers of all resources in the network are bound to the identity identifier of the publisher. After a user logs into the network, the spatial location identifier and the accessed network resources will be recorded in the network supervision node of blockchain for security supervision and data protection.

The identifier registration steps are as follows.

Step 1 is resource content registration. The network node receives the resource content registered by the user. At the same time, it adds the identity identifier of the content publisher and the spatial location identifier according to the location of the node where the content is stored.

Step 2 is network node authentication. After receiving the identifier registration request transmitted by the user, the network node will review the content and its user information, register the resource identifier, and then register the generated identifier to the upper-level domain and add the local identifier prefix.

Step 3 is identifier registration request transmission. After receiving the identifier registration request, the upper-level network node transmits its registration identifier message to the controller of the located domain, for subsequent authentication and registration operations based on the predefined data transmission protocol.

Step 4 is identifier verification. After receiving the identifier registration request from the subordinate network domain, the network node in the top-level domain will verify the data of the request and return the corresponding confirmation signal to the original application node. The distributed storage scheme ensures that all registered identifiers cannot be tampered with. The original identifier information will be stored on the distributed database of the top-level domain. After a predefined time, corresponding database synchronization will be carried out within the entire network to confirm that the resource identifier information between the respective top-level domains is equivalent and unified.

The network resource requesting steps are as follows.

Step 1 is inquiry request. Transmitting a query request to the nearest network node.

Step 2 is local identifier data query. When the nearest multi-identifier network node receives the request sent by the user, it will distinguish the identifier type according to the identifier of the query. If it is an IP address, it will go on with the traditional DNS query process. Otherwise, if it is an identity or content identifier, then it will query the forwarding table. If the identifier content recorded in the forwarding table already exists in the local database, the corresponding identifier content will be returned, otherwise Step 3 will be executed.

Step 3 is requesting query transmission. When there is no corresponding identifier contained in the local database, the query request will be uploaded to the upper-level network node. After receiving the query request, the upper-level network node will query the identifier following Step 1 to Step 2. If the corresponding identifier content is queried, it will be returned to the low-level network node; otherwise, the query request is subsequently transmitted to the upper-level network node recursively until the top-level domain network node.

Step 4 is identifier query, verification, and interworking. After the top-level domain nodes find the relevant registered identifier, it will automatically issue the relevant shortest path according to the dynamic topology of the existing network. The related multi-mode network nodes on the forwarding path in the network will receive a new forwarding path table and establish a data transmission path through multi-hop routing; if the nodes in the top-level domain do not find the corresponding identification and query other network identification information corresponding to the identification in the database, proceed to Step 5.

Step 5 is the identifier request distribution. The network node in the top-level domain will distribute the query request to the specified network domain according to the original identifier and the first prefix after the identifier is converted, until the lowest-level network node specified by the query request is locally queried. If the corresponding identifier content is found successfully, it is delivered to the query requester; otherwise, the query error information is returned.

4 Inter-Translation of Multiple Network Identities

When a piece of content is registered and published on a multi-identifier network, the name content can be bound with multiple identifiers, such as identity, content, location information, and IP address. Therefore, there is a need for multiple identifiers to be commonly addressed. In addition, the identifiers in the industrial Internet should be application-oriented and record the product information. On the other hand, it should support addressing and routing. Due to the diversity of the applications, it is difficult to establish a global hierarchical naming scheme that is suitable for all applications.

Therefore, on the multi-identifier-based industrial Internet service platform, multiple network identifiers and multiple standard identifiers coexist. A globally unique namespace needs to be established, as well as a unique namespace for each application. The multi-identifier translation table is utilized to establish an Inter Translation Table (ITT) and interoperability mechanism with existing common identifiers.

4.1 Translation Process Between Name and Identity

In order to maintain a secure network environment, we bind the name of the content to the identity of its original publisher, and use a valid extension to identify network resources in the following mode: $/UniqueID_A/SubID_A/Name/Sig(Name,PrK_A)$. $UniqueID_A$ is the globally unique identifier of the publisher A, and no collision occurs; it will generate the public-private key pair of the user. $SubID_A$ is the secondary identifier when the content is published, because the same user in the network may have multiple identities. *Name* is the hierarchical content name and $Sig\ (Name,\ PrK_A)$ is the signature of the content name signed by *A*. Before the content is received by the user or cached at the intermediate routing node, its signature must be verified to ensure its legitimacy based on the security mechanism described above. As a result, any resource in the

network can be traced back to its original publisher, which guarantees the regulatory nature of the publishing behavior and the security of network transmission. Under this representation, an identifier can be regarded as a particular form of extension names, that is, those with empty content names. Therefore, we use the prefix tree data structure to support storage and query operations on names and identities.

Under this representation method, identity can be regarded as a special form of extension name, that is, when the content name is empty, we use the prefix tree as a data structure to support the storage and query operations of names and identities (**Fig. 4**).

4.2 Translation of Location, Name, and Identity

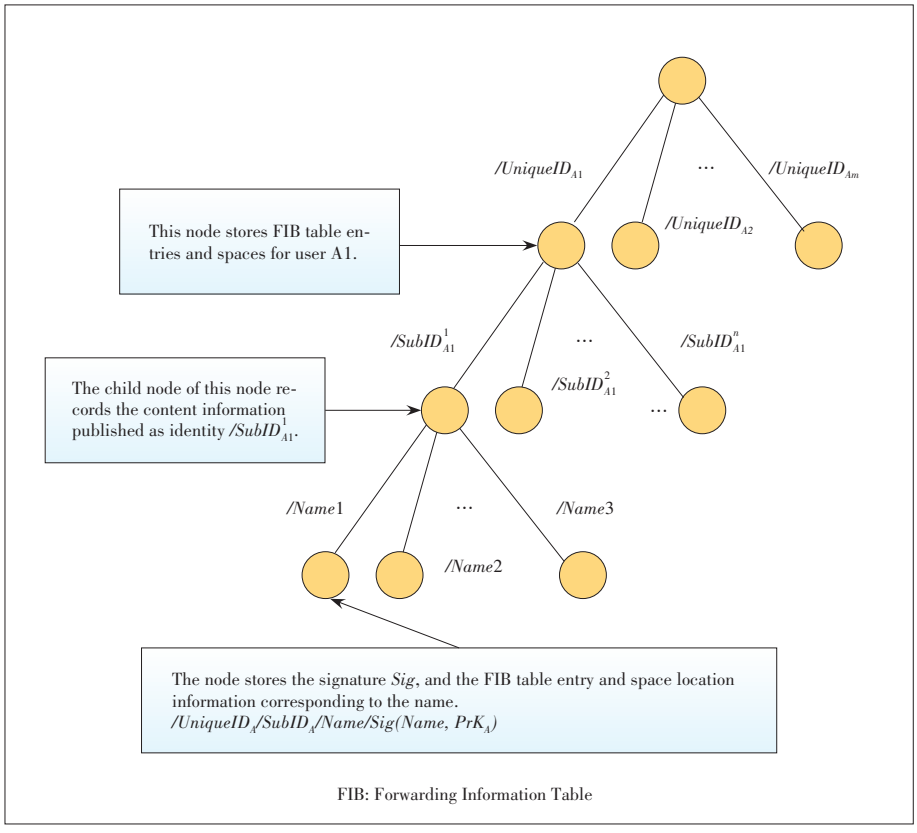
As mentioned above, each user corresponds to a uniquely real or virtual spatial location identifier. In order to reduce the routing delay, we set the location identifier of the name in a network to the nearest node location holding the corresponding content of the name, which is calculated and distributed by the upper control node. **Fig. 5** shows the transformation sequence with the following four steps.

1) A resource request is issued with a particular identifier.

2) The multi-identifier system performs queries based on the identifier type. If the request is issued with traditional domain names, DNS is queried directly. If it is an IP address and exists in the identification Inter-translation Forwarding Table (IFB), mutual translation is performed; otherwise, the agent accesses traditional IP networks. If it is other type of identifiers such as an NDN identifier, or an identity identifier, the content identifier is first queried in the Content Store (CS), Pending Interest Table (PIT) and inter-translation forwarding table. If it exists, an inter translation is performed; otherwise, go to Step 3.

3) If the identifier does not exist in the current domain, the multi-identifier system will recursively query up to the top domain.

4) If there is no such identifier information in the top-level domain, the query will be performed according to the specific lower-level domain of the identifier information, until the bottom-level domain specified by the identifier, and the corresponding result will be returned if it exists. Otherwise, a query error message is returned.



▲**Figure 4. Multiple identifiers forwarding architecture using prefix tree structure.**

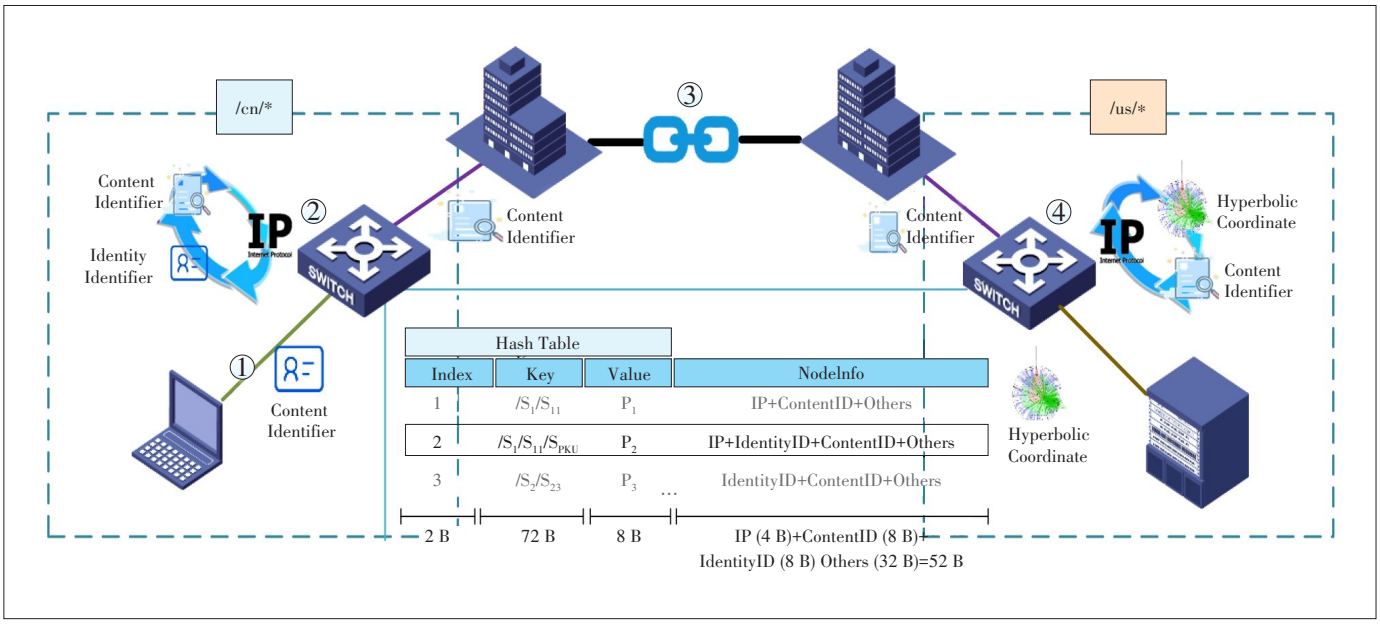
5 Addressing Algorithm for Large-Scale Identifier Space

In order to meet the needs of distributed storage, classification, addressing and forwarding services of ultra-billion-level industrial Internet identifier, a hierarchical distributed storage strategy is proposed to study the hyperbolic addressing routing mathematical model and the fusion Hash Prefix Tree (HPT) algorithm. The index expansion problem of the forwarding table has to be solved and the forwarding strategy optimized to improve the success rate of the addressing route.

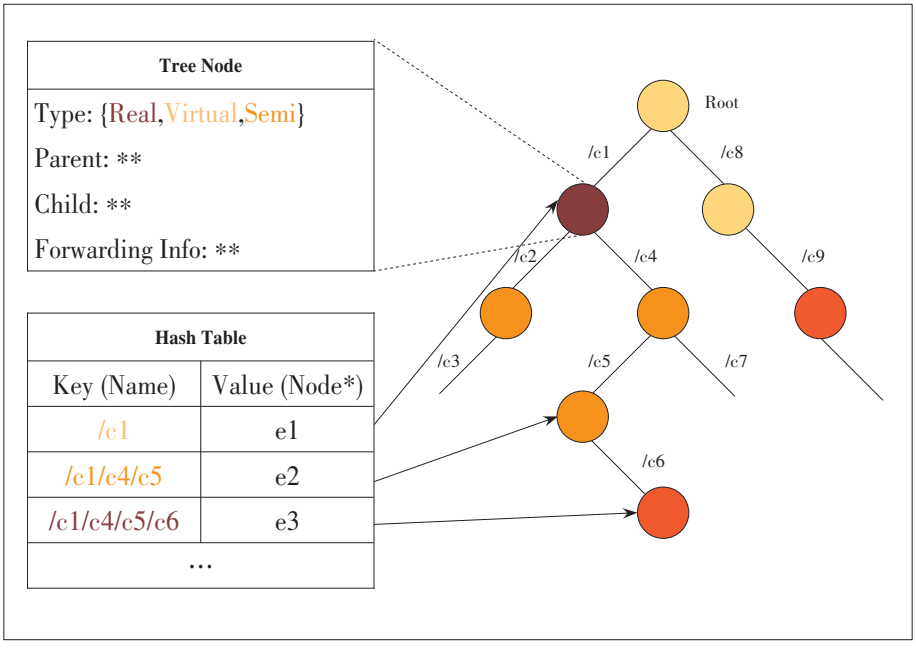
We designed a FIB composed of a hash table and a prefix tree [20], where the hash table is used to support fast lookups, and the prefix tree is used to store logical relationships between names. The main structure of FIB is demon$^{1}_{A1}$strated in **Fig. 6**.

In the hash table, the name (such as /C1/C4/C5) is used as the key. Moreover, the pointer to the node in the prefix tree is used as the value. Thus, the fast retrieval of forwarding information from name to tree is realized.

The edge in the prefix tree represents a name component (such as /C1). On the other hand, each node represents a splicing of all components in the path from the requester node to the root node. The node stores the forwarding information corresponding to the name, the corresponding category of the table item, and the pointer used to maintain the tree structure. Because the name



▲Figure 5. The translation process of location, name, and identity.



▲Figure 6. Hybrid fowarding information table of hash table and prefix tree.

does not need to be recorded repeatedly in the tree, the introduction of tree structure will only bring limited additional storage overhead.

The prefix tree is introduced for the following three purposes:

1) The categories of non-real table items are modified conveniently in a dynamic environment. For example, if "/C1" is inserted into FIB, all virtual table items prefixed with "/C1" need to change their categories into semi-virtual ones. For the diversity of the NDN identifier, this modification can only be realized by traversing the whole table without the help of tree structure.

2) The backtracking process is speeded up in the search algorithm. Each node in the tree has only one parent node, the process of backtracking does not need to query and match names or components, so it achieves a faster search speed.

3) It facilitates the removal of the obsolete unreal table items in time, that is, the leaf nodes with non-real types. In the process of table algorithm, as long as all kinds of leaf nodes are real, unnecessary table items can be cleaned up.

6 Conclusions

The ubiquitous industrial Internet makes it a challenge to design a suitable identifier resolution system. In this paper, an industrial Internet identifier resolution management strategy based on multi-identifier network architecture is proposed, which supports content name, identity, service, and location, besides the traditional IP address. Identification management is also included in our proposal, such as identification registration and request and data addressing and forwarding. The inter-translation scheme and address algorithm proposed in this paper show a better performance in the identification resolution management of the industrial Internet.

References

[1] QIN W, CHEN S Q, PENG M G. Recent Advances in Industrial Internet: Insights and Challenges [J]. Digital Communications and Networks, 2020, 6(1): 1 – 13. DOI: 10.1016/j.dcan.2019.07.001
[2] YANG Z, ZHANG D, LI J, et al. Identifier Technology in Industrial Internet [J]. Telecommunications Science, 2017, 33(11): 134 – 140, DOI: 10.11959/j.issn.1000-0801.2017296
[3] CHEN W. Intelligent Manufacturing Production Line Data Monitoring System for Industrial Internet of Things [J]. Computer Communications, 2020, 151: 31 – 41. DOI: 10.1016/j.comcom.2019.12.035
[4] HANDLE.NET (Ver. 9) Technical Manual [EB/OL]. (2019-07-26) [2019-11-28]. http://hdl.handle.net/20.1000/113
[5] SOUSA P, SILVA A R, MARQUES J A. Object Identifiers and Identity: a Naming Issue [C]//IEEE International Workshop on Object Orientation in Operating Systems. Lund, Sweden, 1995: 127 – 129.DOI: 10.1109/iwoos.1995.470569
[6] CenterU. I.. Ubiquitous Code: Ucode2009 [EB/OL]. (2009-07-28) [2019-12-01]. http://www.uidcenter.org
[7] GS1 Data Excellence Inc. GS1: The Global Language of Business [EB/OL]. [2019-01-12] (2020-01-02). https://www.gs1.org
[8] REN Y, XIE R, ZENG S, et.al. Survey of Identity Resolution System in Industrial Internet of Things [J]. Journal on Communications, 2019, 40(11): 138 – 155. DOI: 10.11959/j.issn.1000-436x.2019238
[9] SISINNI E, SAIFULLAH A, HAN S, et al. Industrial Internet of Things: Challenges, Opportunities, and Directions [J]. IEEE Transactions on Industrial Informatics, 2018, 14(11): 4724 – 4734. DOI: 10.1109/tii.2018.2852491
[10] LIU D. Promote the Integrated Development of 5G and Industrial Internet [R]. World 5G Convention, 2019
[11] LI H, QI Z. Thinking on Secondary Node Construction of Industrial Internet Identifier Resolution [J]. Information and Communications Technology and Policy, 2019, 296(02): 68 – 72. DOI: CNKI: SUN: DXWJ.0.2019-02-019
[12] JACOBSON V, SMETTERS D K, THORNTON J D, et al. Networking Named Content [C]//ACM Conference on Emerging Networking Experiments and Technologies. Rome, Italy, 2009: 1 – 12. DOI: 10.1145/1658939.1658941
[13] ZHANG L X, AFANASYEV A, BURKE J, et al. Named Data Networking [J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66 – 73. DOI: 10.1145/2656877.2656887
[14] SHANG W T, BANNIS A, LIANG T, et al. Named Data Networking of Things (Invited Paper) [C]//2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI). Berlin, Germany, 2016: 117 – 128. DOI: 10.1109/iotdi.2015.44
[15] NOUR B, SHARIF K, LI F, et al. A Unified Hybrid Information-Centric Naming Scheme for IoT Applications [J]. Computer Communications, 2020, 150: 103 – 114. DOI: 10.1016/j.comcom.2019.11.020
[16] ARSHAD S, AZAM M A, REHMANI M H, et al. Recent Advances in Information-Centric Networking-Based Internet of Things (ICN-IoT) [J]. IEEE Internet of Things Journal, 2019, 6(2): 2128 – 2158. DOI: 10.1109/jiot.2018.2873343
[17] LI H, HAN Y X, LI G X, et al. Prototype and Testing Report of a Multi-identifier System for Reconfigurable Network Architecture Under Co-Governing [J]. SCIENTIA SINICA Informationis, 2019, 49(9): 1186 – 1204. DOI: 10.1360/n112019-00070
[18] DIB O, BROUSMICHE K L, DURAND A, et al. Consortium Blockchains: Overview, Applications and Challenges [J]. International Journal on Advances in Telecommunications, 2018, 11(1): 51 – 64.
[19] YI C, AFANASYEV A, WANG L, et al. Adaptive Forwarding in Named Data Networking [J]. ACM SIGCOMM Computer Communication Review, 2012, 42 (3): 62. DOI: 10.1145/2317307.2317319
[20] LI Z, XU Y P, ZHANG B C, et al. Packet Forwarding in Named Data Networking Requirements and Survey of Solutions [J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1950 – 1987. DOI: 10.1109/comst.2018.2880444

Biographies

WANG Yunmin received his B.Sc. from Tianjin University, China in 2000. Now, he is a Ph.D. candidate at School of Electronics Engineering and Computer Science, Peking University, China. His research interests include future network architecture and the industrial Internet.

LI Hui (lih64@pkusz.edu.cn) received his B.Eng. and M.S. degrees from Tsinghua University, China in 1986 and 1989 respectively, and Ph.D. degree from The Chinese University of Hong Kong, China in 2000. He is now a full professor of the Shenzhen Key Lab of Information Theory and Future Network Architecture, Future Network PKU Lab of National Major Research Infrastructure, Shenzhen Graduate School, Peking University, China. His research interests include future network architecture, cyberspace security, blockchain technology, and distributed storage systems.

XING Kaixuan is a postgraduate student at Shenzhen Graduate School, Peking University, China. His research interests include new architectures and new generations of information communication technology.

HOU Hanxu received his B.Eng. degree in information security from Xidian University, China in 2010, and Ph.D. degrees from the Department of Information Engineering, The Chinese University of Hong Kong, China in 2015 and from the School of Electronic and Computer Engineering, Peking University, China. He is now an assistant professor with the School of Electrical Engineering & Intelligentization, Dongguan University of Technology, and honorary postdocter of the Department of Computer Science and Engineering, The Chinese University of Hong Kong. His research interests include erasure coding and coding for distributed storage systems.

Yunghsiang S. HAN received his Ph.D. degree from the School of Computer and Information Science, Syracuse University, USA in 1993. He is currently with the School of Electrical Engineering and Intelligentization, Dongguan University of Technology, China. He has also been a chair professor with Taipei University, China since 2015. He is an IEEE Fellow in error-control coding, wireless networks, and security.

LIU Ji is the director of the information office at Shenzhen Graduate School, Peking University, China. His research focuses on new network architecture.

SUN Tao is the director of The Network Information Center of Shenzhen University Town. His research interests include blockchain and cyberspace security.

Risk Analysis of Industrial Internet Identity System

TANG Kai
(ZTE Corporation, Shenzhen, Guangdong 518057, China)

Abstract: The risks of the current identity system represented by Domain Name System (DNS) and Object Identifier (OID) are studied. According to the characteristics of the industrial Internet Identity (III) system, four open ecosystem planes are divided, and a corresponding risk analysis view is established to analyze risks for various planes. This paper uses Isaiah Berlin's definition of liberty to more generally express the concept of security as positive rights and negative rights. In the risk analysis view, the target system is modeled from four dimensions: stakeholders, framework, architecture, and capability delivery. At last, three defensive lines are proposed to establish the identity credit system.

Keywords: industrial Internet; identity credit system; risk analysis view; right framework; security attribute

DOI: 10.12142/ZTECOM.202001007

http://kns.cnki.net/kcms/detail/34.1294.TN.20200316.1140.004.html, published online March 16, 2020

Manuscript received: 2019-12-10

Citation (IEEE Format): K. Tang, "Risk analysis of industrial internet identity system," *ZTE Communications*, vol. 18, no. 1, pp. 44 - 48, Mar. 2020. doi: 10.12142/ZTECOM.202001007.

1 Introduction

The traditional Internet identity system is based on Domain Name System (DNS) and Public Key Infrastructure (PKI) technologies, with which the Internet Corporation for Assigned Names and Numbers (ICANN)/Certificate Authority (CA) and other institutions maintain the Internet's root of trust and facilitate host-oriented addressing and authentication to meet the identity requirements of massive asymmetric web computing models. As the Internet economy penetrates into all areas of society, infrastructure maintainers and industry regulators have full credit to provide diversified identity endorsement capabilities without relying on the Internet's root of trust. For the sake of security and controllability, independent identity systems have been proposed in the industrial Internet field.

2 Risks of Traditional Industrial Identity Systems

Traditional industrial identity systems are dedicated identity systems for different industries. Object Identifier (OID) is a typical one, jointly proposed by International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) and International Telecommunications Union-Telecommunication Standardization Sector (ITU-T) [1]. An OID consists of identifier system, registration system and resolution system. Its resolution system makes use of the ubiquitous resolution capabilities of DNS.

As an important part of the Internet infrastructure, DNS is designed just like the Internet at the beginning, without security considerations, which has made it a main target and means for various network attacks, such as:

1) Distributed Denial of Service (DDoS) attacks against

DNS servers: including host exhaustion-based DNS query denial of service attacks and bandwidth exhaustion-based DNS reflector denial of service attacks (also known as DNS amplification attacks).

2) DNS hijacking against users: including DNS server address hijacking, hosts file hijacking, cache poisoning, Kaminsky cache poisoning, hacking DNS servers, etc.

Generally speaking, the traditional industrial identity systems have several risks as follows.

· Lack of authentication: Traditional DNS based industry identity systems need to be combined with other technologies to provide authentication capabilities. Due to the diversification of industry authentication scenarios, unified authentication mechanism cannot be specified from top design of the identity system.

· Lack of permission control: Finer-grained permission control is not available to meet the higher security requirements in some special scenarios.

· Lack of credible endorsement for identity: Authorized identity organizations do not have strong credit themselves, and often require third parties (such as regulatory authorities) to endorse in order to provide sufficient credit to the public and industry chain. However, the establishment and maturity of the identity credit system takes time.

· Interoperability risks with international roots: Not all root nodes of the identity system have backup in every country. Therefore, when interworking occurs, risks arise.

· Long authorization chain that leads to the dilution of credit: The superior nodes to inferior nodes lacks visibility and controllability from management to technology. As the authorization chain grows longer, the trust relationship weakens rapidly.

· Inadequate business admittance and certification: Lack of a mature certification standard and practice in the industry identity system is not conducive to the establishment of an identity credit system and long-term healthy development.

3 Ecosystem Planes of Industrial Internet Identity

In the 5G era, the Industrial Internet Identity (III) system is emerging with important meaning and rich connotation, covering all aspects of the industrial Internet in a broad sense. Its essence is an open identity system with a series of ecosystem characteristics. First of all, in an open Internet environment, the asset and value are the main characteristics of an identity ecosystem; secondly, the industrial Internet is based on the integration of Information Technology (IT) and Operational Technology (OT), and the identity has the characteristics of field and environmental relevance. The last, with strong industrialization, vertical regulation and control are often necessary.

In this paper, the III ecosystem is divided into four planes: the environment plane, service plane, asset plane, and business plane, according to [2]. As shown in **Fig. 1**, the III ecosystem combines new security characteristics at different planes to facilitate risk analysis.

4 Risk Analysis Process, View and Implementation

4.1 Risk Management Processes

In order to manage risks, each III ecosystem plane needs to support risk management processes, which are based on the ISO series of risk management guidelines, including risk analysis, risk evaluation, risk treatment, risk monitoring, etc. This article focuses on risk analysis (including risk identification).

ISO 31000: 2018 [3] and ISO 27005: 2018 [4] define general risk management guidelines and information security risk management guidelines, which can be used to guide the construction of a risk management system.

4.2 Building an III Oriented Risk Analysis View

The view of risk analysis is important for risk analysis and even risk management. As required by the principles in [3], risk management should be structured, comprehensive, customized and inclusive. It is necessary for III risk analysis to study the scope and open ecosystem characteristics of III system, conduct a comprehensive analysis based on a structured plane, and fully consider the demands of different stakeholders.

In order to analyze risks of different identity ecosystem planes, this paper builds a risk analysis view oriented to the characteristics of III system, based on mature methods and practice in the field of risk management and threat modeling. This is a more structured view of risk analysis for more logical processes and results (**Fig. 2**). The following is the analysis process with the proposed view.

1) Determining the scope and boundaries of the target system.

When using the risk analysis view, one first needs to determine the scope and boundaries of the target system and identi-

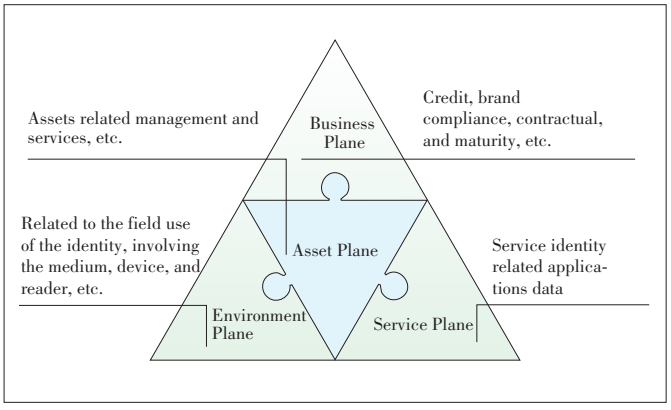
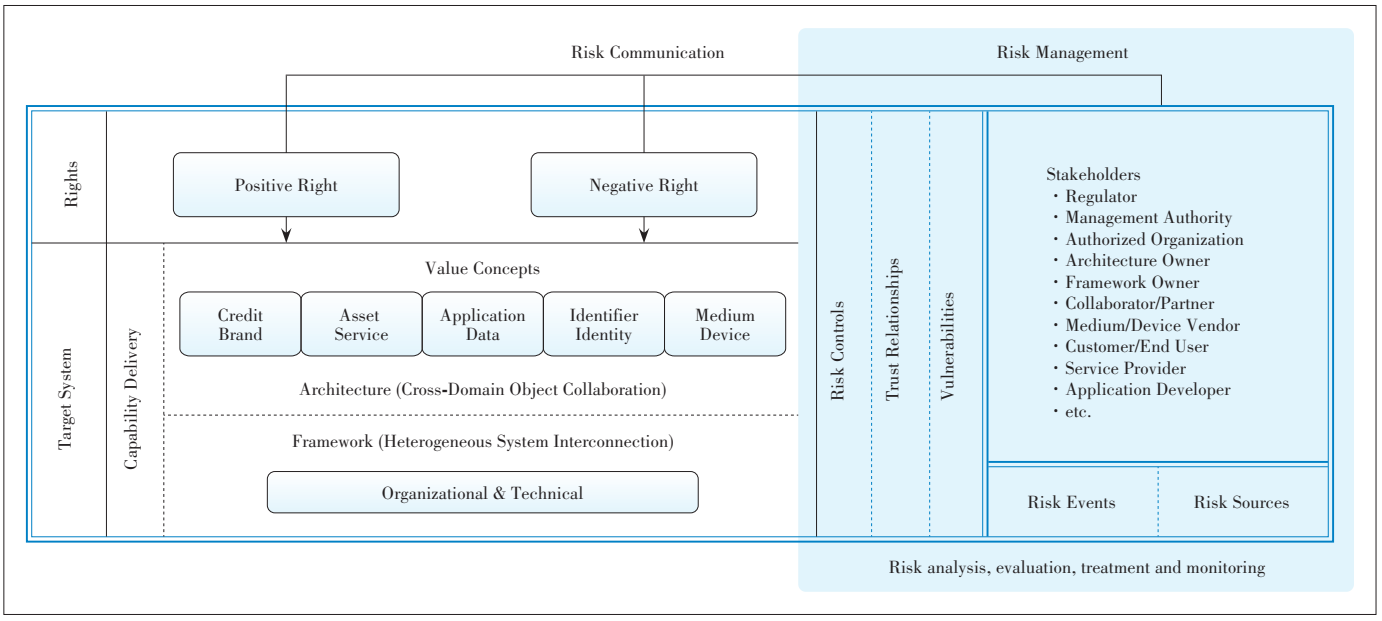


Figure 1. Industrial Internet Identity (III) ecosystem.



▲**Figure 2. Proposed view of the Industrial Internet Identity (III) risk analysis.**

fy III related objects. Different ecosystem planes have different scopes and objects. It is not appropriate to extend the scope and boundaries outside the III ecosystem. The main objects related to identity include identity related organizations and individuals, identified equipment or assets, various identity media such as Quick Response (QR) code, various basic identity services and auxiliary services, identifier and identity, various business information and data related to identity, etc.

2) Identifying stakeholders and right frameworks.

Isaiah Berlin has two definitions of the liberty: negative liberty and positive liberty [5]. Liberty is a sociological right, and security is a more general concept of rights. Here we use the definition of Isaiah Berlin to divide security into positive rights and negative rights. The right is closely related to the concept of stakeholders, and risk analysis always focuses on the rights of different stakeholders for different value concepts. Sometimes right is also treated as a security attribute.

The opposite of stakeholders is various sources of risks. They will use system vulnerabilities to launch attack events and bring risks to stakeholders.

Different ecosystem planes have different sets of right frameworks depending on the value concept of interest. For example, information security is mainly concerned with availability, confidentiality and integrity. Corresponding to security control, it is further expressed as Authentication, Authorization, Auditing (AAA) capabilities. This is also the theoretical basis of the six dimensions that Microsoft's Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE) threat model focuses on [6]. The privacy right that General Data Protection Regulation (GDPR) is concerned about is another type of right for human. Risk analysis requires more consideration of the sensitivity of different stakeholders to different rights.

The rights of different stakeholders may conflict, especially with the rights of regulators or decision makers. At this time, the use of a right framework can more clearly express this conflict relationship and help to form a balanced solution. In this process, risk communication is essential.

3) Reference industry mature practices.

After the above work is completed, mature reference models (attack models and abuse models) can be leveraged to conduct further risk analysis for capability delivery, object collaboration, and target system's framework, respectively. If required, further cuts can be made to the target system, with independent risk analysis for each subsystem.

Some examples of reference models are the Common Attack Pattern Enumeration and Classification (CAPEC) basis, DNS basis, cases of abuse based on traditional industry identification systems, and credit risk cases.

4) Analyzing the risks of capability delivery.

The goal of any system is to deliver some form of capability. Capability delivery risks are related to other risks of the target system, as well as to risks existing in the delivery process.

5) Analyzing the risks of object collaboration.

Security is the isomorph of the target system, the logical collaboration between objects is the foundation of the target system's capabilities and the basis to identify the value concepts. For different value concepts, objects have different types and different observation granularities, and need to be mapped to the corresponding stakeholders and right frameworks for further analysis. The risks of objects in different states and locations need to be fully considered, such as storage state, processing state, and transmission state.

The logic of the collaboration process between the objects is also subject to risks, which will bring risks to some types of value concept.

Object collaboration architecture needs to be mapped onto the target system's framework in order to achieve its basic functions. If the target system's framework does not provide the corresponding risk control or is not trusted, object collaboration architecture needs to implement risk control independently.

6) Analyzing the risks of the target system's framework.

The target system's framework includes organizational framework and technical framework, which is the physical foundation of object collaboration. For example, software is a technical framework component of digital object collaboration. The overall availability and integrity of the target system's framework is the primary consideration for risk analysis. The risks of the various components that constitute the target system's framework need to be considered as risks for another target system.

4.3 Risk Analysis Implementation and Risk Classification

This section adopts the above risk analysis view and combines the new security characteristics of various vertical industries proposed in [2] to carry out risk analysis on the four III ecosystem planes and obtain a risk list (**Table 1**). Due to the complexity of risks, this table only lists some important objects and value related risks.

5 Risk Control

Risk means uncertainty. Finding deterministic attacks and abuse patterns from these uncertainties is a long-term task for the security industry. Risks can be treated by multiple ways after risk evaluations. The trust framework is a positive assumption that exists among stakeholders. Stakeholders can ignore risks and reduce costs based on trust from each other. The more general way to treat risks is to implement risk control for the target system.

From the perspective of trust, the target system's framework, collaboration architecture, and capability delivery of the target system respectively reflect the characteristics of heterogeneous system interconnection and cross-domain collaboration. Risk analysis and control need to focus on the trust boundaries of these interconnections and collaborations.

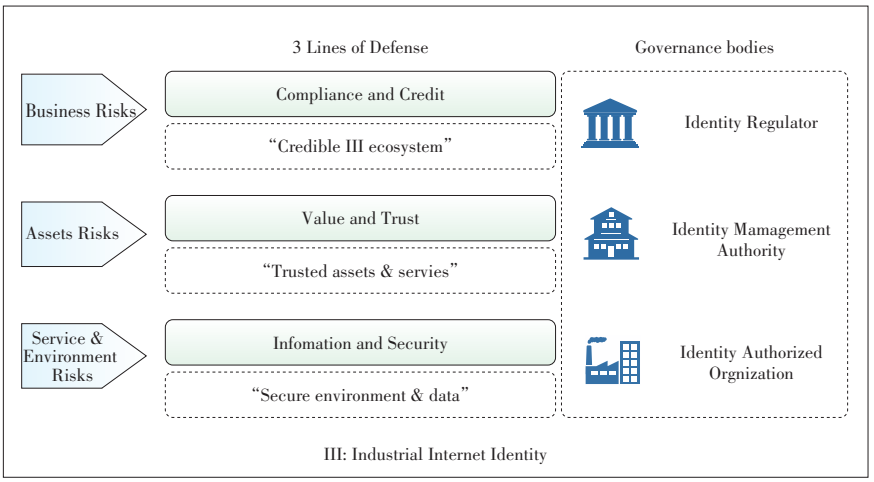
There are different types of risk control such as deterrent, preventative, detective, corrective, and restorative, based on three different dimensions: people, process, and technology. Risk control requires reference to mature standards, imple-

▼**Table 1. Examples of the Industrial Internet Identity (III) risks**

Ecosystem	Right Framework	Stakeholders	Examples of Vulnerability and Risks
Business plane	Credit, Brand Compliance, Contractual, Maturity	Identity regulator (IDR), Identity management authority (IDMA), Identity authorized organization (IDAO)	Lack of penetrating regulatory capacity Inappropriate regulation Falsify/delete/tamper with identity-related date to avoid regulatory responsibility Lack the ability to identity business operations Lack of control over agencies and authorized organizations Emergency response mechanism failed Identity spam Failure to use the Identity for the intended purpose and manner
Asset plane	Identity management service, Identity resolution service, Identity authentication service, Identified asset ownership, Administrator right, Income right, Right to use	IDR, IDMA, IDAO, Identity collaborator	Lack of long-term and continuous identity services operation Insufficient identity service performance and unresponsiveness Interoperability risks Lack of auditing for identity services Insufficient privacy protection for users of identity services Lack of sufficient strength for identity authentication Inadequate protection of ownership and administrative rights of identity, and easy to be misappropriated Improper use of identity and the disposal of income rights are prone to disputes Identity information and services that have been tampered with and redirected Supply chain collusion attack
Service plane	Identity application, Identity data availability, Confidentiality, Integrity	IDAO, Application developer, Partner, Customer, End user	Signaling storm brought by massive III related equipment Reliance on external identity services compromises low latency and high availability
Environment plane	Identity, Identifier, Medium, Device Confidentiality, Integrity, Fault tolerance, Efficiency, Manageability	IDAO, Device vendor, Medium vendor, End user	The identity medium lacks anti-fouling and error correction capabilities The identifier code can be maliciously modified The length and structure of the identifier affect the efficiency of field identification Low-power devices are difficult to achieve high-intensity authentication and encryption for identity related tasks Unmanned environment lacks field maintenance for identity security In an open environment, identity credentials and information can be stolen

mentation and deployment at different stages of the target system's lifecycle, and monitoring and management in accordance with the unified requirements of risk management.

Trust and control are parallel concepts and their relationship is of a supplementary character in generating confidence [7]. Trust can be established or strengthened in the process of continuous collaboration, but the trust relationship and risk control itself will also bring abuse risks to the system. Therefore, the target system needs to fully analyze and dynamically monitor the changes of the three.



▲**Figure 3. Three lines of III credit system.**

6 Building an Identity Credit System with Governance

The III system is an emerging technology system. In the short term, it is short of management and operation experience of ecosystem and also lacks mature governance and assessment standards, which will lead to the absence of admittance and regulation. Participants' capabilities are uneven, which is not conducive to the establishment of an identity credit system and long-term healthy evolution. Therefore, in the early stage of the III ecosystem, it is necessary to clarify governance responsibilities, and build three risk control defense lines with regulation as the core: the identity authorized organization line of defense, the identity management authority line of defense, and the identity regulator line of defense (**Fig. 3**). In the course of continuous operational practice, various incentive mechanisms should be implemented to strengthen the credit of the III system.

The risk governance of the III system should not be limited to the risks associated with the identity business identified in this paper, but should be based on a series of comprehensive organizational governance such as compliance of regulations, corporate governance, IT and information security governance, and field and personnel security governance. III-related risk governance need to be integrated into the basic activities of organizational governance.

Because the governance of the III system is often cross domain and organization, unified standards and specifications will be a very important part.

7 Conclusions

The III system needs to strengthen the awareness of comprehensive risk management. Through the introduction of a systematic risk analysis view, it comprehensively identifies various risk factors and establishes corresponding governance systems and standards. With the continuous enrichment of industrial Internet applications, various new technologies and scenarios including 5G, blockchain, and OLE for Process Control Unified Architecture (OPC UA) plus Time Sensitive Networking (TSN) will continue to emerge, which will pose new challenges to the security of the III system, and simultaneously bring new opportunities.

References

[1] ITU-T. Information Technology—Procedures for the Operation of Object Identifier Registration Authorities: General Procedures and Top Arcs of the International Object Identifier Tree:X.660, Jul. 2011
[2] TANG Kai. New Characteristics and Countermeasures for Vertical Industries Security in 5G [J]. ZTE Technology Journal, 2019, 25(4): 50 – 55. DOI: 10.12142/ZTETJ.201904009
[3] ISO. 2018 Risk Management: ISO/TC 31000 [S]. 2018
[4] ISO/IEC. Information Technology—Security Techniques—Information Security Risk Management: ISO/IEC 27005 [S]. 2018
[5] SHOSTACK A. Threat Modeling: Designing for security [M]. Hoboken, USA: John Wiley&Sons, 2014
[6] BERLIN I. Liberty: Incorporating Four Essays on Liberty [M]. Oxford, UK: Oxford University Press, 2002
[7] DAS T K, TENG B S. Between Trust and Control: Developing Confidence in Partner Cooperation in Alliances [J]. Academy of Management Review, 1998, 23 (3): 491 – 512. DOI: 10.5465/amr.1998.926623

Biography

TANG Kai (tang.kai2@zte.com.cn) is a senior system architect of ZTE Corporation. He is also a member of the Security Technology Expert Committee and Blockchain Technology Expert Committee. He has been engaged in the research, architecture design and R & D management of 3G core network systems and IMS systems, as well as research and project incubation in the Internet of Things identity, blockchain and security. Currently, he focuses on solutions and new technology research in 5G security, the Internet of Things and its applications in vertical industries. He has participated in the writing of a number of Chinese national standards and proposed more than 10 patents of invention.

Security Risk Analysis Model for Identification and Resolution System of Industrial Internet

MA Baoluo, CHEN Wenqu, and CHI Cheng

(Institute of industrial Internet and Internet of Things, China Academy of Information and Communications Technology, Beijing 100191, China)

Abstract: Identification and resolution system of the industrial Internet is the "neural hub" of the industrial Internet for coordination. Catastrophic damage to the whole industrial Internet industry ecology may be caused if the identification and resolution system is attacked. Moreover, it may become a threat to national security. Therefore, security plays an important role in identification and resolution system of the industrial Internet. In this paper, an innovative security risk analysis model is proposed for the first time, which can help control risks from the root at the initial stage of industrial Internet construction, provide guidance for related enterprises in the early design stage of identification and resolution system of the industrial Internet, and promote the healthy and sustainable development of the industrial identification and resolution system.

Keywords: industrial Internet; identification and resolution system; security risk analysis model

DOI: 10.12142/ZTECOM.202001008

http://kns.cnki.net/kcms/detail/34.1294.TN.20200316.1730.006.html, published online March 17, 2020

Manuscript received: 2019-12-01

Citation (IEEE Format): B. L. Ma, W. Q. Chen, and C. Chi, "Security risk analysis model for identification and resolution system of industrial internet," *ZTE Communications*, vol. 18, no. 1, pp. 49 – 54, Mar. 2020. doi: 10.12142/ZTECOM.202001008.

1 Introduction

The security of identification and resolution system of the industrial Internet is one of the keys for securing the industrial Internet. The popularization of industrial identification and resolution may affect production security, social security and even national security. Industrial identification and resolution system is one of the significant parts of industrial internet network architecture, and it is the key to realize the interconnection among equipment, system, data and networks. With the identification and resolution system of the industrial Internet, information can be shared and used across enterprises, industrial sectors and regions; enterprises can vertically and horizontally integrate their global supply chain systems and production systems respectively, to realize intelligent production, personalized customization, important product traceability and product life cycle management. The identification and resolution system is the "neural hub" of the industrial Internet for coordination. Therefore, catastrophic damage to the whole industrial ecology may be introduced or even become a national security threat, if the identification and resolution system is attacked.

2 Concept Design of Security Risk Analysis Model

2.1 Concept Design

Through the analysis of security architecture of the Internet

This work was supported by the 2018 Industrial Internet Innovation and Development Project —— Industrial Internet Identification Resolution System: National Top-Level Node Construction Project (Phase I) .

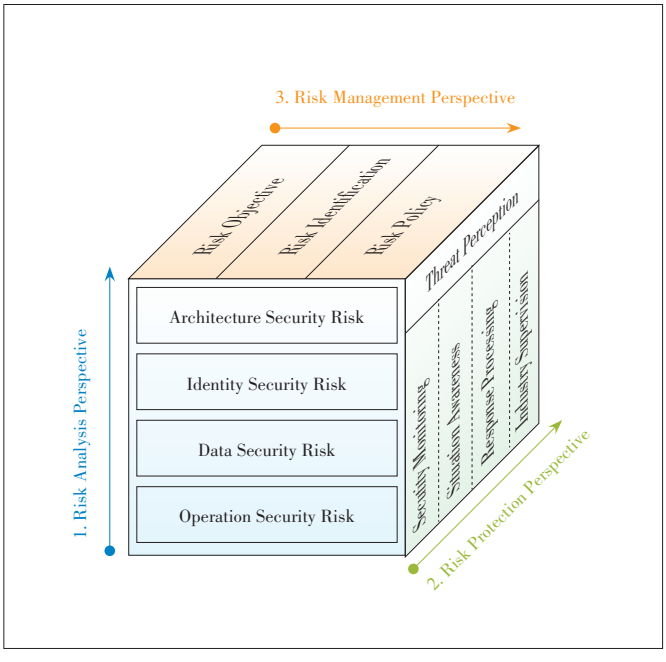
and the industrial Internet abroad [1], an innovative security risk analysis model has been developed combing the characteristic of the industrial identification and resolution system of the industrial Internet, to provide guidance for security construction of the identification and resolution system of industrial internet, help control risks from the root at the initial stage, and improve the security protection capability.

2.2 Overall Architecture of Security Risk Analysis Model

The core of the security risk analysis model are three perspectives: the security risk analysis perspective, the security risk management perspective and the security protection perspective. The key elements in each of the perspectives are outlined in **Fig. 1**.

In the architecture, the security risk analysis perspective includes four key risk analysis elements: the architecture security risk analysis, the identity security risk analysis, the data security risk analysis and the operation security risk analysis. The security risk management perspective includes the security risk objective, the security risk identification and the security risk policy. The security risk protection perspective includes industrial sector supervision, security monitoring, situation awareness, threat perception and response processing.

As shown in Fig. 1, these three perspectives form the basis of the security analysis model. They are relatively independent, while they are intertwined and form an organic architecture of the security risk analysis model for the identification and resolution system of the industrial Internet. The security risk analysis often performs within each of the perspectives to which they belong. However, this is not to imply



▲Figure 1. Overall architecture of the security risk analysis model for identification and resolution system of industrial internet.

that the risk analysis is always to be resolved within each of the perspectives, being separated with that in other perspectives. In the following sections, a detailed illustration will be introduced.

2.2.1 Security Risk Analysis Perspective

The security risk analysis perspective includes the architecture security risk analysis, the identity security risk analysis, the data security risk analysis and the operation security risk analysis, as shown in **Fig. 2**.

The architecture security risk analysis is mainly composed of the node of identification and resolution availability risk, the inter-node collaboration risk and the key node correlation risk.

The identity security risk analysis mainly includes four kinds of risks about people, machines and objects, which are identity deception, unauthorized access, the authority chaos, and the device vulnerabilities [2].

The data security risk analysis [3] mainly focuses on the risk of theft and tampering identity resolution registration data, resolution data and log data, the risk of privacy data disclosure, and the risk of data loss.

The operation security risk analysis includes the risk of personnel management, institutional management and operation process management.

2.2.2 Security Risk Management Perspective

The objective of the security risk management perspective is to provide guidance for constructing a risk management mechanism with the ability to improve the security continuously, illustrated by **Fig. 3**.

In Fig. 3, the risk objective refers to the object of risk assessment and business guarantee of the identification and resolution system of the industrial Internet.

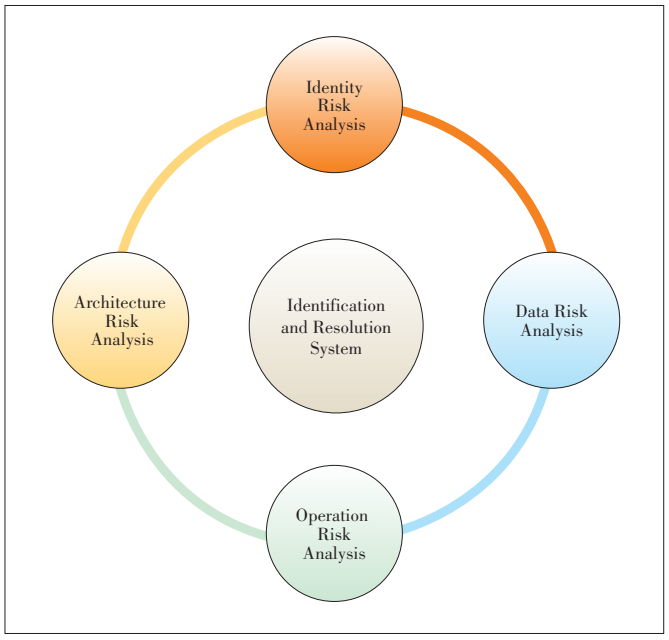
Risk identification refers to possible identified risks that may occur according to the risk objective.

Risk policy provides corresponding security protection strategies according to the existing risks.

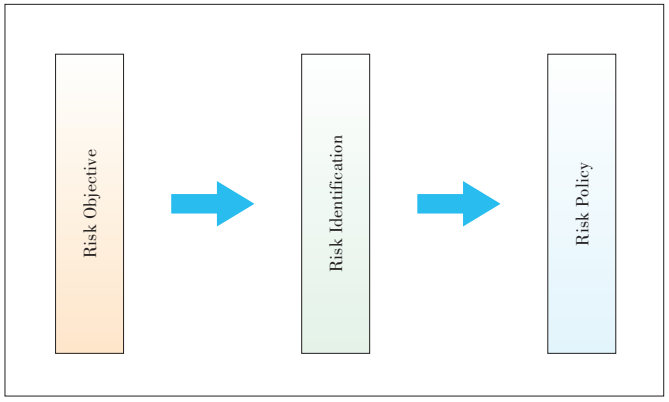
2.2.3 Security Risk Protection Perspective

In view of the various risks faced by the identification and resolution system of the industrial Internet, the security risk protection perspective clarifies the guidance from the whole life cycle and facilitates the risk closed-loop control. **Fig. 4** shows the core of the security risk protection perspective, including five areas: the industrial supervision, the security monitoring, the security situation awareness, the threat perception, and the response processing. The supervision from industrial sectors is centralized in this perspective, which implicates that attention needs to be paid during the construction of the security protection network.

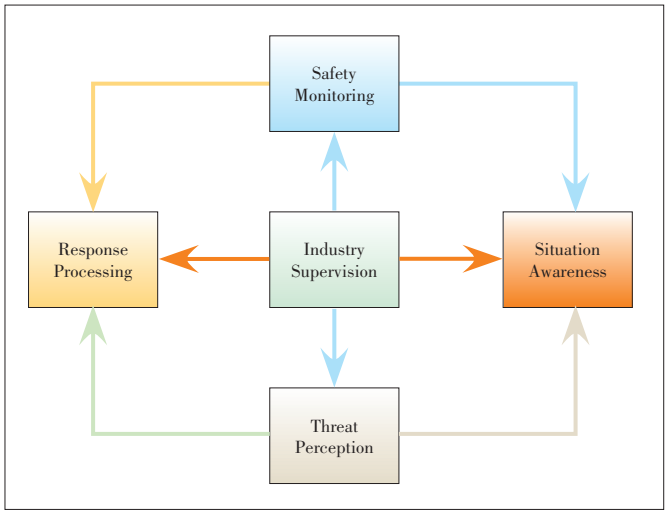
In Fig. 4, the supervision from industry represents the unified leadership and command, in order to establish a joint-action mechanism. The security monitoring aims at four risk



▲Figure 2. Schematic diagram of the security risk analysis perspective.



▲Figure 3. Schematic diagram of the security risk management perspective.



▲Figure 4. Schematic diagram of the security risk protection perspective.

analysis objects above to carry on risk monitoring. The security situation awareness refers to the deployment response and real-time awareness of security risks. The early threat perception addresses the risks found by the situation awareness and issues early warnings. The response processing deals with security risks in time by the establishment of a response mechanism.

3 Proposed Security Risk Analysis Model

3.1 Architecture of Risk Analysis Model

The architecture of the identification and resolution system of the industrial Internet adopts the tree hierarchical architecture (**Fig. 5**); basically, it is a distributed information system. The identification and resolution system of the industrial Internet consists of clients, resolution servers, mirror servers, proxy servers, and cache servers. The security of this architecture depends on the security of each part. A problem arising at any layer of the architecture may affect the security of the whole architecture to some extent [4].

There are many risks in the identification and resolution system of the industrial Internet, such as the risk of node availability, the risk of inter-node collaboration, and the risk of key node correlation.

1) Risk of node availability.

The risk of node availability refers to the risk of availability faced by each node in each layer of the architecture. If one node is attacked, the availability of the node will be threatened, as a consequence, the node function will be failed or inaccessible. To be specific, the main risk of node availability is Distributed Denial of Service (DDoS) attack.

2) Risk of inter-node collaboration.

The risk of inter-node collaboration is an intrinsic risk of identification and resolution system of the industrial Internet. It refers to the risk of delay in the process of data synchronization or replication, which may consequently result in data inconsistency or data integrity problems, when there is a problem in the process of resolution. The risk of inter-node collaboration mainly includes proxy service delay, mirror server delay, and more.

3) Risk of key node correlation.

The risk of key node correlation exists in the failure of key node functions caused by the problems of other key nodes in the identification and resolution system of the industrial Internet, weakening the system's reliability or robustness. The risk of key nodes correlation includes cache breakdown, cache penetration, and attack reflection/magnification.

3.2 Identity Risk Analysis

Identity security is the important entrance of identification and resolution system of the industrial Internet. The user system requires users to authenticate first; obviously, the identity security is of great importance. Different roles, from people,

machines to objects, in the identification and resolution system have different authentication levels, and any risk point can cause authority or trust to be infringed [5].

The main risk points for different identity roles are shown in **Table 1**.

1) Identity deception.

Identity deception can also be called identification defraud in the identification and resolution system of the industrial Internet. The related risk analysis will be conducted in three perspectives: people, machines and objects.

2) Unauthorized access.

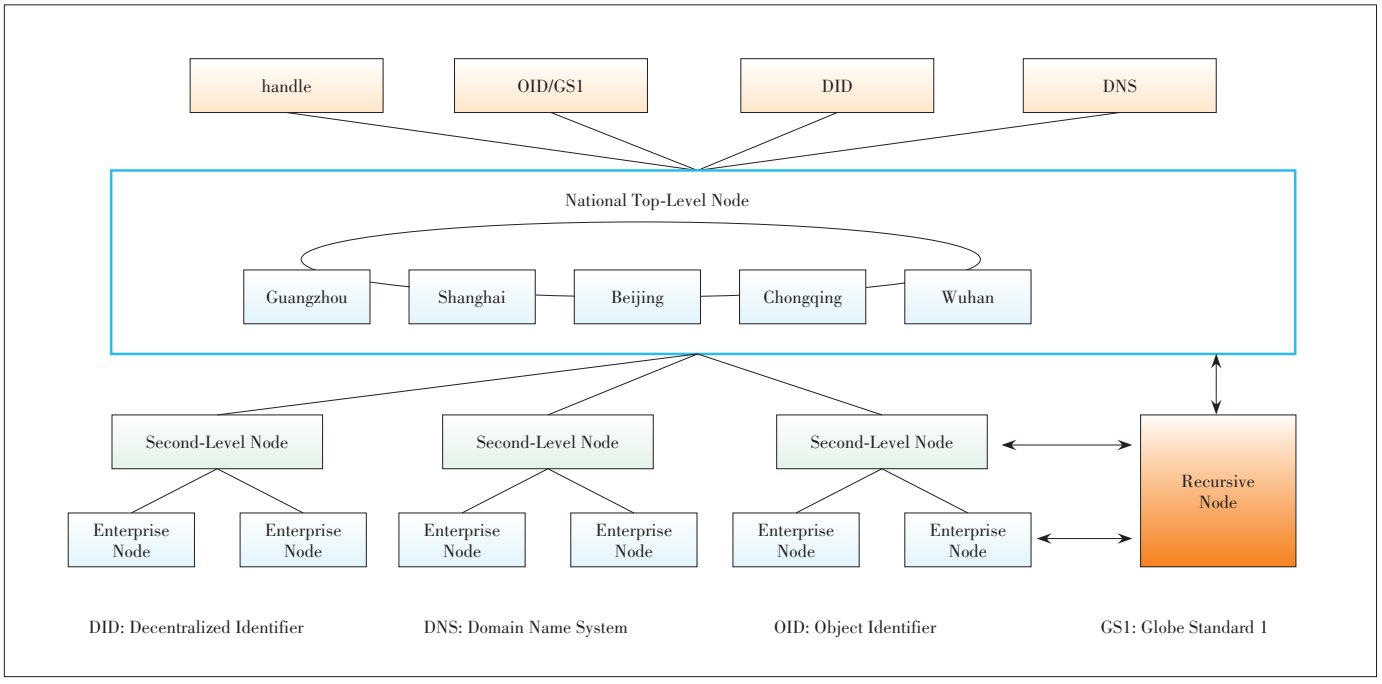
Unauthorized access mainly refers to the ability to access resources that exceed the user's authentication. For example, the identity administrator should only manage the identity function without the function of the ordinary user; if the identity administrator appears to have the function of the ordinary user, this is unauthorized access.

3) Disordered authority.

There are a vast number of devices and people using the identification and resolution service. This gives hackers the chance to enter the system without proper authentication, by means of injection, infiltration, etc., to cross the access management system.

4) Device vulnerabilities.

The servers, clients or terminals in the identification and resolution system of the industrial Internet may have security vulnerabilities or use components with known vulnerabilities. Device vulnerability [6] makes it easier for attackers to pass the set access control policy, get remote control and tamper the device data.



▲**Figure 5. Architecture of identification and resolution system of industrial Internet.**

▼**Table 1. Security risks for identity**

Identity Category	Specific Identity	Risk Points
People	Administrator for identification data	Identity deception; unauthorized access; authority chaos
	User	
	Administrator for identification	
	Third party supervisor	
Machines	International root node	Identity deception; device vulnerability
	National top level node	
	Secondary node	
	Enterprise node	
	Recursive resolution node	
	Industrial client	
Objects	Industrial Internet terminal	Identity deception; false correlation between identification and product; device vulnerability

3.3 Data Risk Analysis

There are three types of data in the identification and resolution system of the industrial Internet, including identification registration data, identification resolution data, and log data. Data security includes three dimensions: data integrity, data confidentiality and data availability. According to GB/T 37988/2019 "Information Security Technology Data Security Capability Maturity Model" [7], identification data security involves data acquisition, data transmission, data storage, data usage, data exchange, and data destruction. Based on the aforementioned, the security risk is mainly composed of the risk of date theft and tampering, the risk of privacy data leakage, and the risk of data loss.

1) Data theft.

The risk of industrial identification resolution data theft is mainly to destroy the confidentiality of data. The data is obtained by unauthorized users, which makes the identification registration data, identification resolution data or log data breach. It may occur in the data acquisition process, data transmission process, data exchange process and data storage process.

2) Data tampering.

When industrial devices are connected to the industrial Internet, attackers have the opportunity to read and modify the data stored in the devices by physical or remote access to the connected devices. There is a risk that the data is maliciously tampered and falsified, which makes the algorithm and processing cracked, leading to the registration data, the resolution data and the log data in the identification system are tampered.

3) Private data leak.

The absence of effective safety protection measures is high likely to cause private data leak of industrial enterprises such as key equipment data, product data, management data, and customer data in the process of using identification and resolution service. The consequence could be significant loss for person and enterprise. In some case, it could even bring incalculable losses to the whole country.

4) Data loss.

In the process of using identification data, if there are no secure protection measures and proper backups, data may be lost due to several reasons. First, illegal operative may maliciously delete the data after obtaining access through attacks on the cache or proxy server. Second, data loss may be caused by the server damage in natural disasters. Last but not least, data loss may be caused by operation mistakes, like unintentionally deleting data. Data loss and failure in recovery of important data such as key equipment data, key product data and user data, could be great losses to industrial enterprises.

3.4 Operational Risk Analysis

Operational risk management plays a vital role in identifying, measuring, supervising, controlling and reporting the operational risk of second-level nodes. With the development of identification ecology, more and more participants involved. The increasingly growth of user number and continual system expanding bring new challenges to the operation of identification and resolution system of the industrial Internet. The internal and external risks will affect the security and controllable operation of the whole identification and resolution system. The operational risks include risks from personnel management, branch management and process management.

1) Risk from personnel management.

The operation of the identification and resolution system of industrial internet requires high reliability and high security. All employees who may affect the operation of identity allocation, identity resolution, business management, data management, etc. (collectively referred to as "personnel") may affect the normal operation of the system. They are referred to as trusted roles. The risk of personnel management includes the risk of role identification, key position role management, personnel operation and personnel control.

2) Risk from branch management.

Branch management risk mainly refers to the life cycle management risk of entities that provide corresponding identification services in the identification and resolution system of the industrial Internet. The risk of branch management mainly includes the authorization risk of branch office, the operation risk of branch office and the risk of service termination of branch office.

3) Risk from process management.

The operation of the identification and resolution system of the industrial Internet involves a series of business processes. The management of business processes is necessary. Otherwise, operators can only use their own experience in their work with great arbitrariness, negatively affecting the system operation and potentially bringing the risk of application process management of secondary nodes.

4 Conclusions

An innovative unified security analysis model for identification and resolution system of the industrial Internet is proposed in this paper, based on the thorough study of the security risk in industrial internet. This is significant for promoting the industrialization of identification and resolution system and corresponding service. First, it helps control risks from the root at the initial stage of identification and resolution system of industrial internet construction. Within this model, the risk points, risk events including their cause and possible consequence, appropriate protection measures, can be identified in early stages. Second, it provides guidance for security construction of the identification and resolution system of industrial internet. Last but not least, it promotes the industrial common view to develop and use the identification and resolution

system of industrial internet healthy and sustainability, to achieve the tremendous economic benefits that the industrial internet offers.

References

[1] DOLEZEL D, MCLEOD A. Managing Security Risk Modeling the Root Causes of Data Breaches [J]. Health Care Manager, 2019, 38(4): 322 – 330. DOI: 10.1097/HCM.0000000000000282
[2] HUANG K, KONG N. Research on Status of DNS Privacy [J]. Computer Engineering and Applications, 2018, 54(9): 28 – 36. DOI: 10.3778/j. issn. 1002-8331.1801-0101
[3] XU K, ZHAO Y D, CHEN W L, et al. Paradigm-Based Routing & Switching System for Data Interception Attacks [J]. 2017, 40 (7): 1649 – 1656. DOI: 10.11897/SP.J.1016.2017.01649
[4] DAI F F, Fan X H, CUI X F, et al. Analysis on Typical Application Architecture Security Risk and Countermeasures of Blockchain [J]. Information and Communications Technologies, 2018, 12(6): 51 – 59
[5] GROTHOFF C, WACHS M, ERMERT M, et al. Toward Secure Name Resolution on the Internet [J]. Computers & Security, 2018, 77: 694 – 708. DOI: 10.1016/j.cose.2018.01.018
[6] ZHENG Y W, WEN H, CHENG K, et al. A Survey of IoT Device Vulnerability Mining Techniques [J]. Journal of Cyber Security, 2019, 4(5): 61 – 73. DOI: 10.19363/J.cnki.cn10-1380/tn
[7] Standardization Administration of the People's Republic of China. Information Security Technology - Data Security Capability Maturity Model: GB/T37988-2019 [S]. 2019

Biographies

MA Baoluo received the B.S. and M.S. degrees in information and communication engineering from Xinjiang University, China in 2013 and 2016 respectively. He is currently a researcher of Institute of industrial Internet and Internet of things, the China Academy of Information and Communications Technology. His research interests mainly include identification and resolution security of industrial Internet and network security. He has published severa papers in various journals and conferences in the field of industrial Internet and network security.

CHEN Wenqu received the Ph.D. degree in mechanical engineering from the University of Sheffield in 2015. She is currently a researcher of Institute of industrial Internet and Internet of things, the China Academy of Information and Communications Technology. Her research interests mainly include identification and resolution of the industrial Internet, digital manufacturing, and digital twin. She has published five papers in various journals and conferences.

CHI Cheng (chicheng@caict.ac.cn) received the B.S. degree in electronic information engineering from Nanjing University of Posts and Telecommunications, China in 2013, and M.S. degree in electronic technology from the University of Sheffield in 2016. He is currently a deputy director of Institute of industrial Internet and Internet of things currently, the China Academy of Information and Communications Technology. His research interests mainly include identification and resolution security of the industrial Internet, as well as industrial Internet architecture. He has published several white papers in the field of the industrial Internet.

Construction and Application of Identifier Resolution in Automotive Industrial Internet

LIN Chengjian[1] and LIU Xinwei[2]

(1. Foton Motor Inc., Beijing 102206, China;
2. School of Electronic and Computer Engineering, Peking University, Shenzhen, Guangdong 518055, China)

Abstract: Identifier resolution system in the automotive industrial Internet is necessary for building a fully interconnected infrastructure with people, machines, factories, products and clients. The resolution system can not only ensure the comprehensive interconnection and efficiency of research and development, procurement, production, sales, and after-sales service in automotive industry, but also promote the integration of automotive industrial data, which facilitates the integrated development of traditional automotive manufacturing and the industrial Internet. This paper focuses on processes and methods of building identifier resolution system for the automotive industry and summarizes the construction and development of secondary node in the automotive industrial Internet in order to explore a suitable road to a rich and completed application ecosystem.

Keywords: industrial Internet; identifier resolution; secondary node; auto industry

DOI: 10.12142/ZTECOM.202001009

http://kns.cnki.net/kcms/detail/34.1294.TN.20200316.1730.008.html, published online March 17, 2020

Manuscript received: 2019-12-18

Citation (IEEE Format): C. J. Lin and X. W. Liu, "Construction and application of identifier resolution in automotive industrial internet," *ZTE Communications*, vol. 18, no. 1, pp. 55–65, Mar. 2020. doi: 10.12142/ZTECOM.202001009.

1 Introduction

Gone through mechanization, electrification and automation, the world's industrial communities now move towards a digital, networked and intelligent era, which promotes the rapid development of the industrial Internet in the automotive industry. With the development of the industrial Internet, it is increasingly urgent to develop flexibility, intelligence and informationization in the automotive industry, where different kinds of resources including equipment, parts, products and customers need to be connected to achieve the integrated development of traditional automotive manufacturing and industrial Internet. The construction of identifier resolution system for the industrial Internet has brought a glimmer of light to the development of the automotive industrial Internet.

At present, the Chinese automotive field is facing major opportunities and challenges. On the one hand, under the great pressure of competing with foreign-invested and joint venture car companies, Chinese car companies are in the dilemma of improving quality and controlling costs, lacking of technical improvement and polices of intellectual property protection. On the other hand, Chinese automotive manufacturing industry must figure out ways of making headway in the blue ocean of the industrial Internet and improving the comprehensive competitiveness of products through new technologies in new areas. For instance, the technology of industrial Internet identifier resolution can facilitate a fully interconnected infrastructure with people, machines, products, factories and customers and achieve the full interconnection of industrial elements

such as research and development, procurement, production, and sales, which improves collaboration efficiency and then promotes both horizontal and vertical integration of automotive industry data. With such technological support, Chinese automotive industry would jump to a new level through optimal integration of industrial resources and leading the technological innovation and product development of the automotive industry based on large-scale on-demand customization, open collaborative manufacturing, intelligent production, and targeted service.

2 Challenges in Automotive Industry Internet

In China, the automotive industry is the country's key industry. Its innovative research based on industrial Internet technologies is important but has been faced with many challenges and the efforts for constructing the automotive industrial Internet need more forward-looking and practicable research and application in the industrial Internet. Three major challenges are discussed as follows.

1) Connection of heterogeneous data.

There are a large number of heterogeneous data in the automotive industry, which lack unified standard and have insufficient identifiers and limited data collection. A standard system for multiple protocols is therefore needed to achieve interconnection and interoperability of industrial data. A resolution node in identifier resolution system is used as a link to obtain heterogeneous industry data and translate multi-format identifier data to gain complete data in the industry [6].

2) Optimal allocation of identifier resources.

There are lots of identifier resources in automotive resource information, from product development design to purchase, assembling and after-sales service. In order to connect the whole industry chain, identifier resources need to be processed, analyzed and fed back to industrial manufacturing enterprises. However, it is very difficult to integrate and manage these fragment resources, and the application costs will increase as well. An identifier resolution system for automotive industry which can optimize the allocation of resources by creating the query entry and allocation entry of the automotive Industry Internet.

3) Coordinated development of industrial ecosystem.

The development of the industrial Internet will trigger major reforms in the automotive manufacturing industry and related industries, and as a result, new requirements for the development of the automotive industry will be raised as well. However, as the development of the automotive industry's industrial Internet has just begun, uncertainties and lack of motivation make the industrial ecological development imperfect. The construction of the identifier resolution system will effectively link Chinese next-generation industrial Internet development plan with the scientific and technological innovation plan. It will find the suitable scenarios for industrial Internet operations and services and explore the appropriate development paths of industrial Internet technology for China to speed up future automotive manufacturing and regional economic development.

3 Overview of Identifier Resolution

Used to identify different objects, entities, and industrial Internet objects, the identifier, a character string, can be composed of numbers, letters, symbols and characters with certain rules. The identifier resolution in the traditional Internet translates the domain name identity into an IP address, while in the industrial Internet it translates the physical or virtual digital object identity into object address, and adds a process of querying the association information of item [5]. There are two changes in the industrial Internet identifier resolution technology: first, the granularity is refined from the host to resources such as goods, information and services; second, the function of supporting intelligent association of different hosts, different places and heterogeneous information is set [6].

Similar to the domain name in the Internet, which gives the target object an Identification Code (ID) that can recognize and manage the resources by switching identifier between the physical world and the network world freely, the industrial Internet identifier of the automotive industry is a key resource for identifying and managing complete vehicles, parts and equipment. The resolution of the identifier in automotive industrial Internet gives the ability of looking up the server address, which stores product information through the product's unique ID, or looking up the information and related services of product. Therefore, the resolution of the identifier in automotive industrial Internet is an important basis for realizing the revolution of connecting services and the automotive industrial Internet.

4 Identifier Resolution System in the Automotive Industrial Internet

The identifier resolution system is an important part of the architecture of automotive industrial Internet, as well as a neural hub that supports the interconnection in the industrial Internet. Foton Motor is constructing a secondary node for the identifier resolution system in the industrial Internet and divides the process of identifier resolution into eight steps: 1) identification of identifier objects, 2) formulation of identifier codes, 3) selection of identifier terminals, 4) maintenance of identifier data, 5) assurance of the identifier security, 6) construction of identifier resolution in the secondary node, 7) compilation of the standard identifier resolution system, and 8) development of identifier-based application software.

4.1 Identification of Identifier Objects

The automotive industrial Internet identifiers cover all aspects of the automotive industry value chain. Foton Motor

mainly uses vehicles, parts, organizations and equipment as the major ingredients to construct an identifier resolution system in combination with the condition of Chinese automotive industry management and related standards.

1) Vehicle identifiers.

Vehicle identifiers are mainly related to vehicle research and development, production, sales and maintenance. It includes vehicle model identifiers, vehicle announcement identifiers, Vehicle Identification Number (VIN) identifiers, vehicle configuration list identifiers, vehicle production order identifiers, sales order identifiers, vehicle maintenance order identifiers, and so on.

2) Parts identifiers.

The identifiers of parts are generated through production and maintenance, including parts classification identifiers, single/batch parts identifiers, parts purchase order identifiers, parts production order identifiers, parts logistics order identifiers, parts storage order identifiers, and parts maintenance order identifiers.

3) Equipment category identifiers.

The equipment category identifiers are mainly needed during production, transportation and sales in the automotive industry. They are equipment classification identifiers, equipment identifiers, equipment failure identifiers, equipment function identifiers, and equipment location identifiers.

4) Institution identifiers.

Institution identifiers refer to various types of objects in the ecological value chain of the automotive industry. Generally speaking, institution identifiers include company vehicle manufacturing identifiers, company component manufacturing identifiers, sales enterprise identifiers, and company aftermarket service identifiers. In enterprises, institution identifiers also denote factory identifiers, workshop identifiers, and internal management department identifiers.

5) Quality category identifiers.

Quality category identifiers express the standards and grades of products inspected by the automotive industry, including product inspection standard identifiers, quality grade identifiers, defect cause identifiers, and defect level identifiers.

4.2 Encoding of Identifiers

Encoding is a basic technical means for people to unify their views and exchange information, which improves the efficiency of information processing. Identifier encoding is a technology for defining, assigning and managing the data structure of the encoding format of industrial Internet identity objects. At present, the mainstream encoding technologies include Globe Standard 1 (GS1), Electronic Product Code (EPC), Handle, Object Identifier (OID), Entity Code for Internet of Thing (Ecode), and more [6].

The encoded automotive industrial Internet identifier consists of a prefix and a suffix [4]. The primary and secondary nodes assign the prefix, and the suffix is mainly composed of an application identifier and a unique code. The application identifier is used to distinguish between different identification objects in the automotive industrial Internet. **Table 1** is an example of encoded identifiers from the identifiers resolution system of Foton Moter, where (V) represents the vehicle identifier and (91) denotes the identifier of automotive.

4.3 Selection of Identifier Terminals

The selection of identifier terminals includes the selection of carrying methods and carriers. Existing carriers generally include bar codes, Quick Response (QR) Codes, Radio Frequency Identification (RFID) tags and sensors [5]. The carrying methods generally include nameplates, tags, labels, laser etching and mechanical stamping.

Automotive industry prefers direct marking of identifiers at present. A label and list are used when direct marking is not suitable. If the methods mentioned before do not work well, external packing can come in handy. Thanks to the development of QR code, the automotive industrial Internet identifier terminals currently adopt engraving with QR code and bar code. Laser etching used on key components can be long-term identifiable. RFID is valued in the automotive industry with the development of the industrial Internet.

4.4 Management of Identifier Data

Identifier data is the key parameter information expressed by an identifier object. There are a large number of Original Equipment Manufacturers (OEMs), component manufacturers, distributors and service providers in the automotive industrial Internet, and all of them have their own identifier data based on their data standards. On the one hand, the owner of each identifier needs to register key information in the identifier resolution system that has the function of registration, review and update in order to enable other people to query data. On the other hand, the identifier data need to integrate with heterogeneous industrial Internet application system data due to the diversity of identifier data environment. It is necessary to map identifier data to various types and maintain them in order to strengthen the interoperability of industrial Internet resources in the automotive industry and facilitate the search and discovery of industrial Internet resources between different industrial Internet systems.

4.5 Security of Identifiers

The industrial Internet identifier resolution system is an important network infrastructure of the automotive industrial In-

▼**Table 1. An example of identifier encoding**

Prefix	Separator	Application Identifier	Unique Code
88.107.00001	/	(V)	LRDXXXXXXXXXXXXX
88.107.00001	/	(91)	XXXXXXXX

ternet. The identifier data are important information generated during the production and operation of an enterprise, which need to be protected carefully since it may involve the company's trade secrets and core assets. It is necessary to display different information according to the users' levels and support the secure channel function to prevent sensitive information from interception during the construction of the identifier resolution system.

The construction of the industrial Internet identifier resolution system in the automotive industry is separated into three fields at the security level;

· The software filed security. The rationality of the software architecture and the completeness of relevant protocols are all issues for overall consideration of identifier security;

· The data filed security. It includes security guarantees for the exchange storage of massive data, optimized aggregation management of multi-source heterogeneous data and countermeasures against illegal data use;

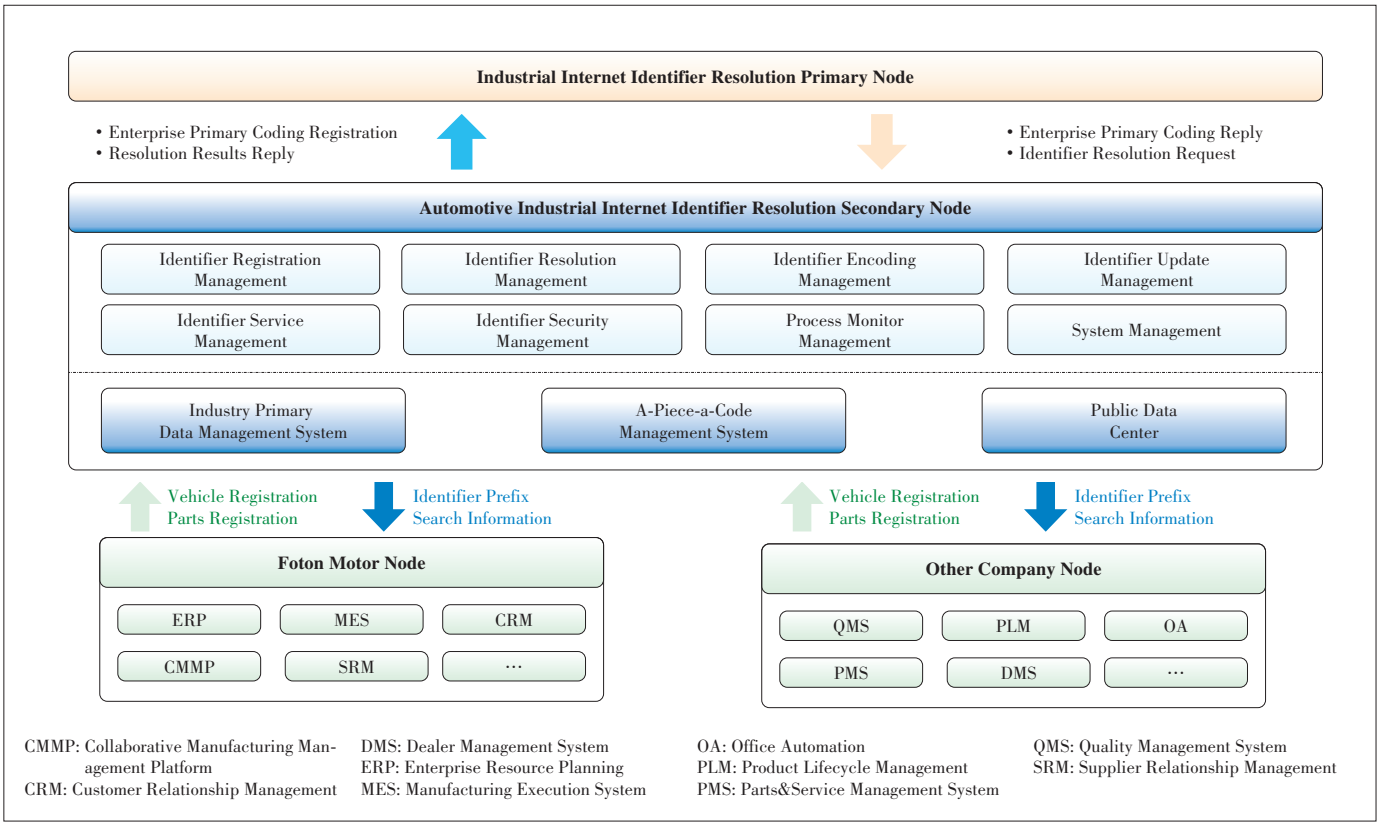
· The operation field security. It would avoid misuse of registration and illegal registration, allocate reasonable identification resources and improve the security of environment for identification management.

4.6 Construction of Secondary Node

The identifier resolution system in automotive industrial Internet secondary node is the core system that implements the registration, query and resolution of identifiers by various application subjects in the automotive industry. Foton Motor has taken the lead in constructing a secondary node for the resolution of the automotive industrial Internet in China. The resolution system supports the registration and resolution of physical resources such as vehicles, equipment and parts, as well as virtual resources such as algorithms and processes. As an industry public service platform, the identifier resolution secondary node in the industrial Internet is linked up to the national primary nodes, which can query the network location of secondary nodes and linked down to the local data or local resolution system of each company in the automotive industry value chain, which can query the enterprise data storage location from the secondary node [1].

The construction of identifier resolution in secondary nodes faces a large number of different hosts, different places and heterogeneous systems due to the complexity and diversity of the industrial Internet environment. The simple resolution of storage location can no longer meet the increasingly sophisticated requirements for industrial Internet data in automotive industry. Therefore, Foton Motor builds the identifier resolution system of secondary node based on the industry master data system, the a-piece-a-code system and a public data center, as shown in **Fig. 1**.

The industry master data system, as a data standard management system, will unify the classification and description



▲**Figure 1. Integration diagram of a secondary node in automotive Industrial Internet identifier resolution.**

of vehicles, parts and accessories in the automotive industry, or solve the problem of "same things with different names" among different enterprises through mapping of backend data. An a-piece-a-code system is used for the unique code management of single piece or single batch in the industry, providing the entire network with unique codes for the entire vehicle and parts. The public data center serves as a shared data storage center that stores the core data registered in secondary node by enterprises so that it can support association and mapping of identifiers. The secondary node built on this basis can analyze the network storage location and associated information of the same identity object. It can provide data support for the development of new business forms and new ecology in the automotive industry as well.

4.7 Standard of Identifier Resolution System

At present, the mainstream identification standard systems include Handle, OID , Ecode, EPC and so on. These systems are used to uniquely mark item objects and digital objects at the first time and provide information query for them. Now they have developed into a low-level information architecture, similar to Domain Name System (DNS) in the Internet [4].

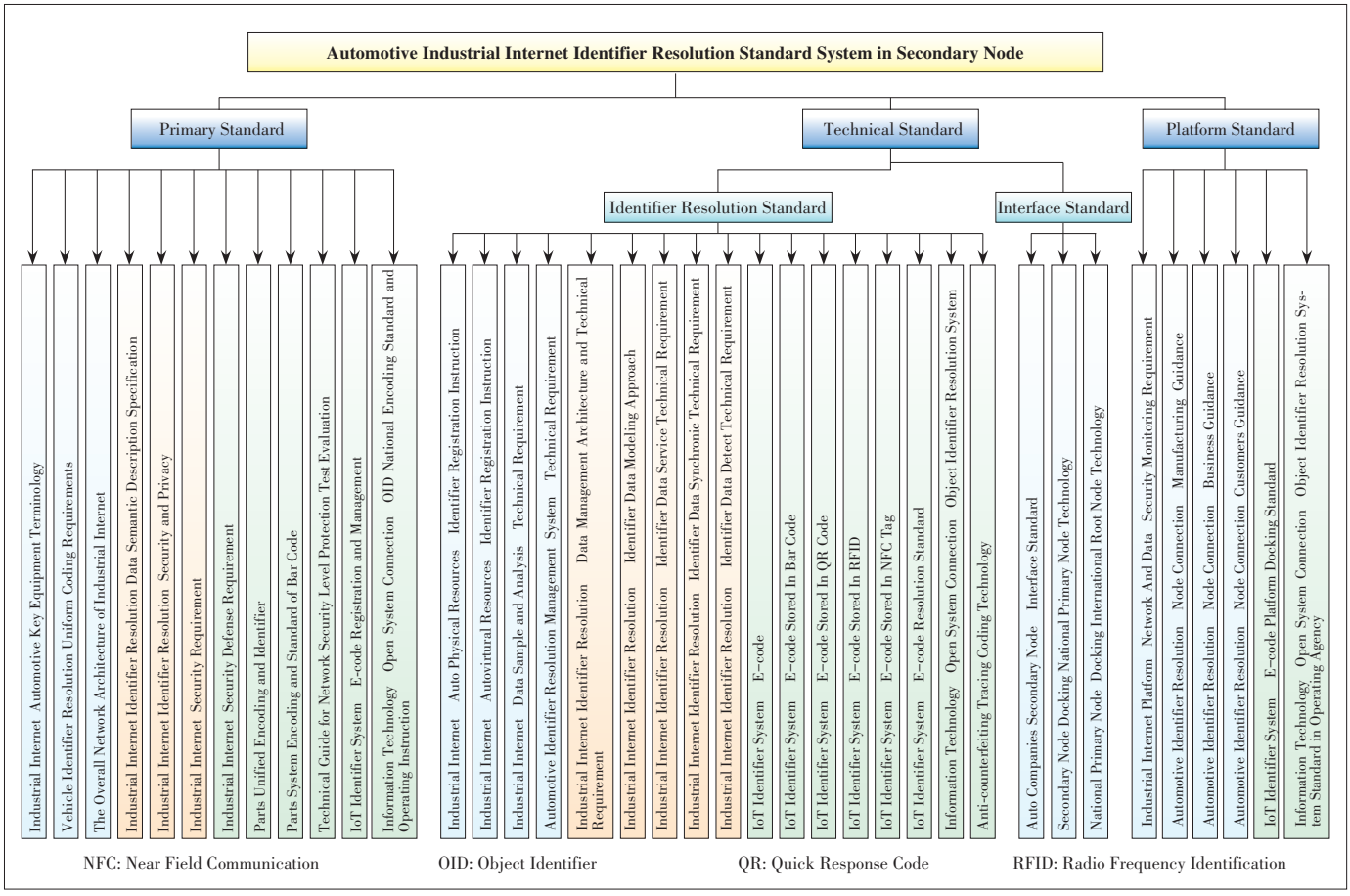
The demands in automotive industry have been fully considered and the research results in other industries have been drawn on while constructing the identifiers resolution standard system in automotive industrial Internet. The resolution system takes technology standards as the main line, identifiers and resolution the core. At present, it is initially composed of three parts: basic standards, technical standards and platform standards, as shown in **Fig. 2**.

1) Primary standards.

The basic standards mainly define automotive production lines, electrical and safety equipment, coding principles, data structures and symbolic representation methods for vehicles, parts and accessories. The standards can achieve data integration across enterprises and regions and provide standard coding rules for OEMs, component manufacturers and distributors.

2) Technical standards.

The technical standards mainly cover three parts. The first is to standardize the registration and resolution principles of identifiers in physical resources including complete vehicles, equipment, parts and components, and in virtual resources including algorithms and processes. Secondly, the technical requirements of the sources of automotive industrial Internet identification data, resolution methods and storage specifica-



▲**Figure 2. Standards for automotive Industrial Internet identifier resolution system.**

tion are standardized. Thirdly, the interface technical requirements are standardized, including data transmission methods and interface methods, to ensure the intelligence, feasibility, advancement and reliability of multi-platform interconnection after the platform is connected.

3) Platform standards.

The platform standards mainly specify the technique for network data security monitoring and privacy protection of the industrial Internet in automotive industry. Operating guidelines are also standardized for OEMs, component manufacturers, dealers and other participants in the construction of the identifiers resolution in industrial Internet.

4.8 Applications Based on Identifiers

The development of the industrial Internet identifier resolution in the automotive industry cannot be separated from the application and promotion of the industry. In the process of constructing the secondary node, Foton Motor focuses on the development of application systems based on the characteristics of the automotive industry such as logo engraving, logo collection and logo query, which provides strong support for the industrial innovation of the automotive industrial Internet.

The development of identifier-based applications and its industrial ecology have gradually improved with the development of industrial Internet applications. In addition, software engineering can get more abundant application scenarios and promote the development of other related software with the development of software ecosystems such as dedicated encoding and decoding software, decoding query software with product information, general coding query software and social and e-commerce portal coding query software.

5 Exploration of Identifier Applications

The construction of the industrial Internet identifier resolution system in the automotive industry is an important basis for the application of the automotive industrial Internet. On the one hand, an identifier database for products, parts and accessories in the automotive industry is established based on the automotive industrial Internet identifier resolution standards, and used as the entrance to the Internet identification query of automotive industry. On the other hand, the entrance to the industrial Internet resource management of the automotive industry is established through the implementation of the new technologies and key equipment in industrial Internet and IT. The big data service platform in automotive industry is established based on the entrance that covers national automotive manufacturers, suppliers, service providers, dealers, customers and other industry agencies.

Foton Motor sets a goal of connecting the internal resources and external services of automotive companies to create higher value for OEMs, suppliers and customers while exploring the development of industrial Internet applications. Foton Motor uses the industrial Internet identifier resolution platform as the basis to open up all aspects of resources in the commercial vehicle industry chain and the value chain of OEMs, in order to build a complete industrial Internet service system for the automotive industry. Foton Motor actively carries out explorations and applications in supply chain coordination, quality traceability, accurate service and other aspects, as shown in **Fig. 3**.

5.1 Supply Chain Collaboration Based on Identifiers

Collaborative management of the supply chain is an interconnected ecosystem covering the entire value chain of planning, procurement, supply, logistics, warehousing, quality, transportation, sales and service. Network storage location codes are assigned to the entire vehicle, parts, suppliers, equipment and tooling equipment with the help of the identifier resolution platform in automotive industrial Internet. In order to build a good basic environment for supply chain collaboration, the location codes are combined with their own unique codes in their respective systems to ensure that each participating interconnected data has unique identification information.

Taking customer needs as the starting point and based on a unified identifier resolution service, companies link physical objects such as complete vehicles, production parts and spare parts in the supply chain in implementation. Companies also exam the weak points of supply chain management in order to build a collaborative and efficient supply chain collaborative management system.

In the supply chain collaborative application scenario in automotive industry, the specific application process of using identifier resolution are as follows (**Fig. 4**):

• Step 1: The identifier of a collaborative resource is encoded.

• Step 2: The above resource is registered in the identifier resolution system.

• Step 3: In the product design phase, the R&D department designs products based on the same identifier.

• Step 4: The procurement department's design requirements for R&D are communicated to the supplier in time.

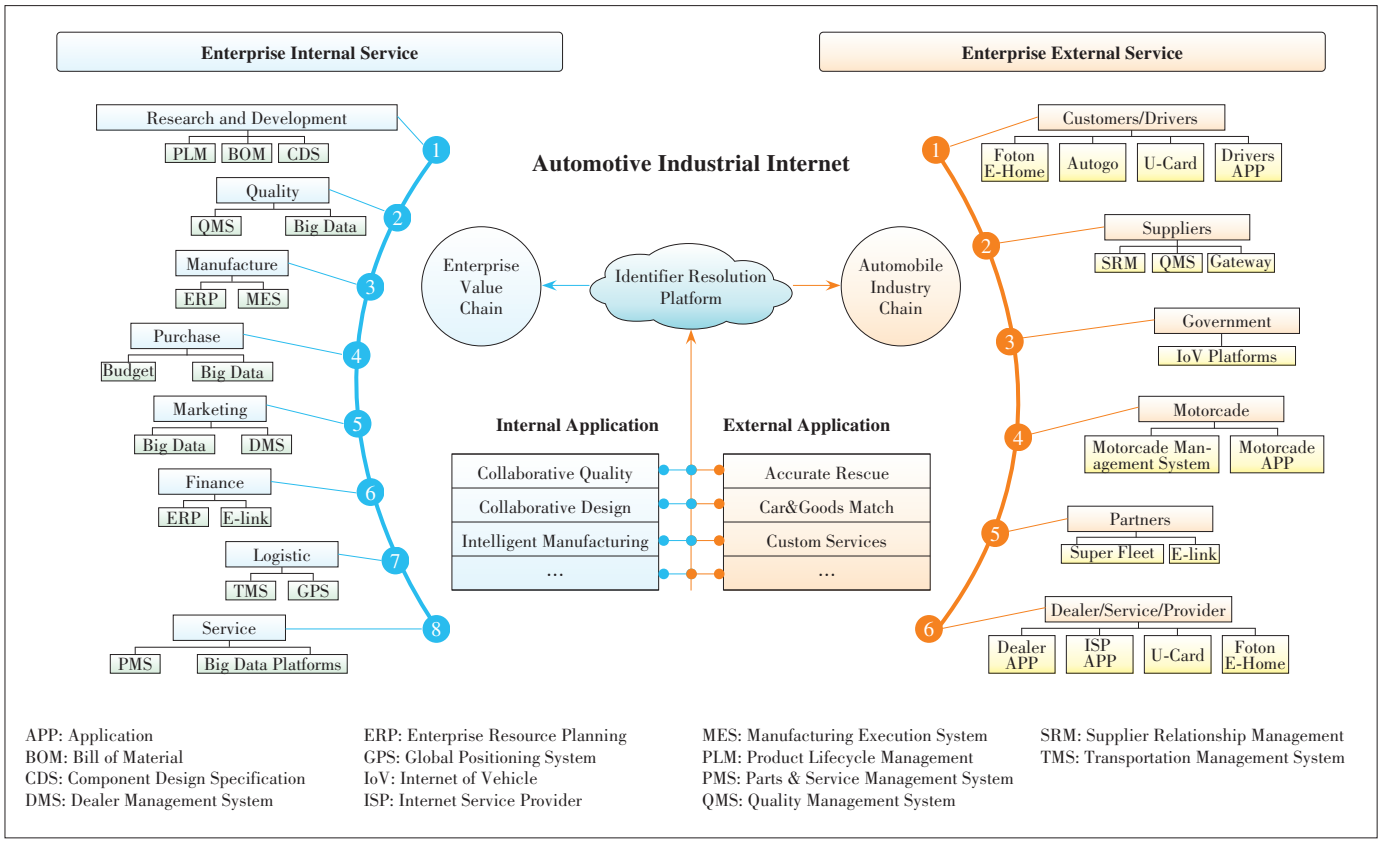
• Step 5: The supplier obtains the R&D requirements based on the unified identifiers and promptly gives feedback.

• Step 6: The logistics company gives timely feedback about the logistics status of the product based on the unified identifiers.

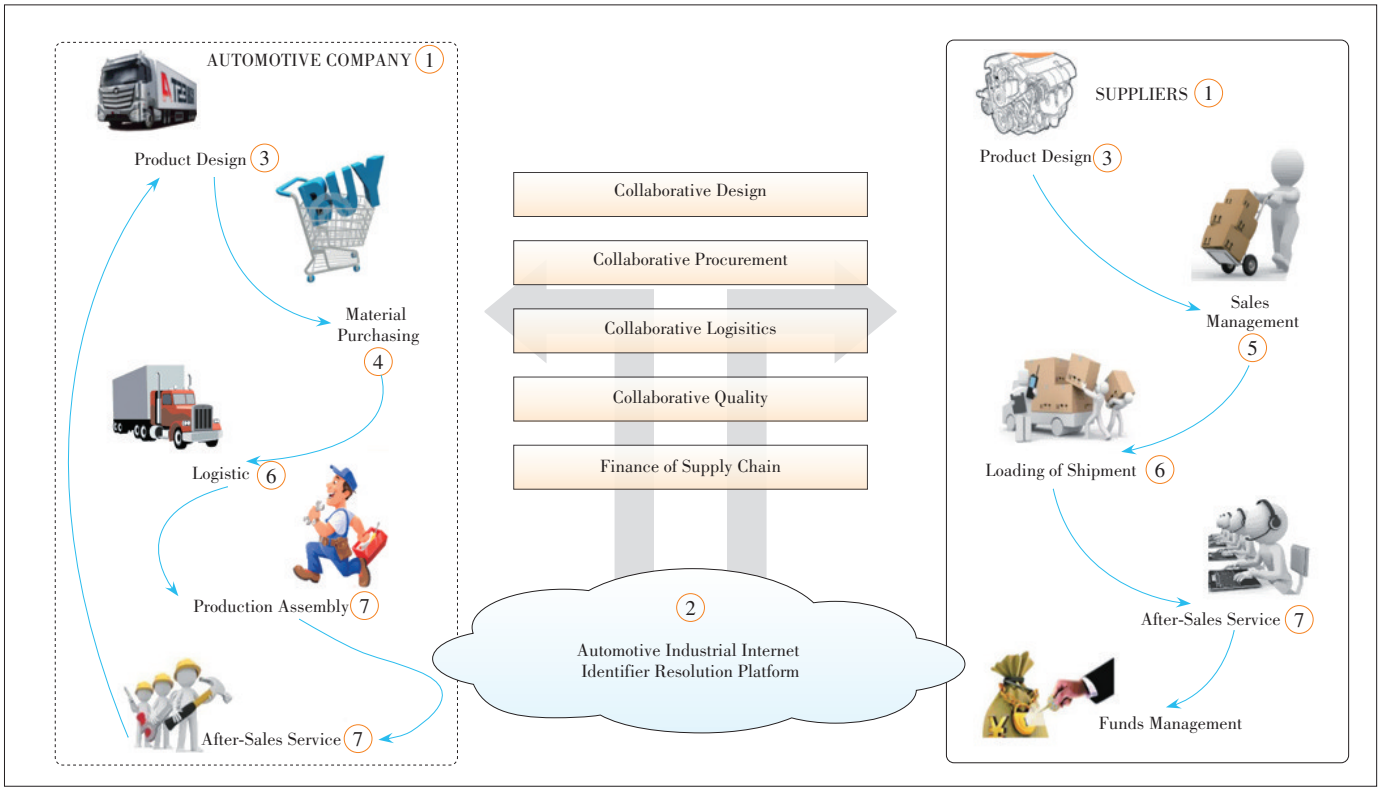
• Step 7: Based on the unified identifiers, the quality department reports the quality inspection information to the R&D department and suppliers.

Compared with traditional supply chain management, the supply chain management based on identifier resolution is improved in the following five areas.

The collaborative design shortens the development cycle. Through the identifier resolution technology, the research and development resources are fully shared in the industrial Inter-



▲Figure 3. Explorations on the innovative applications of the automotive industrial Internet identifier.



▲Figure 4. Supply chain collaboration based on identifier resolution.

net field and it becomes possible for suppliers and dealers to participate in the design and evaluation of vehicle products. The synchronous and collaborative development situation are formed and the development cycle is shorter.

The collaborative procurement lowers the risk of material shortage. Through the industrial Internet identifier resolution technology, OEMs and suppliers can obtain real-time dynamic information of customer orders, inventory levels and purchase orders, which will reduce the risk of material shortage.

The logistics collaboration reduces logistics costs. OEMs and supplier can obtain the logistics information if the vehicle logistics information and cargo information are registered in the identifier resolution system in time. The vehicle efficiency will improve and transportation cost will reduce due to the collection of the cargo flow.

The quality collaboration improves supplier capabilities. Service providers and customers can register the collected quality problems in the identifier resolution system while using the vehicle, and then suppliers can obtain quality feedback in time and optimize the design and improve the quality of supplier parts.

The finance of the supply chain. The identifier resolution technology can obtain the real-time location and maintenance information of the vehicle combined with the Internet of Vehicle that provides financial guarantees for partners and expands the business of assistant partners.

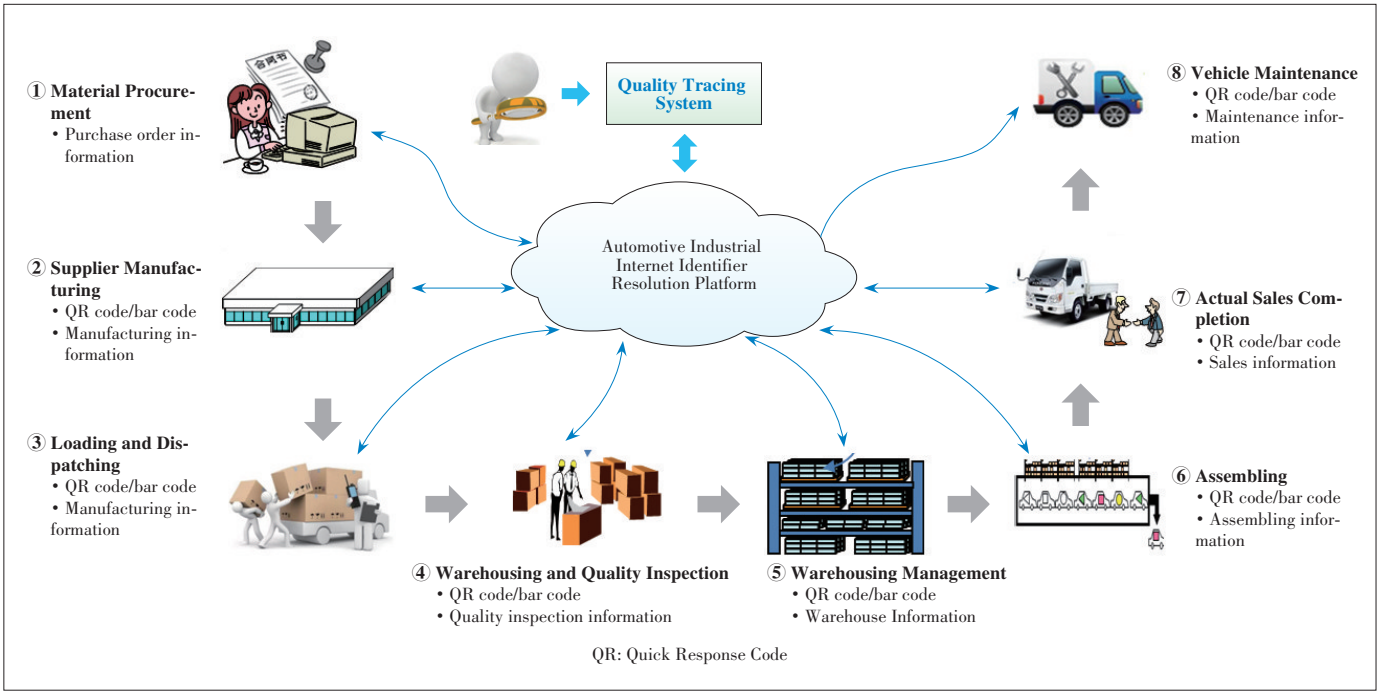
5.2 Quality Traceability Based on Identifier Resolution

With the help of the automotive industrial Internet identifier resolution standard and the application platform, a quality traceability coding standard that complies with the automotive industry standards is established. It makes coding rules of raw materials, semi-finished products and finished products traceable. On the one hand, automotive companies use the same traceability code rules to implement quality traceability management in order to improve the readability of the code and reduce the cost pressure of parts traceability on the automotive industry supply chain. On the other hand, the resolution system collects quality data for the entire life cycle of core components from manufacturing, transportation, quality inspection, storage, assembly of complete vehicles, terminal sales, maintenance services, replacement, and retirement to recycling, so that the product quality of companies can be optimized and improved [2].

The quality traceability of key components in the automotive industry needs to accurately record the correspondence between the vehicle and the components during the assembly process of vehicles. Besides, it should accurately record the information of vehicle dealers and customers during the vehicle sales process and the replacement of parts in the after-sales service. The vehicle manufacturer can quickly determine which vehicles the problematic parts are installed on, which areas these vehicles are sent to and which end users are sold to through this way. If end users need to repair or replace parts, they can know where the nearest service outlet is.

In the application scenario of quality tracing of automotive key components, the specific application process of using identifier resolution is as follows (**Fig. 5**):

• Step 1: Suppliers encode the key components of the car with QR code, bar code or RFID and register them in the iden-



▲**Figure 5. Quality tracing based on identifier resolution.**

tifier resolution system.

• Step 2: According to the coding identifier, the OEM records product information such as storage, quality inspection, warehousing and assembling and registers related information in the identifier resolution system.

• Step 3: The OEM marks the entire vehicle with an identifier, then records the correspondence between the vehicle and the components, and finally registers the vehicle identifier in the identifier resolution system.

• Step 4: When the vehicle is sold to the customer, the dealer binds the customer's information (name, age, occupation, purpose, etc.) with the vehicle information and registers the information in the identifier resolution system.

• Step 5: The service provider obtains the production, logistics, quality inspection and other information of the parts and records the replacement information of the old and new parts by scanning the QR code of the parts during the maintenance.

5.3 Intelligent Production Based on Identifier Resolution

Customer needs, product resources, production materials, logistics transportation and other information related to production are registered for the identifier resolution system in the manufacturing process in the industrial Internet ecology of the automotive industry in order to lay the foundation of intelligent production. The process mainly includes the following steps (**Fig. 6**):

• Step 1: Registration of customer identifier order. Customers complete product customization in the Dealer Management System (DMS) and get an order number, then the system automatically registers the order information in the identifier resolution system.

• Step 2: The product design department obtains the information about the specific model and configuration involved in the order according to the order identifier and registers the designed product Bill of Material (BOM), parts and other identifier to the identifier resolution system.

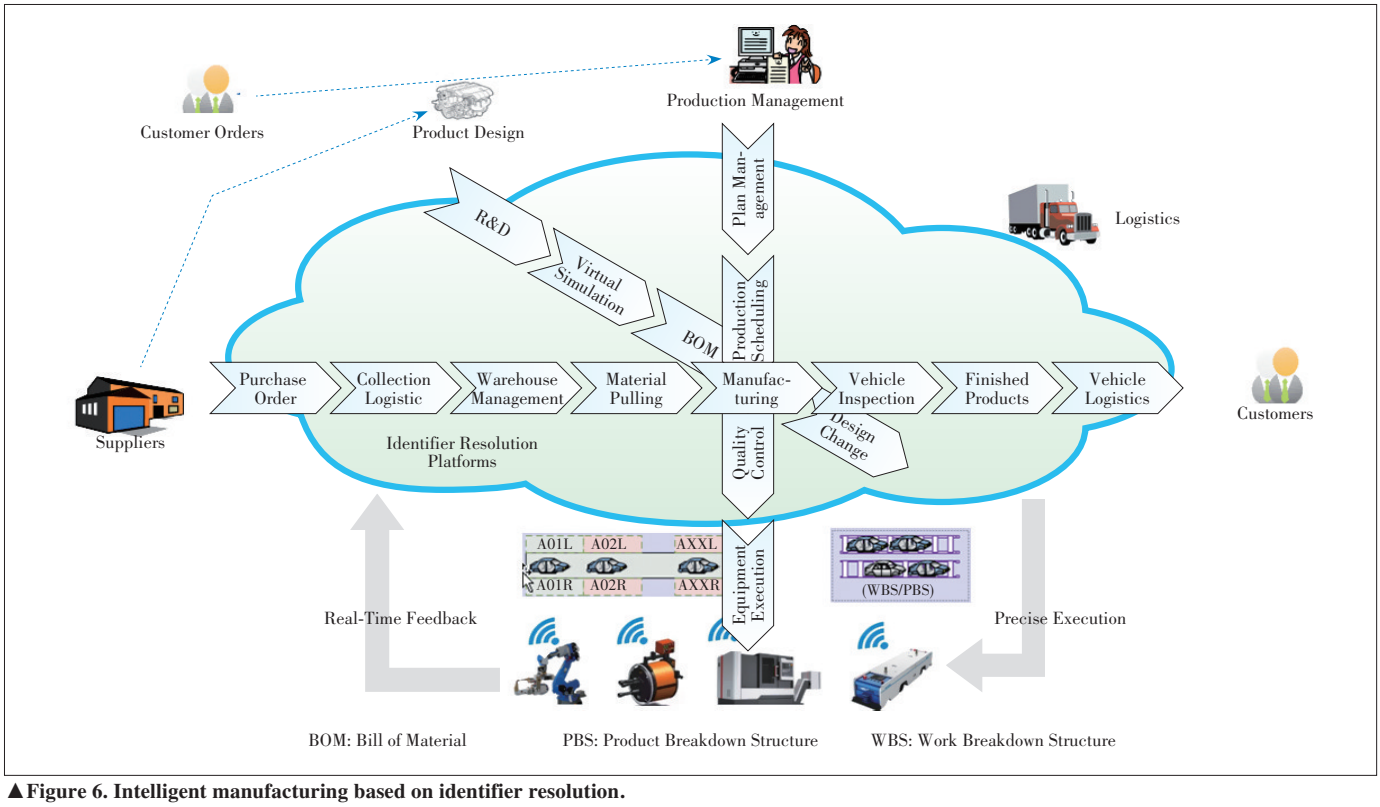
• Step 3: Purchasing and production management departments formulate purchase requisitions, production orders and production plans and register the purchase order and production plan information in the identifier resolution system.

• Step 4: The supplier obtains the material specific information and order date required by the purchase order through the identifier resolution system and then starts the production order.

• Step 5: The logistics company obtains information such as the specific delivery date and quantity of parts according to the production order identifier and purchase order identifier and transports the materials to the warehouse where the production is located.

• Step 6: According to the order identifier, material identifier and equipment identifier, the production department obtains the resource information required by customers and production and translates it into job instructions to guide the equipment to execute accurately. At the same time, the equipment reports the processing results in time, and the execution result is registered in the identifier resolution system.

• Step 7: Through the identifier resolution system, custom-



▲**Figure 6. Intelligent manufacturing based on identifier resolution.**

ers can get the specific production process of their customized products in time.

5.4 Service Innovation Based on Identifier Resolution

An intelligent service system based on the industrial Internet identifier resolution system is established by creating an intelligent and differentiated customer service system. It can promote information interconnection between the product end and the client and upgrade the traditional after-sales service to active services, remote online services and intelligent services [3].

In the traditional vehicle after-sales service, the vehicle's operating status data cannot be grasped immediately. The service engineer cannot get the fault information at the first time when the vehicle has a problem, and can only diagnose and maintain on the spot. This situation makes the vehicle service passive. The vehicle production data, product data and customer data are registered in the industrial Internet identifier resolution system based on the industrial Internet big data platform, which can grasp the running status of the vehicle at any time, predict the possible faults of the vehicle and timely detect the damaged parts of the vehicle for customers. Fault reminders, maintenance reminders and driving behavior guidance can be provided through this, as shown in **Fig. 7**.

1) Fault reminder.

We can connect vehicle production and assembly data, customer sales data and real-time data during product operation through the industrial Internet identifier resolution system and then establish a big data analysis model to monitor the performance indicators and damage levels of key vehicle components effectively. Besides, we can use short messaging service (SMS), applications (APP) and cars to push message reminders automatically and communicate with customers on the phone in time according to the fault level. If a customer raises a problem, we should ask him if there is a problem with the vehicle on the phone and immediately send related staff to solve the problem so that the expansion of the fault will avoid and it makes the vehicle operation economic and safety.

2) Maintenance reminder.

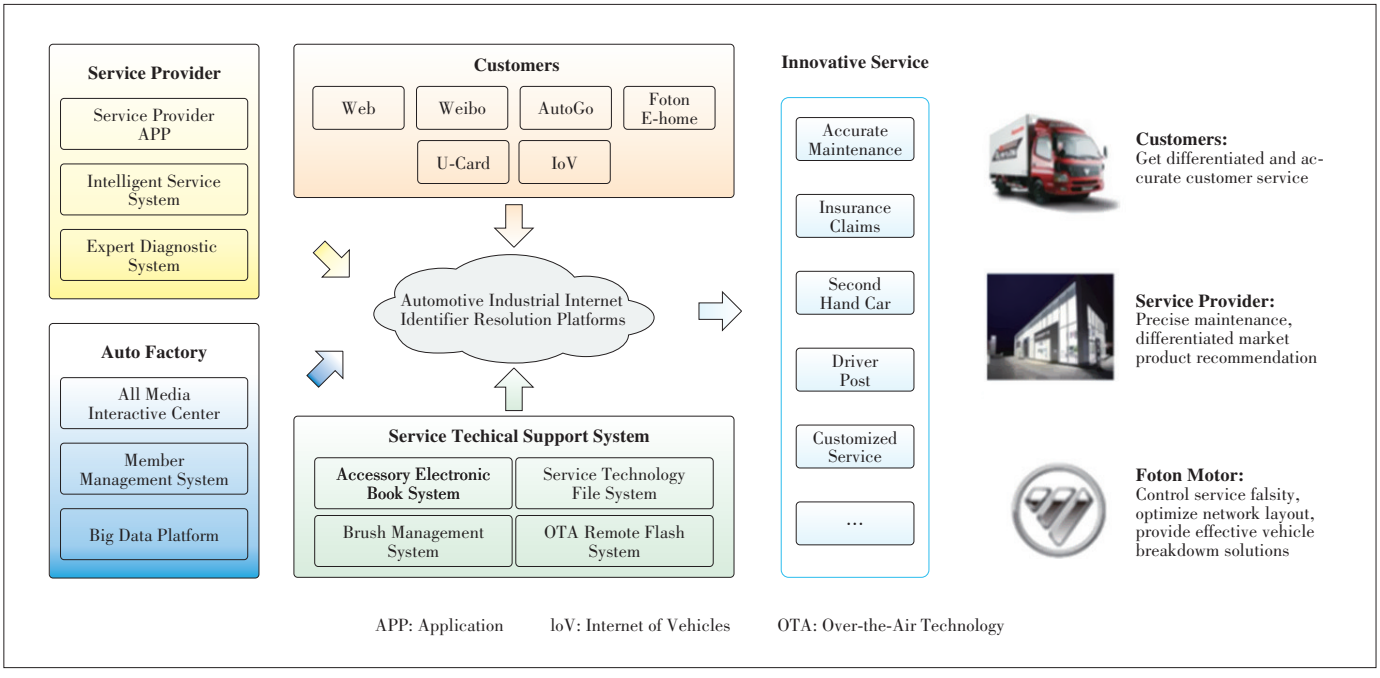
The travelled distance and vehicle operating condition information are registered in the identifier resolution system through the combination with the Internet of Vehicles. When the vehicle needs upkeep, the maintenance invitation will be sent through APP and SMS so as not to affect the service life of the vehicle due to improper maintenance. This will save maintenance costs, improve driving safety for customers, bring profits to service stations, reduce the failure rate, and increase the company's brand reputation at the same time.

3) Driving behavior guidance.

Big data generated in the operation of the vehicle in back end like vehicle's gear, speed, fuel consumption and other operating data, is used to analyzing the customer's driving behavior in order to provide driving behavior guidance to customers. Good driving habits to a certain extent will prolong the service life of the vehicle and reduce the failure rate of the vehicle.

6 Conclusions

The identifier resolution system is set up to standardize the



▲**Figure 7. Service innovation based on identifier resolution.**

registration and application process of the automotive industrial Internet identifier through the implementation of new technologies and key equipment of the industrial Internet and IT. Foton Motor is operating a secondary node of the industrial Internet in China, led by the Ministry of Industry and Information Technology of People's Republic of China. It has applied the identifier resolution system to the automotive industry on manufacturing, marketing and after-sales services.

In order to provide a large number of accurate identifier resolution data to support the development of the automotive industry, we should greatly improve the quantity of equipment identifiers, product identifiers and resource identifiers in the automotive industry. The industry ecology of automotive industrial Internet based on the identifier resolution system should be built at the same time. The ecology may achieve continuous innovation from the three aspects of the enterprise, the car ecology and the car life. Besides, customers should be provided with ecological services; in this way, customer loyalty is expected to be enhanced, influence of products and companies to be expanded, and industry upgrading to be promoted.

References

[1] Alliance of Industrial Internet. Guidelines for the Construction of Secondary Nodes for Industrial Internet Identifier Resolution (trial version) [R/OL]. (2019-06-25) [2020-01-31]. http://www.aii-alliance.org/index.php?m=content&c=index&a=show&catid=23&id=698
[2] Alliance of Industrial Internet. Industrial Internet Identifier Resolution - White Paper on Product Traceability [R/OL]. (2019-06-25) [2020-01-31]. http://www.aii-alliance.org/index.php?m=content&c=index&a=show&catid=23&id=111
[3] Alliance of Industrial Internet. White Paper on Industrial Internet Platform [R/OL]. (2019-06-25) [2020-01-31]. http://www.aii-alliance.org/index.php?m=content&c=index&a=show&catid=23&id=673
[4] Alliance of Industrial Internet. White Paper on Industrial Internet Identifier Resolution Architecture [R/OL]. (2019-06-25) [2020-01-31]. http://www.aii-alliance.org/index.php?m=content&c=index&a=show&catid=18&id=583
[5] JIA X Q, LUO S, HU Y. Industrial Internet Identification and Its Application Research [J]. Information and Communications Technology and Policy, 2019(4): 1 – 5. DOI: CNKI:SUN:DXWJ.0.2019-04-001
[6] ZHANG Y W, CHI C, ZHU S Y. Information and Communications Technology and Policy [J]. Information and Communications Technology and Policy, 2019 (8): 43 – 46

Biographies

LIN Chengjian (linchengjian@foton.com.cn) is a data management engineer in the Department of Information Technology, Foton Motor Inc. Since 2018, He has been in charge of the construction of secondary node at the automotive industrial Internet and also participated in making standards for encoding of automotive identifier, encoding of a-piece-a-code system and connectivity and innovation application based on identifier resolution between primary node and secondary node. He is one of the main technical leaders of constructing identifier resolution for secondary node in the automotive industrial Internet.

LIU Xinwei received her B. Sc. from Huazhong University of Science and Technology, China in 2017. Now she is a graduate student in School of Electronics and Computer Engineering, Peking University, China. Her research interests include computer network architecture and named data networking.

Application of Industrial Internet Identifier in Optical Fiber Industrial Chain

SHI Zongsheng, JIANG Jian, JING Sizhe, LI Qiyuan, and MA Xiaoran
(Jiangsu ZTT LINK Limited Company, Nantong, Jiangsu 226000, China)

Abstract: The industrial Internet has germinated with the integration of the traditional industry and information technologies. An identifier is the identification of an object in the industrial Internet. The identifier technology is a method to validate the identification of an object and trace it. The identifier is a bridge to connect information islands in the industry, as well as the data basis for building a technology application ecosystem based on identifier resolution. We propose three practical applications and application scenarios of the industrial Internet identifier in this paper. Future applications of identifier resolution in the industrial Internet field are also presented

Keywords: industrial Internet; application of identifier; ecology of information application; industrial big data; identifier resolution

DOI: 10.12142/ZTECOM.202001010

http://kns.cnki.net/kcms/detail/34.1294.TN.20200318.1103.004.html, published online March 18, 2020

Manuscript received: 2019-11-18

Citation (IEEE Format): Z. S. Shi, J. Jiang, S. Z. Jing, et al., "Application of industrial internet identifier in optical fiber industrial chain," *ZTE Communications*, vol. 18, no. 1, pp. 66 - 72, Mar. 2020. doi: 10.12142/ZTECOM.202001010.

1 Introduction

The Identifier Resolution System (IRS) is an important part of industrial Internet network architecture. It is a center to connect every segment of the industrial Internet. Once the big data of every company are connected, the information islands may be linked and the information barriers may be broken [1]. Also, the resolution system is the groundwork for technology such as the Internet of Things (IoT), Artificial Intelligence (AI) and intelligent manufacturing in the Industrial internet. In this system, the identifiers map to the articles in the physical environment by digital simulation [2].

Combining the advantages of industrial manufacturing and information technology [3], the IRS provides basic supports for both the Internet companies and the industrial field. Especially, the system may promote the growth of their intersection. Therefore, a new industry may be set up and developed. Moreover, the applications of identifiers will support the modernization of economic system and promote economic development with high quality. The identifier can be used to monitor the all-life-cycle and trace the quality of a product [4].

From now on, the development of the industrial Internet is in an acceleration period. It is also a critical period of information infrastructure upgrading and industry data integration. Thus, the Chinese government is increasing the speed of the construction of the industrial Internet resolution system.

This paper introduces concepts, mainstream technologies and applications of the identifier. The paper develops the objects, scenarios and challenges of the application in the optical fiber industrial chain [5]. It also analyzes the application

directions of the identifier in the future.

2 Background

2.1 Identifiers and Identifier Technology

An identifier is a string that consists of digits, letters, and symbols organized by some rules and standards, and it aims to identify an object. It plays a similar role as the "pointer" in computer language. The pointer points to an address that stores the value in the register. Analogously, the identifier maps the address that stores the description of the object. A user may access the address and request the description by submitting an identifier from a terminal device, such as a smartphone, Radio Frequency Identification (RFID) card reader and bar-code scanner to the resolution system. After the identifier being authenticated, the details of the object can be acquired and retrieved.

The whole system constructs an underlying architecture that connects all the resolved information and other data. The architecture provides the services and functions that the industrial manufacturers need. For example, the system may be used to trace back the product quality by analyzing the time and space record of the product. Besides, the manufacturer may conduct warehouse management by stocking and storing data.

The identifier technology mainly consists of encoding, the identifier carrier, and resolution [6].

The encoding technology gives an entity object such as a product and a process a set of scientific and standardized digits, symbols or other information that can be recognized by terminal equipment. Encoding is aimed to set encoding norms for various industries and fields and provide a unified standard for data exchange and collection between different enterprises.

An identifier carrier implements data transfer. The identifier exists in real life as a carrier such as an RDIF card, 2D code or bar code. Terminal equipment may recognize the identifier and its address. A user with authority may request more descriptions by accessing the address.

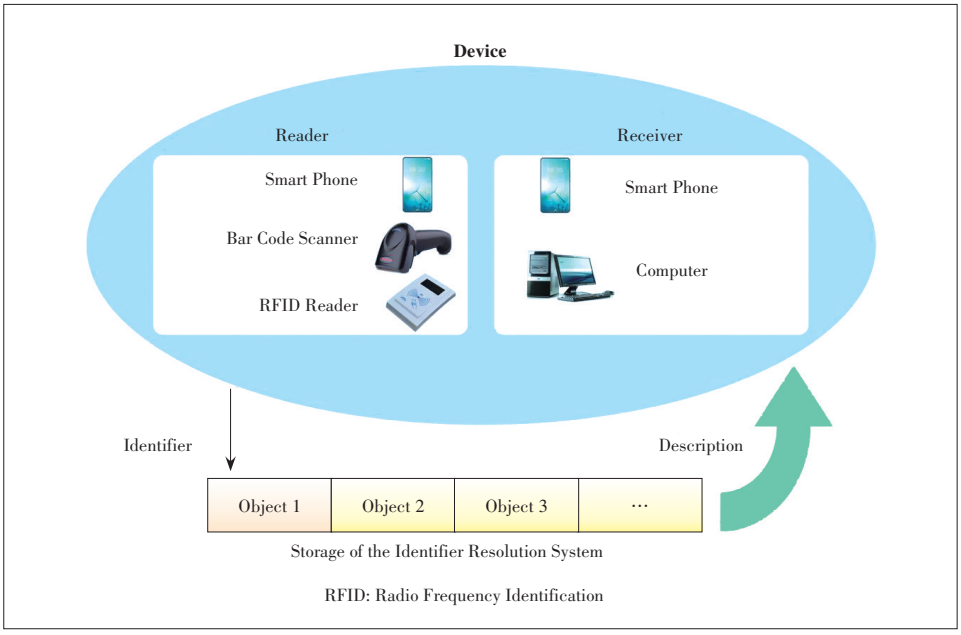
The resolution technology is the process that is mapping the identifier to the descriptions stored in the servers. For example, the resolution result may be a URL link to the detail description of the product.

2.2 Application of Identifiers in the Industrial Internet

The industrial Internet is a new network that serves industrial manufacturing. The identifier in it is similar to the domain name on the Internet, which is unique identification information of every material, product, component, equipment, system or technical proposal. As the identifier technology collects the production data, the resources are classified and managed effectively. Likewise, the resolution of the industrial Internet is like the domain name resolution. In the IRS (**Fig. 1**), a domain name could be achieved by a 2D code which contains the identifier information. Besides, the data, service record and flow record in the industrial manufacture management system of objects may be retrieved by the identifier.

The industrial Internet is the basic part of the process of informational upgrading and transition of the manufacturing enterprises. Nowadays modern industrial producers manage a large number of information systems and equipment, which are difficult to recognize. Moreover, the data is collected by dis-unified mechanisms, rules, and frames because of the wide spectrum demand of software and hardware equipment and the diverse suppliers. Thus, the factories have no effective way to link the inside and outside and cannot connect the front-back end information in the industrial chain [7]. This restricts the national modernization and informatization process.

The significance of the application of identifiers in the industrial Internet is that the application is a bridge linking the data simulation environment and the real environment, which map to each other. By mapping, the operational effec-



▲**Figure 1. The Industrial Internet resolution system.**

tiveness of all types of modeling optimized environment may be applied rapidly and the best method of management and control may be chosen for maximum efficiency and cost reduction.

Identifiers and identifier technologies may be widely applied in the primary and secondary factories. The industry informatization upgrading process can list entities like materials and products by some standardized regulations such as their names and features in a digital system and making entities digitized, modularized, systematized, robotized and intelligent. In the process, the industrial Internet plays an important role and the identifier is the core part.

According to the breadth of the industry, to give every product an identifier, a scientific digital basis accepted by the system is in need. The most important work is mapping the topology structure based on the digit to the industrial Internet, realizing the unity of opposites of the basic entity objects structure, meeting the demand of industrial manufacturing by software development and data operation, interacting products, people and software data. The ultimate goal of the application is developing an industrial mode and build an informational ecosystem whose core is the identifier.

3 Applications of the Industrial Internet

3.1 Industrial Equipment Cloud Platform

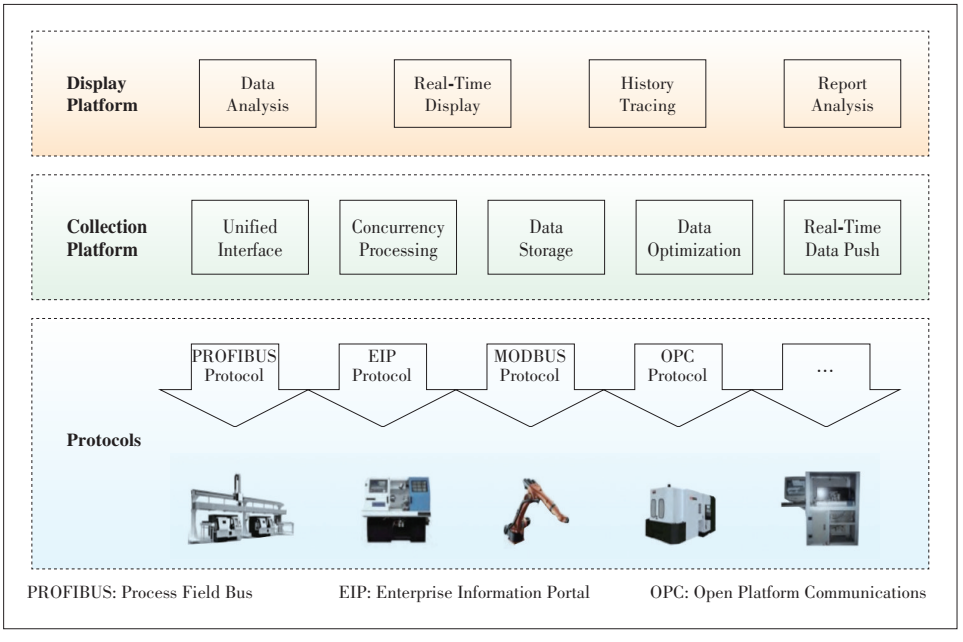
Manufacturing enterprises have their systems in data interconnection, producing process joint and equipment coordination. The monitoring of equipment is the most important function in these systems. Using new technologies such as big data, AI and IoT, the modern industrial equipment cloud platform [8] combines image big data and hardware like industrial robots, monitor and switch, and supports multiple communication protocols. This cloud platform can help the enterprises use industrial equipment effectively.

The equipment management is integrated into the cloud platform management system (**Fig. 2**). Using identifier resolution technology, 2D code, and RFID, the system realizes full-lifecycle equipment management. This system provides abundant functions such as centralized equipment monitoring, equipment management, maintenance management, inspection management, spare parts management, tools management, statistics analysis, unit organization, and basic setting. This platform has a sound mechanism and high-level security. In addition, it stores huge amounts of data and intelligent management equipment in the cloud.

Different from the common equipment cloud management, this equipment cloud connects the national industrial Internet identifier system. Every equipment access to the platform has registered in the identifier resolution secondary node and is given a unique industrial Internet identifier. The user can acquire the information about equipment and use the functions on the platform by the resolution system. This platform realizes the informationalization of equipment management, paperless processing, system modulization, and the improvement of management modes.

The industrial cloud platform is able to realize real-time data collection, real-time monitoring, failure data collection, equipment health management, and predictable maintenance. Moreover, the platform can store the equipment ledger and basic data that are easy to lose. Based on the data collected by the platform, the big data technology implements the analysis of the life cycle of workpieces, rational equipment inspection and alert to maintenance. Early maintenance may reduce the loss of sudden failure. The identifier of a workpiece may associate with the equipment identifier to match the workpiece with the equipment. The platform enables data statistics, which are required by the production management. The data analysis facilitates the operation management and producing strategy.

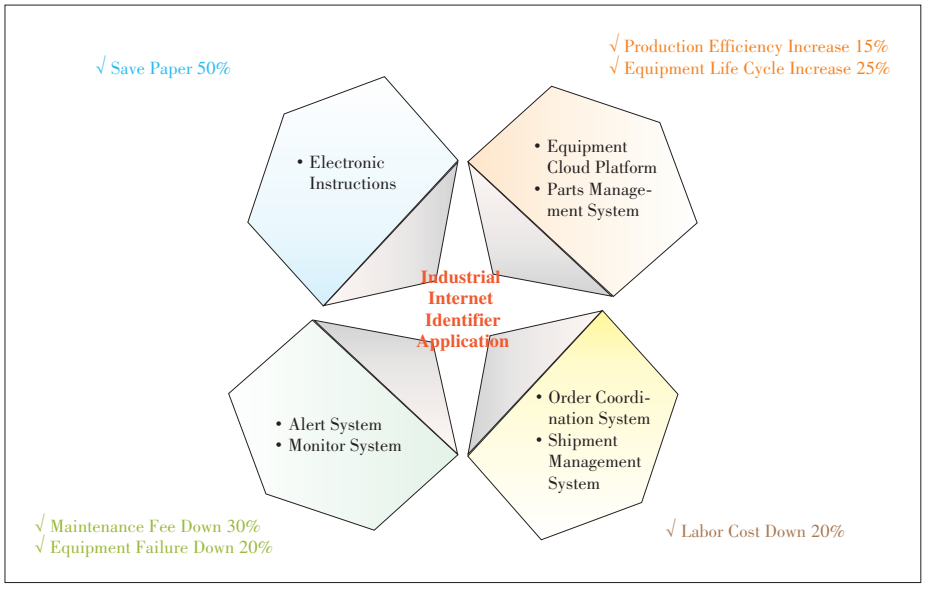
On the cloud platform, different roles have distinct authorities. After scanning the identifier code, the common employees can only retrieve the basic parameters, maintenance tasks, repairing record and inspection record while the man-



▲**Figure 2. Cloud platform management system for equipment monitoring and collection [9].**

ager can read two more reports that are the real-time monitored data and alert record. The separated authorities enhance information security.

The cable production of Zhongtian Technology (ZTT) LINK Company has applied the industrial Internet equipment cloud platform (**Fig. 3**). The platform guarantees the stability of the cable quality. In the Modified Chemical Vapor Deposition (MCVD) processing line, the staff can monitor the equipment continuously, and test the gas Mass Flow Controller (MFC) online. The platform can also test every part of the lathe and keep the stability of the operating parameters. According to the practice of ZTT LINK Company, the maintenance fee has been down by 25% – 30%, the life of equipment has prolonged by 25% – 30%, the unpredictive shutdown of equipment has dropped by 30% – 40%, and the production efficiency has promoted by 15% – 25%.



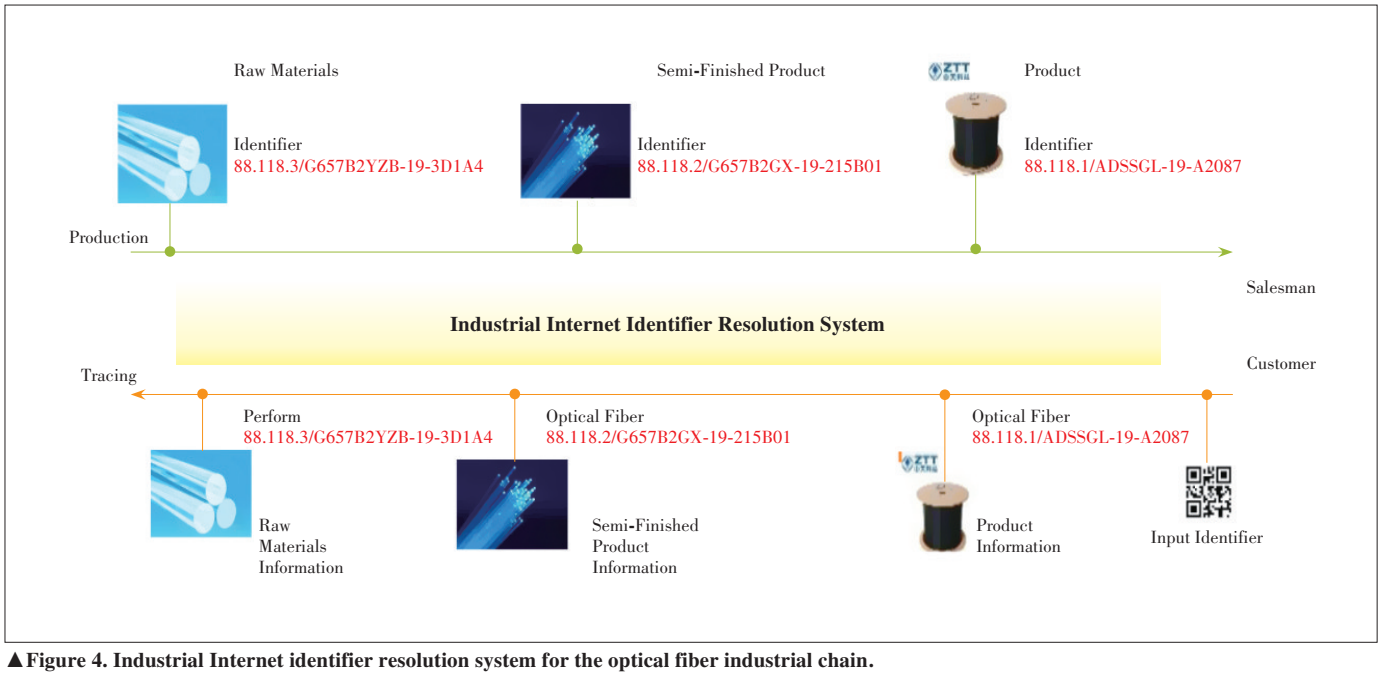
▲**Figure 3. Application of the Industrial Internet identifier at ZTT LINK Company.**

3.2 Tracing Quality

The identifier resolution system provides a method to trace the product. In this system, every company has a unique identifier. Every product made by this company would be given a product code which could be its serial number or a code representing its features. Thus, a product will have a unique identifier consists of the company identifier and product code [10].

An identifier of a product can map to an address in the resolution system where the product information is stored. After scanning the code and uploading the identifier, a user would be able to access the address of the identifier and get the details of the product. Therefore, the product information can be traced by the identifier.

ZTT LINK Company has applied the identifier resolution system in the optical fiber manufacturing chain (**Fig. 4**). This company distributed different identifiers to its factories. The identifier of the optical fiber preform factory is 88. 118. 3 while the identifier of the optical fiber factory is 88. 118. 2 and the identifier of the raw materials factory is 88. 118. 1.



▲**Figure 4. Industrial Internet identifier resolution system for the optical fiber industrial chain.**

Identifiers are distributed to products made by these three factories. The optical fiber preforms are produced in the material factory. In the semi-finished factory, the optical fibers are made. The optical cables are then manufactured in the production factory. All the products made by these three factories are attached by a 2D code label.

ZTT fiber industrial chain has realized the tracing function of the identifier in the three factories. Both the factory staff and clients can search the information by inputting the identifier. When a problem happens in the production process, the staff may scan the 2D code to find the origin of the materials. If the clients find a bad product, they can search the producer and the parameters of the product in the tracing system.

In the identifier system, different users have distinctive authorities. The clients can check the basic information and access the logistics page. The manager and quality inspectors have the authority to check two more pages that are quality information and tracing information.

In the optical cable resolution page, the product information contains basic information, structure parameters, and technical parameters. While installing the cable, a client may scan the 2D code to check the parameters. When the client has a bad cable, the producer can find out by the identifier resolution system. This is the tracing function.

The logistic page consists of the order number and tracking number. The client can trace the product when it is on the way. Once receiving a bad product, the client can check whether the logistics company should take responsibility for the problem.

The quality information includes optical fiber features, mechanism features, and environmental performance. It is very important and therefore, it can only be acquired by factory managers.

In the tracing page, the quality report of the optical fiber is shown. Furthermore, the factory staff can access the report of the optical fiber and the preform. Due to the confidential data in these quality reports, only the factory staffs have the authority to read them.

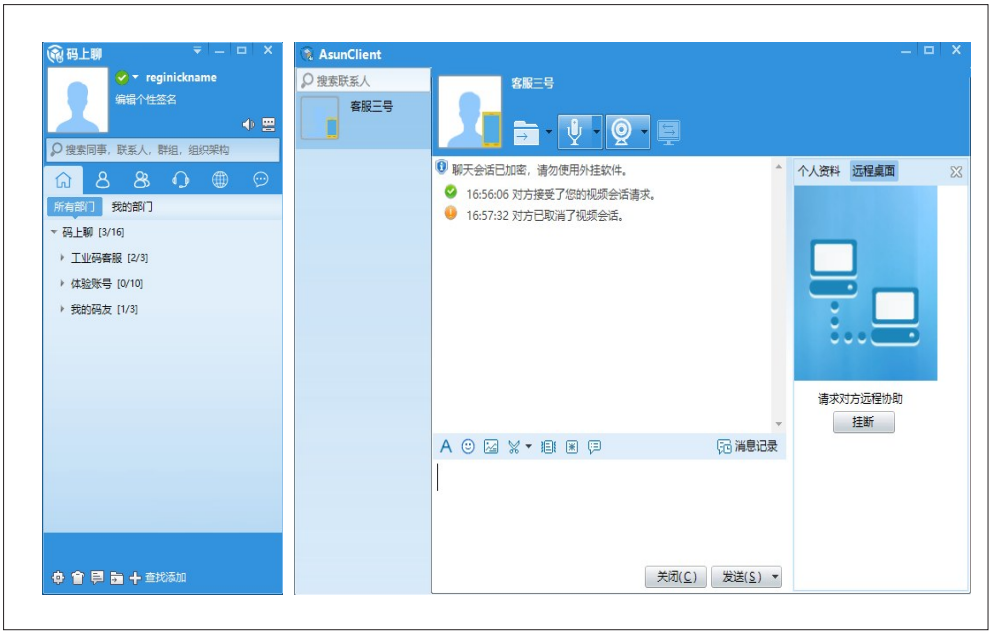
3.3 After-Sales Service Feedback

After-sales service feedback includes system information collection, comment query, and data statistics. This application can collect the data of a product identifier, comment records, comment time, device location and trading code, aiming to increase the satisfaction of customers. It can manage and display these comments and can also analyze the correlation between locations, clients, and their satisfaction. Thus, the suppliers will be able to solve problems specifically. Moreover, this applicationmay promote product quality and increase sales. It also enables enterprises to optimize their production parameters, adjust the processing flow, and improve production efficiency and product quality.

An identifier is the carrier of information. The after-sales service application can collect and analyze the data of consumers. By dynamically updating these data, the application may be used to push and show the products and services that are suitable for customers to satisfy their interests. Technologies like machine learning and data mining can be used to predict the deep demands of users. The precise marketing may expand the consumer group and increase the profit of the enterprise [11].

Base on the identifier, the after-sales service application can feedback the market by analyzing the collected data. This application helps manufacturers improve their products and provides methods for sellers to manipulate the market. The user may access the online retailers of the producer by scanning the 2D code of the product, which benefits the brand spreading. This application can also facilitate and monitor a promotional campaign.

Combining with social networks, the after-sales service feedback system can get through the barriers among the manufacturing enterprise, dealers and customers. This application also links the production and use, and supports the upgrading of products. ZTT LINK Company has released an instant messaging app based on the identifier, MaMsg (**Fig. 5**),



▲**Figure 5. User interface of MaMsg.**

which integrates the factories on the supply chain for convenient communication and cooperation of upstream and downstream enterprises.

4 Identifier-Based Industrial Internet Ecosystem

In China, the industrial Internet is expanding and extending to various fields of the real economy and setting up connections across various enterprises, fields, and industries. The standardization and further research of identifiers and the identifier technology are significant for data sharing and diversified operation, facilitating the forming of an identifier-based industrial Internet ecosystem.

Thus, the definition of industry semantics (standard) based on the identifier and the corresponding standardization of the expansion of the semantics need pushing. The standard of identifier codes and the definition of industry semantics are the basement of the interconnection of everything. The former provides a basis for the connection of enterprises on the whole industry chain. The product object may be digitized by effectively monitoring and counting the data generated in the full-life circle of the object. Enterprises may establish and improve the criteria of the data interpretation according to their own demands or those of the industry. An enterprise may refine the standards of identifier codes to improve its manufacturing process. Furthermore, a country may lead and set a couple of standards to enhance the level of its industrialization and informationalization.

There are still several challenges to be solved during the development of the industrial Internet, identifier and identifier technology in terms of the following four aspects.

1) Technology: The identifier is not only a code but also the description of information. It is necessary to deeply explore what information to be kept or rejected, how to connect the isolated information and how to integrate the information of the present and the future.

2) Standardization: This involves multiple fields and nations and is difficult to make a decision of compromise or reset.

3) Benefits of enterprises: In the process of establishing the criteria of encoding, some powerful companies may play the leading role, while small businesses have a high probability to be out.

4) Promotion: The industrial Internet has a long way to go. It is especially hard to promote the identifier resolution system. It would be better to insist on a long-time strategy. Meanwhile, one standard, mass registration, and high value need a long time to achieve.

The industrial Internet resolution system involves many crucial industrial fields that influence the national economy and people's livelihood. As a bond connecting the layers of production management, commerce circulation, and marketing, the identifier resolution system will build an ecosystem of information application. In the future, the system tends to the omnidirectional development and becomes a cornerstone of the development of the national industrial Internet.

5 Conclusions

The collision and integration of the industry and the Internet are not only in the construction and use of the network but also in the communication of information. The industrial Internet identifier, the identifier technology and the application of the identifier are the core of the informatization upgrading, as well as the important components of the basic information infrastructure such as the IoT, smart cities and intelligent manufacturing. Now, the industrial Internet identifier has been applied in various industrial scenarios. The identifier technology enables the customization based on business demands and some technologies may be applied across multiple platforms. ZTT LINK Company is operating a second node of the industrial Internet led by the Ministry of Industry and Information Technology of People's Republic of China. It has applied the identifier resolution system to the optical fiber industry for sake of manufacturing, logistics, and marketing. Besides, it provides solutions for identifier applications of other industries. It has applied functions such as equipment cloud platform, anti-fake, anti-fleeing and quality tracing to the industries of energy, home textiles, and medicine. The development of the identifier application has a long way to go. Especially the standardization of identifier encoding has to correspond to the practical demands of the manufacturing enterprises. The standards should be set scientifically and corresponding to certain criteria.

References

[1] WU J. Big Data, Machine Intelligence and Their Impacts to the Future World [J]. Telecommunications Science, 2015, 31(2): 7-16
[2] ZHANG Y, CHI C, ZHU S. Development Trend of Industrial Internet Identification Resolution System [J]. Information and Communications Technology and Policy, 2019(8): 43 - 46
[3] DU J, WANG F. Connotation, Service System of Internet and Its Integrating Path to Manufacture [J]. Telecommunications Science, 2016, 32(1): 98 - 104
[4] YU X, Xu H, Li H, et al. Industrial Internet Identifier Resolution System-Product Tracing [EB/OL]. (2019-04-18) [2019-11-05]. http://www.aii-alliance. org/index. php? m=content&c=index&a=document_download&ftype=3&fid=111&fno=0
[5] MANTHOU V, VLACHOPOULOU M, FOLINAS D. Virtual e-Clain (Vec) Model for Supply Chain Collaboration [J]. International Journal of Production Economics, 2004, 87(3): 241 - 250. DOI: 10.1016/S0925-5273(03)00218-4
[6] YANG Z, ZHANG D, LI J, et al. Identifier Technology in Industrial Internet [J]. Telecommunications Technology, 2017, 33(11): 134 - 140
[7] Anderson D, Lee H. Synchronized Supply Chains: The New Frontier [J]. ASCET, 1996, 6(1): 12 - 21
[8] YANG S W. Impact of the Upgraded Version of German "Industrial 4 Platform" on China's Manufacturing Industry [J]. Telecommunications Science,

2016, 32(1): 108 - 111
[9] Jiangsu ZTT LINK Limited Company. Equipment Monitoring and Data Collecting System [EB/OL]. (2019-06-30) [2019-11-08]. http://www.asuncloud.com/platform/show-9.html
[10] WU S L, YAN Y. Innovative Application of Drug Electronic Monitoring Code Based on IoT Identification [J]. Capital Food Medicine, 2012(10): 11 - 12
[11] LI J Z. The Collision Between Big Data and Marketing [J]. Modern Marketing, 2017(9): 40

Biographies

SHI Zongsheng received his M.E. degree in software engineering and domain engineering from Nanjing University of Science and Technology, China in 2013. He is currently the general manager of Jiangsu ZTT LINK Limited Company. He is also the chief of the Nantong Software Association, the associate head of the Ad Hoc Group of the League of the industrial Internet Identifier and a committee member of the Security Standard of the industrial Internet System. His research interests include the industrial Internet platform, cloud platform, application of the identifier. He received the Nantong Software Award, Jiangsu Province Innovation Achievements Award, the National Excellent CIO, the Excellent CIO of Manufacturing Industry, and the Jiangsu Intelligent Manufacture Innovation Competition Award.

JIANG Jian received his M.E. degree in software engineering from Fudan University, China in 2016. He is the CTO of Jiangsu ZTT LINK Limited Company. His research interests are the system architecture of the industrial Internet and cloud platforms.

JING Sizhe received his M.S. degree in information system from The University of Sheffield, UK in 2013. He is a project manager of Jiangsu ZTT LINK Limited Company. His research interests are the application development of the cloud platform, big data, and the project design of identifier system.

LI Qiyuan (liqy@chinaztt.com) received his B.E. degree in information engineering from Shanghai University, China in 2019. He is a software development engineer at Jiangsu ZTT LINK Limited Company. His research interests are the application development of the cloud platforms, big data, and the project design of the identifier system.

MA Xiaoran (maxr@chinaztt.com) received his M.S. degree in computer science from Stevens Institute of Technology, USA in 2018. He is a software development engineer at Jiangsu ZTT LINK Limited Company. His research interests are the application development of the cloud platform, big data, and the project design of the identifier system.

Towards Converged Millimeter–Wave/Terahertz Wireless Communication and Radar Sensing

GAO Xiang, Saqlain MUHAMMAD, CAO Xiaoxiao, WANG Shiwei, LIU Kexin, ZHANG Hangkai, and YU Xianbin

(College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, Zhejiang 310027, China)

DOI: 10.12142/ZTECOM.202001011

http://kns.cnki.net/kcms/detail/34.1294.TN.20200316.1103.003.html, published online March 17, 2020

Manuscript received: 2019-12-18

Abstract: Converged communication and radar sensing systems have attained increasing attention in recent years. The development of converged radar-data systems is reviewed, with a special focus on millimeter/terahertz systems as a promising trend. Firstly, we present historical development and convergence technology concept for communication-radar systems, and highlight some emerging technologies in this area. We then provide an updated and comprehensive survey of several converged systems operating in different microwave and millimeter frequency bands, by providing some selective typical communication and radar sensing systems. In this part, we also summarize and compare the system performance in terms of maximum range/range resolution for radar mode and Bit Error Rate (BER) /wireless distance for communication mode. In the last section, the convergence of millimeter/terahertz communication-radar system is concluded by analyzing the prospect of millimeter-wave/terahertz technologies in providing ultrafast data rates and high resolution for our smart future.

Keywords: system convergence; wireless communication; radar sensing; millimeter-wave; terahertz

Citation: (IEEE Format): X. Gao, S. Muhammad, X. X. Cao, et al., "Towards converged millimeter-wave/terahertz wireless communication and radar sensing," *ZTE Communications*, vol. 18, no. 1, pp. 73–82, Mar. 2020. doi: 10.12142/ZTECOM.202001011.

1 Introduction

The invention of radio ushered the history of mankind into a new era, and wireless communication and radar sensing are two prominent types of radio applications. Radar detection plays an important role in our daily life. Up to date, it has been used to cover different aspects of requirements with its distinctive properties. For instance, SHERRIF et al. used 94-GHz Frequency Modulated Continuous Wave (FMCW) radar to invent a powered wheelchair in 2017 which can help the handicapped to improve their mobility when facing some inconvenient phenomena, such as entering in a building with non-barrier-free areas [1], and ZHANG et al. realized hand gesture recognition using double channels 5.8 GHz Doppler-radar [2].

In order to recognize targets more accurately, the tendency pushes the radar frequency into higher bands, such as the millimeter-wave band, even the terahertz band. Besides that, millimeter-wave and terahertz are indeed more resistant to fog, snow, and other natural conditions than presently available laser radar. The first application of the millimeter wave in the radar was traced back in 1958, when C. W. TOLBERT used a millimeter radar to successfully receive 8.6 mm (34.8 GHz) and 4.3 mm (69.7 GHz) signals reflected from a phantom target [3]. After that, many researchers devoted themselves to explore this specific area. For example, an active millimeter-wave radar system operated over the frequency band 15–40 GHz was used to obtain information about the structure of dressing materials and hand support cast [4], and a millimeter-wave radar permits short-range, high-resolution detection and imaging of the airport movement area for safety [5].

Moreover, the fast growing industry researches for remote sensing applications, such as Light Detection And Ranging (LIDAR), which can provide high resolution and be used for the mapping and monitoring of wetland to monitor sea levels.

This work is supported in part by National Natural Science Foundation of China (NSFC) under Grant No. 61771424, and in part by Natural Science Foundation of Zhejiang Province under Grant No. LZ18F010001.

By comparison, terahertz sensing technology has some advantages, as terahertz waves provide better capability of penetrating some materials, less atmospheric disturbance as well as less difficulty in tracking the beam.

The territory of wireless communication was traced back to 1880, when Alexander invented and patented a particular telephone that conducted audio conversations wirelessly over modulated light beam. In the modern era of wireless communication, 5G technologies are currently widely researched in the international academia and industry, targeting a downloading speed of up to 10 Gbit/s. However, it has been reported that by 2020, the number of connecting wireless devices will exceed more than 20 million, which must have a stringent demand of more frequency spectrum resources.

Moving forward, new technologies to converge communication-radar systems would be highly appreciated. Definitely, this further development will not only enable the efficient usage of the spectrum, but also bring about many benefits including architecture unification and simplification, functional reconfiguration, energy enhancement, as well as cost reduction. The early work on fusing wireless communication and radar sensing was reviewed in 1987, when the NASA space shuttle orbiter was operated either as a radar system for rendezvous with other space vehicles, or as a two-way communication system with the ground through the tracking and data relay satellite system [6]. After that, the converged radar-communication system has made tremendous progress and combined with numerous emerging technologies for enhancing its performance. Up to date, the radar resolution in such joint systems has been retained up to centimeter level [7], and the data rate gets to over 10 Gbit/s in a photonic system [8].

The rest of this paper is organized as follows. An overview of convergence technology for joint system design is reviewed in Section 2. Several selective demonstrations of joint systems and their performances comparison are presented in Section 3. In Section 4, a concept of integrating millimeter-wave/terahertz radar sensing and wireless communication is highlighted. Finally, we give the conclusion in Section 5.

2 Overview of Convergence Technology for Converged Systems

Under specific circumstances, it is quite difficult to precisely combine different functions required to operate communication and radar systems simultaneously. To cope with this problem, convergence operations are typically done using reconfigurable circuits based on software programming, and hence provide a good flexibility to implement joint system operation together.

2.1 Communication-Radar Convergence Schemes

Table 1 summarizes some typical single and multi-carrier communication-radar convergence schemes that have been recently proposed in [7], [9] – [18]. Integrating wireless and sensing functions within a single platform helps reduce system cost and complexity as well as increase operational reliability. For single carrier systems, communication and radar signals are divided into the frequency domain [17], code domain [7], [19] and time domain [18], [20], [21], while multiple carrier techniques are also employed to achieve multifunctionality [22]. The code domain (spread spectrum) in single carrier systems is a popular technique that was first implemented for two-way transmission system for vehicular communication and ranging applications [23]. Spread spectrum techniques have been exploited for convergence functions such as direct-sequence spread spectrum (DSSS) [7], [23] – [26] and Chirp Spread Spectrum (CSS) [19]. Code based schemes provide secure communication and high resolution ranging at the price of excessive spectrum resources utilization for data communication. Moreover, different users share the same frequency band simultaneously but using different codes, which is beneficial for multiuser application scenarios. However, the spread spectrum techniques have two main disadvantages for radar ranging and Doppler estimation. One is limited peak to side-lobe ratio caused by imperfect autocorrelation features of codes and the other is a huge computational time required by the spread spectrum technique for Doppler processing. Generally, the spread spectrum technique is more complex, costly and less efficient in view of system implementation.

Similarly, in multicarrier systems, the Orthogonal Frequency-division Multiplexing (OFDM) technique is the most favorable choice and has been widely used for communication and radar systems. The main advantage of OFDM technique is that it resolves the problem of radar ranging and Doppler processing [27], [28] compared with its counterparts. In recent years, several signal processing techniques have been proposed and implemented. In the beginning, matched filters were used to execute range and Doppler estimation in [29] – [34]. OFDM processing algorithms were proposed [35] – [38] to counter low dynamic range and preserve the resolution and processing gain of correlation based processing method. Advanced OFDM algorithms for joint range and Doppler estimation have much higher dynamic range than the spread spectrum approach in view of high Signal-to-noise Ratio (SNR) level. Moreover, the OFDM technique is efficient in estimating the Doppler frequency from the target range. The OFDM technique requires complex signal processing, and high peak-to-average power increases its implementation cost and still hinders its widespread applications.

Time domain duplex has also attracted research interest due to its high spectral efficiency, easy system implementation and low cost [18], [20], [21], [39], [40]. This scheme minimizes mutual interference as radar and communication functions operate independently. Subsequently, various kinds of waveforms and modulation techniques for converged systems can be applied, respectively, according to the application scenarios.

On the other hand, Radio-over-Fiber (RoF) technology has also become the exciting research area for military and high

▼**Table 1. Summary of fusion technology**

	Method Type	System Type	Domain	Radar Mode	Communication Mode	Year	Reference
Electronics	Joint Waveform	Single Carrier	Frequency	Pulse (DSSS)	ASK	2002	[23]
			Code	Pulse (DSSS)	MSK	2016	[12]
				Pulse	DQPSK	2007	[17]
				Pulse (DSSS)	PPM	2010	[7]
				Pulse (CSS)	QPSK	2011	[16]
		Multiple Carrier	---	Pulse (OFDM)	PSK	2017	[11]
				Pulse	CPM	2017	[13]
				Pulse (OFDM)	OFDM	2009	[60]
				CW (SFCW)	DPSK	2015	[14]
	Time-Domain Duplex	---	Time	Trapezoidal FMCW	BPSK	2011	[9]
				FMCW	FSK	2008	[18]
				Trapezoidal FMCW	PSK	2013	[15]
Photonics	---	Multiple Carrier	---	Pulse (OFDM)	16-QAM	2017	[8]

ASK: Amplitude Shift Keying
BPSK: Binary Phase Shift Keying
CPM: Continuous Phase Modulation
CSS: Chirp Spread Spectrum
DPSK: Differential Phase Shift Keying
DQPSK: Differential Quadrature Phase-shift Keying
DSSS: Direct-Sequence Spread Spectrum
FMCW: Frequency Modulated Continuous Wave
FSK: Frequency Shift Keying
MSK: Minimum-shift Keying
OFDM: Orthogonal Frequency-Division Multiplexing
PPM: Pulse Position Modulation
PSK: Phase Shift Keying
QAM: Quadrature Amplitude Modulation
QPSK: Quadrature Phase Shift Keying
SFCW: Stepped Frequency Continuous Wave

speed sensing applications [41]. The OFDM technique has also been used in RoF system for efficient utilization of spectrum and less inter-symbol interference. Recently, 30 GHz converged OFDM communication and radar sensing system has been reported in [8].

Generally, radar systems can be classified as Continuous-wave (CW) and pulsed modes. FMCW and Linear Frequency Modulated (LFM) pulses are categorized under CW and pulse radar, respectively. FMCW radars have been widely used in the automobile field, and have their distinctive features of lower emission-peak-power, simple modulation and signal processing, and low cost. The FMCW radars have been demonstrated in synthetic aperture radar systems [42], radar imaging [43] – [45] and range localization [46], [47]. Another important kind of CW radar is Frequency-Stepped Continuous Wave (FSCW), as demonstrated in [48], [49]. FSCW technique is more suitable for Ground Penetrating Radar (GPR) since it has such advantages as wide dynamic range, high mean power, low noise figure and probably the most important one, the possibility of shaping the power spectral density [50]. It is important to note that FMCW and FSCW radar waveforms are mostly used in time domain duplex scheme due to its low cost and easy implementation.

With regard to pulse radar systems, pulse modulation realizes signal oscillation that only occurs at a specified time interval. LFM signals have been widely used in pulse radar systems [51], [52] featuring some advantages, such as non-sensitive to the Doppler frequency shift of echo, simple radar signal processing, superior range resolution, and radial velocity resolution. Besides that, Non-Linear Frequency Modulation (NLFM) [53], phase encoding [54], and time-frequency encoding [55] are supplement technologies of pulse modulation.

In converged systems, digital modulation techniques have also been employed for better quality and efficient communication and hence achieve good system performance. Digital modulation provides benefits over analog modulation including available bandwidth and has better noise immunity. In this paper, we generally discuss the modulation techniques listed in Table 1. The Pulse Position Modulation (PPM) format, implemented non-coherently, is suitable for optical communication. However, this format has multipath interference and synchronization problem. Differential Quadrature Phase-shift Keying (DQPSK) technique has been used to avoid the problem associated with lack of phase synchronization between transmitter and receiver. Continuous Phase Modulation (CPM) modulates the data bits in a continuous manner and therefore has high spectral efficiency. This is particularly important in wireless communication where bandwidth is expensive. Similarly, other simple modulation formats like Binary Phase Shift Keying (BPSK), On-Off Keying (OOK) and frequency Shift Keying (FSK) have been commonly used in wireless and optical communication. Both BPSK and OOK have the same bandwidth and not suitable for high data rates applications. The FSK technique occupies more spectrum and is used for high frequency radio applications. The MSK format encodes each bit as a half sinusoid and reduces non-linear dis-

tortion. On the other hand, the Quadrature Amplitude Modulation (QAM) format supports high data rate applications and has been widely used in modern wireless and optical fiber communications. Various combinations of amplitude and phase have been employed to achieve high data rates.

Hence, it is important to choose an appropriate combination of modulation formats, which should enable system optimization and performance improvement.

2.2 Single Carrier and Multiple Carrier Systems

Converged communication-radar systems can be also classified on the basis of carrier types, such as single carrier and multiple carrier. Certainly, both of these two methods have their respective advantages and drawbacks.

From Table 1, we can see that single-carrier systems have been paid more attention due to their simplicity, more stability and relatively mature technology compared with other systems [12], [16], [17]. However, their drawbacks are obvious as well. Spectrum overlapping between radar and communication signals, particularly with data transmission at high data rates, may lead to inter-symbol interference, and as a consequence the system is not extensively used.

Multiple-carrier based schemes, especially OFDM has been widely used in the wireless communication system, as it shows superiority compared with single-carrier in terms of high spectral efficiency, strong rigidity to inter-symbol and inter-channel interference. However, OFDM technology uses subcarrier modulation, which consequently requires costly and complex transceiver design and implementation. The OFDM technique has also been proposed in the design of radar waveform [56], and has been demonstrated in a Multiple Input and Multiple Output (MIMO) radar system [57], for multiple target detection and estimation [58] and drone detection [59], etc. It is worthwhile to note that an OFDM based radar system does not have the range-Doppler estimation which may have serious influence on the precision of range finding [27], [28].

3 Demonstration of Various Joint Systems

In past years, several converged communication and radar systems have been developed. In this section, we selectively present some joint systems that operated in different microwave and mm-wave frequency bands. Single and multi-carrier based converged systems listed in Table 1 are simple and low cost design and provide more consistent performance for both radar and communication modes. Moreover, their practical implementation and system performance of both communication and sensing functions are also discussed and their performance will be compared at the end of this section.

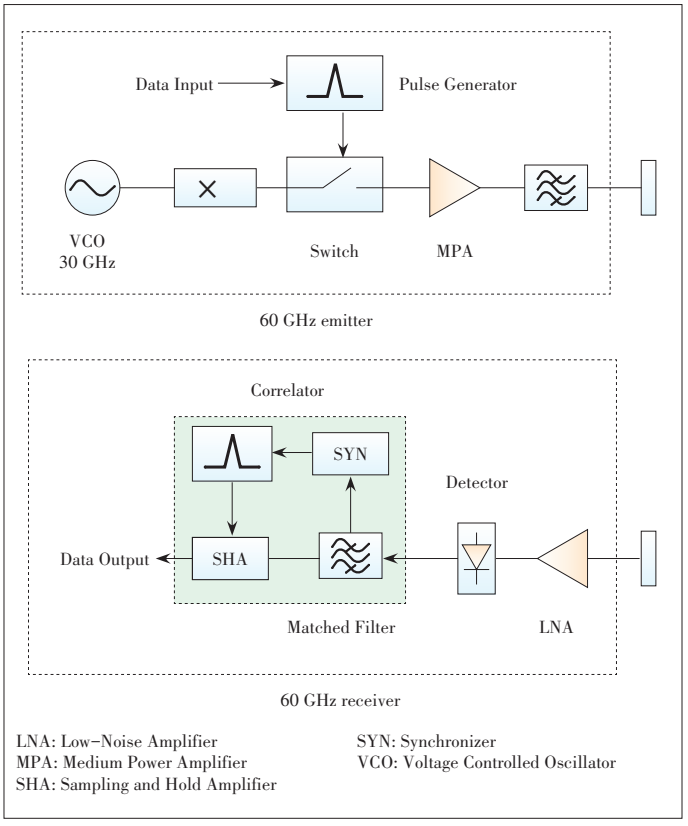
3.1 Single Carrier System

As an example, a single transceiver was proposed to work for two modes in [7], serving as a communication device and a location detector simultaneously. **Fig. 1** shows the experimental system based on PPM that was conducted for communication and accurate location finding based on time reversal process. In this setup, the communication and radar mode ranges are 10 m and 3 m respectively. A 60-GHz system with approximately 300 ps pulse width and modulated signal almost of 3 GHz bandwidth obtained an experimental result for a data rates of up to 200 Mbit/s with measured bit error rate (BER) of less than 10^{-6}. This system prototype realizes 10 m wireless communication and a radar range resolution of 12. 4 cm within the scope of 3 m. To alleviate the multipath interference, a synchronizer was used in the setup to synchronize the incoming signals received from other sensors.

3.2 Multiple Carrier System

As aforementioned, MIMO technology has been widely used in both communication and radar systems [10]. MIMO system typically uses OFDM. This multiplexing technique is used to ensure the separation of each frequency component in order to overcome multi-path interference, which is challenging for the implementation of MIMO systems [57]. For illustration purpose, an OFDM based system is presented here [60].

Fig. 2 shows the joint system based on MIMO technology and this system was setup in the laboratory range of 5 m for both radar and communication modes although the communication mode range could be made more than 10 m. The gen-



▲ **Figure 1. A 60-GHz joint communication and radar system based on Pulse Position Modulation (PPM) technique [7].**

erated OFDM signal is up-converted and amplified in the analog front-end section. The transmitted signal bandwidth is 7 – 8 GHz, aiming at airborne radar sensor networks. The experimentally obtained range resolution is about 0. 30 m, which agrees very well with theoretical range resolution. It should be noted that the effective bandwidth is only 500 MHz when calculating the theoretical range resolution. In addition, data transmission capability is 57 Mbit/s by using 64 sub-carriers.

3.3 Duplex Time-Domain System

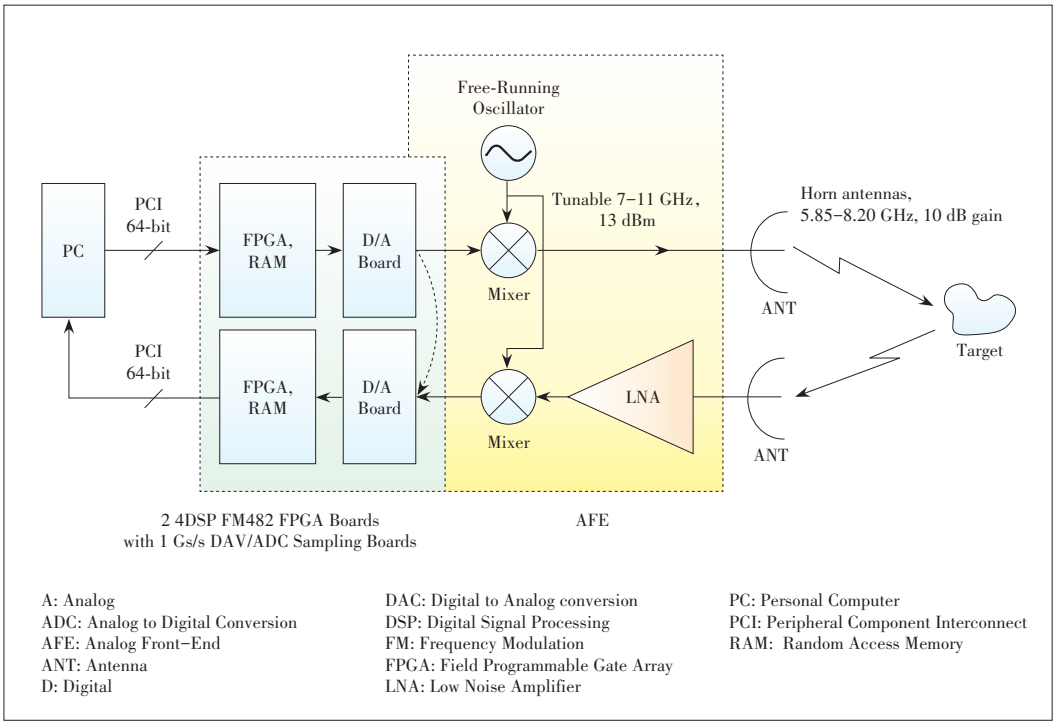
Fig. 3 shows a proposed time domain duplex system based on Trapezoidal Frequency Modulated Continuous Wave (TFM-CW) for radar and Binary Phase Shift Keying (BPSK) for communication [9].

In the radar mode, a Direct Digital Synthesizer (DDS) is used to deal with the transmitted signal, which is then filtered and up converted to an Intermediate Frequency (IF) signal. Further, the IF signal is split into two portions: one is converted to a Radio Frequency (RF) signal and then radiated via the transmitting antenna; the other is preserved for demodulation. On the receiver side, the reflected RF wave captured by the receiver antenna is converted back into the IF domain after amplification, which as a result is mixed with the preserved one for evaluating the range and velocity of the target.

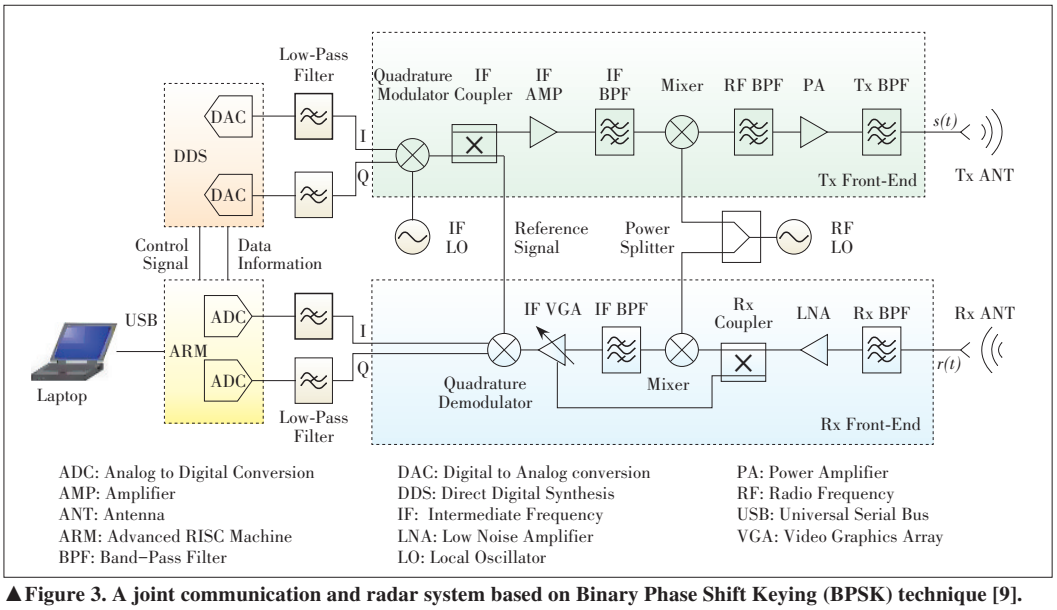
In the communication mode, the modulated signal is transmitted in the same way as in the radar mode. The BPSK modulation format is selected for enhancing the noise and distortion tolerance.

This system operates within the frequency range from 24. 075 GHz to 24. 175 GHz. The demonstrated data rate is 50 Mbit/s with measured BER of less than 10^{-6}, and meanwhile, the maximum detectable radar range is 100 m with a range resolution of 1. 5 m, which indicates the maximum measurable velocity is approximately 260 km/h.

Fig. 4a represents the physical photograph of the radar mode of duplex time domain system and shows six targets and their arrangements in front of the system. **Fig. 4b** shows



▲ **Figure 2. A joint radar and communication system based on Orthogonal Frequency-Division Multiplexing (OFDM) Multiple Input and Multiple Output (MIMO) technique [60].**



▲ **Figure 3. A joint communication and radar system based on Binary Phase Shift Keying (BPSK) technique [9].**

the frequency estimation by using a Fast Fourier Transform (FFT) with zero padding.

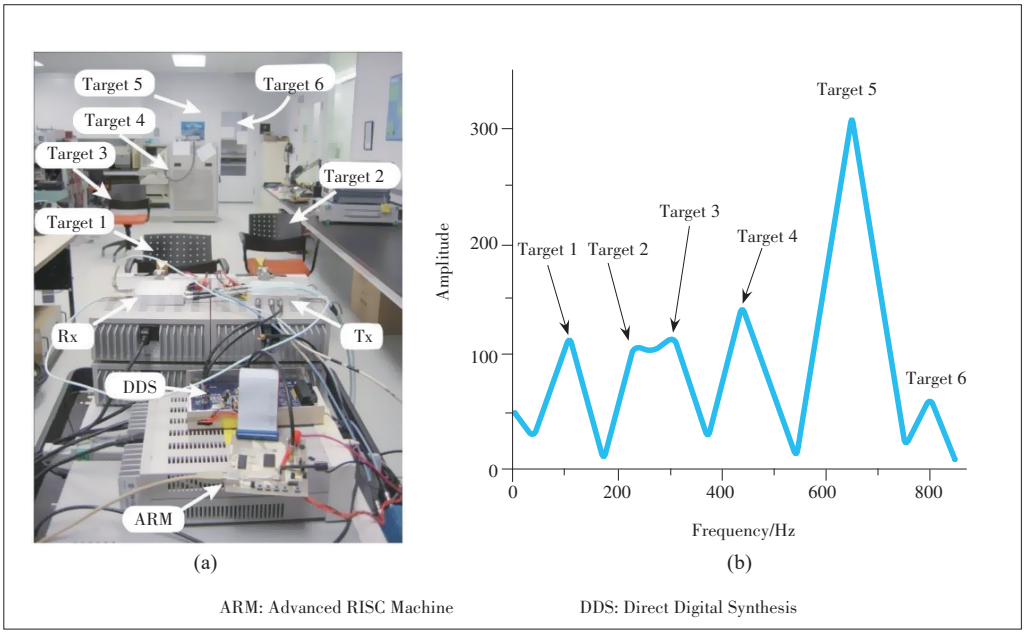
3.4 RoF System

In the past decades, microwave photonics has gained a lot of attention due to its attractive capacity of delivering "last mile" wireless signals. This technology potentially supports large bandwidth, and is capable of generating high frequency signals with better performance in a noisy environment [61], [62]. Therefore, RoF technology has been extensively used for both radar systems and communication systems [63] – [67]. For instance, a system based on RoF technology was proposed to perform both communication and radar sensing functionalities, as shown in **Fig. 5** [8]. In the radar mode, it uses OFDM technique with 10.1 GHz bandwidth. With respect to the wireless communication mode, an Arbitrary Waveform Generator (AWG) is first used to generate a 7 GHz IF signal with 3.62 Gbaud 16-QAM on a single carrier. The IF carrier of 7 GHz is then up-converted to 31 GHz, filtered to eliminate the side-band spurious noise, and modulated onto 1.55 μm light via an Mach-Zehnder Modulator (MZM) and transmitted over the fiber. The modulated light signal after fiber transmission is detected by a Photodiode (PD) and then eventually emitted to free space. The system realizes up to 14.5 Gbit/s data rate within distance of 10 m and the minimum ranging resolution of 5 cm.

3.5 Performance Comparison

Here we summarize and compare performance of the demonstrated communication and radar systems, as presented in **Table 2**.

As we can see, the dual mode 60-GHz system for automotive applications in [7] supports a better data rate compared to other electronic joint systems. In the communication mode, this system has a confined range of 10 m due to serious absorption of oxygen for V-band and U-band frequency signals. Similarly, for the radar mode, it has a superior range resolution of 12.4 cm by exploring 3 GHz bandwidth. The 24-GHz integrated radio and radar system in [9] has dissimilar performance compared with [7]. A joint system with the operating frequency range of 7 – 8 GHz shows an average performance and a worse BER of 5×10^{-2} compared with all the other systems. From above discussion, we conclude that the technologies for converged systems still need more maturity for better performance. The emerging technologies including mm-wave and terahertz facilitate a better feasibility of de-

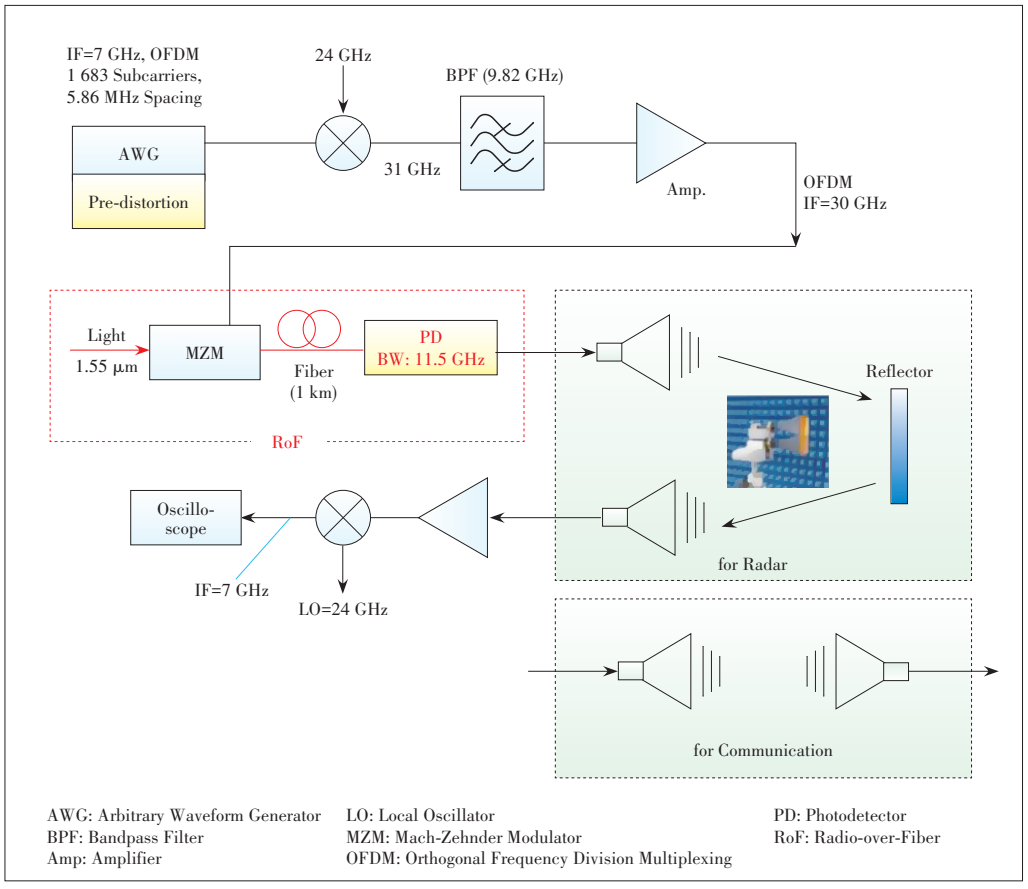


▲**Figure 4. (a) Picture of the measurement setup of radar mode; (b) frequency estimation [9].**

▼**Table 2. Performance comparison of the demonstrated joint systems**

References	Carrier Frequency/GHz	Communication Mode				Radar Mode			
		Modulation Format	Range/m	Data Rate/(Mbit/s)	BER	Signal Type	Bandwidth/MHz	Range/m	Range Resolution/cm
[7]	60	PPM	10	200	$<1\times10^{-6}$	Pulse (single)	3 000	3	12.4
[9]	24.125	BPSK	200	50	$<1\times10^{-6}$	TFMCW	100	70	165
[60]	7.0 – 8.0	OFDM	5	57	$<5\times10^{-2}$	Pulse (OFDM)	1 000	5	30
[8]	25 – 35	16-QAM	10	14 500	$<1\times10^{-3}$	Pulse (OFDM, Photonics)	10 000	5	5

BER: Bit Error Rate
BPSK: Binary Phase Shift Keying
PPM: Pulse Position Modulation
OFDM: Orthogonal Frequency Division Multiplexing
QAM: Quadrature Amplitude Modulation
TFMCW: Trapezoidal frequency modulated continuous-wave



▲**Figure 5. A joint radar and communication system based on ROF technology [8].**

signing a well-structured converged system.

4 Towards a Millimeter-Wave/Terahertz Converged Radar and Communication System

Based on the technical survey above, we can see converged millimeter-wave systems have exhibited better capacity for both radar and communication modes, supporting better ranging resolution and higher data rates. This is fully understandable since there are larger frequency bandwidth available in the higher frequency bands. In fact, this is believed to be the technical tendency from both industrial and academic sides, exploring high frequency bands (millimeter-wave, even terahertz (100 GHz – 10 THz)).

For sake of high resolution radars systems in the future, millimeter wave/terahertz for radar sensing can provide superior performance compared to microwave. Millimeter wave/terahertz sensors have such distinctive features as larger bandwidth enabling better ranging resolution, low possibility of interception and interference, and smaller antenna size than low frequency microwave. Millimeter wave radar systems have been recently well-developed for automotive applications at 24 GHz and 77 GHz [68], [69], and most recently, a terahertz photonic radar has been reported as its potential of enabling mm-scale range resolution [70].

On the other hand, to accommodate the ever increasing wireless data stream, the overall data rate is expected to reach beyond 100 Gbit/s, and eventually Tbit/s; in this context, the carrier frequency naturally goes into the millimeter-wave and terahertz frequency regions [71]. Recently, a lot of efforts are devoted to broadband terahertz wireless communications, and several demonstrations of beyond 100 Gbit/s in the terahertz band have been reported, attributed to the extremely broad terahertz bandwidth available [72] – [75].

Up to date, millimeter-wave and terahertz have been explored for either radar or communication purposes, however, the converged system in such high frequency is not demonstrated yet. This thrusting area needs more breakthrough from academia and industry to develop converged systems based on emerging technologies in near future. Therefore, more technological progress in mm-wave/terahertz is essential for our smart future.

The previous work on the converged systems in the microwave band has opened a door for the researchers to to develop new converged systems based on modern technologies. Moreover, the features of millimeter and terahertz wave technologies can provide a solution to a cost-effective, simple and light, and high bandwidth converged system to support higher date rates compared with microwave technology-based system.

5 Conclusions

The convergence of communication and radar sensing functions within a single platform is expected to provide a better solution to a low cost and high efficiency multi-functional system. In this paper, we have overviewed the technological trend of converged communication-radar systems. We have also presented the convergence technology and summarized several typical converged systems operating in the microwave and millimeter-wave bands. Future convergence work for making the terahertz wireless communication systems robust in differ-

ent indoor environments will be highly appreciated, e. g. , the precise imaging capabilities of radar sensing in the terahertz range can assist terahertz communications system to optimize the indoor scattering environment by providing reflection parameters of different objects, as well as to help radio channel modeling in a particular indoor scenario.

For sake of better ranging resolution and higher data rates, the technical tendency in the near future is expected to explore mm-wave/terahertz high frequency bands for such converged systems, from both industrial and academic sides, while a lot of research is still needed to push convergence forward.

References

[1] ABDULATIF S, KLEINER B, AZIZ F, et al. Stairs Detection for Enhancing Wheelchair Capabilities Based on Radar Sensors [C]//IEEE 6th Global Conference on Consumer Electronics (GCCE). Nagoya, Japan, 2017: 1 – 4. DOI: 10.1109/gcce.2017.8229270

[2] ZHANG J J, TAO J K, SHI Z G. Doppler-Radar Based Hand Gesture Recognition System Using Convolutional Neural Networks [M]//Lecture Notes in Electrical Engineering. Singapore, Singapore: Springer, 2018: 1096 – 1113. DOI: 10.1007/978-981-10-6571-2_132

[3] TOLBERT C, STRAITON A, BRITT C. Phantom Radar Targets at Millimeter Radio Wavelengths [J]. IRE Transactions on Antennas and Propagation, 1958, 6 (4): 380 – 384. DOI:10.1109/tap.1958.1144609

[4] OWDA A Y, SALMON N, ANDREWS D, et al. Active Millimeter-Wave Radar for Sensing and Imaging through Dressing Materials [C]//IEEE SENSORS. Glasgow, UK, 2017. DOI: 10.1109/icsens.2017.8234228

[5] GALATI G, PIRACCI E G, FERRI M. ResolutionHigh, Millimeter-Wave Radar Applications to Airport Safety [C]//8th International Conference on Ultrawideband and Ultrashort Impulse Signals (UWBUSIS). Odessa, Ukraine, 2016: 21 – 26. DOI: 10.1109/uwbusis.2016.7724144

[6] CAGER R, LAFLAME D, PARODE L. Orbiter Ku-Band Integrated Radar and Communications Subsystem [J]. IEEE Transactions on Communications, 1978, 26(11): 1604 – 1619. DOI: 10.1109/tcom.1978.1094004

[7] BOCQUET M, LOYEZ C, LETHIEN C, et al. A Multifunctional 60-GHz System for Automotive Applications with Communication and Positioning Abilities Based on Time Reversal [C]//7th European Radar Conference. Paris, France, 2010: 61 – 64

[8] UMEZAWA T, JITSUNO K, KANNO A, et al. 30-GHz OFDM Radar and Wireless Communication Experiment Using Radio over Fiber Technology [C]//Progress in Electromagnetics Research Symposium—Spring (PIERS). St Petersburg, Russia, 2017: 22 – 25.DOI: 10.1109/piers.2017.8262288

[9] HAN L, WU K. 24-GHz Integrated Radio and Radar System Capable of Time-Agile Wireless Communication and Sensing [J]. IEEE Transactions on Microwave Theory and Techniques, 2012, 60(3): 619 – 631. DOI: 10.1109/tmtt.2011.2179552

[10] HU L, DU Z C, XUE G R. Radar-Communication Integration Based on OFDM Signal [C]//IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). Guilin, China, 2014: 442 – 445.DOI: 10.1109/icspcc.2014.6986232

[11] WANG W Q, ZHENG Z, ZHANG S. OFDM Chirp Waveform Diversity for Co-Designed Radar-Communication System [C]//18th International Radar Symposium (IRS). Prague, Czech Republic, 2017. DOI: 10.23919/IRS.2017.8008139

[12] HUANG R Q, ZHAO X L, ZHANG Q, et al. Spectrum Extension Research of Radar-Communication Integrated Waveform [C]//2nd IEEE International Conference on Computer and Communications (ICCC). Chengdu, China, 2016: 1804-1808. DOI: 10.1109/compcomm.2016.7925013

[13] ZHANG Y, LI Q Y, HUANG L, et al. Waveform Design for Joint Radar-Communication System with Multi-User Based on MIMO Radar [C]//IEEE Radar Conference (RadarConf). Seattle, USA, 2017: 415 – 418. DOI: 10.1109/radar.2017.7944238

[14] HU F, CUI G L, YE W, et al. Integrated Radar and Communication System Based on Stepped Frequency Continuous Waveform [C]//IEEE Radar Conference (RadarCon). Arlington, USA, 2015: 1804 – 1807. DOI: 10.1109/radar.2015.7131155

[15] MOGHADDASI J, WU K. Improved Joint Radar-Radio (RadCom) Transceiver for Future Intelligent Transportation Platforms and Highly Mobile High-Speed Communication Systems [C]//IEEE International Wireless Symposium (IWS). Beijing, China, 2013. DOI: 10.1109/ieee-iws.2013.6616796

[16] XIE Y N, TAO R, WANG T. Method of Waveform Design for Radar and Communication Integrated System Based on CSS [C]//First International Conference on Instrumentation, Measurement, Computer, Communication and Control. Beijing, China, 2011: 737 – 739. DOI: 10.1109/imccc.2011.187

[17] WINKLER V, DETLEFSEN J. Automotive 24 GHz Pulse Radar Extended by a DQPSK Communication Channel [C]//European Radar Conference. Munich, Germany, 2007: 138 – 141.DOI: 10.1109/eurad.2007.4404956

[18] STELZER A, JAHN M, SCHEIBLHOFER S. Precise Distance Measurement with Cooperative FMCW Radar Units [C]//IEEE Radio and Wireless Symposium. Orlando, USA, 2008: 771 – 774. DOI: 10.1109/rws.2008.4463606

[19] SADDIK G N, SINGH R S, BROWN E R. Ultra-Wideband Multifunctional Communications/Radar System [J]. IEEE Transactions on Microwave Theory and Techniques, 2007, 55(7): 1431 – 1437. DOI: 10.1109/tmtt.2007.900343

[20] KONNO K, KOSHIKAWA S. Millimeter-Wave Dual Mode Radar for Headway Control in IVHS [C]//IEEE MTT-S International Microwave Symposium Digest. Denver, USA, 1997: 1261 – 1264.DOI:10.1109/mwsym.1997.596556

[21] Han L, Wu K. Radar and Radio Data Fusion Platform for Future Intelligent Transportation System [C]//7th European Radar Conference. Paris, France, 2010: 65 – 68.DOI:10.1109/ACCESS.2016.2530979

[22] GARMATYUK D, SCHUERGER J, KAUFFMAN K. Multifunctional Software-Defined Radar Sensor and Data Communication System [J]. IEEE Sensors Journal, 2011, 11(1): 99 – 106. DOI:10.1109/jsen.2010.2052100

[23] MIZUI K, UCHIDA M, NAKAGAWA M, et al. Vehicle-to-Vehicle Communication and Ranging System Using Spread Spectrum Technique [C]//Vehicular Technology Conference. Secaucus, USA, 1993: 2 – 5. DOI: 10.1109/VETEC.1993.507206

[24] LINDENMEIER S, BOEHM K, LUY J F. A Wireless Data Link for Mobile Applications [J]. IEEE Microwave and Wireless Components Letters, 2003, 13(8): 326 – 328. DOI: 10.1109/lmwc.2003.815706

[25] XU S, CHEN Y, ZHANG P. Integrated Radar and Communication Based on DS-UWB [C]//3rd International Conference on Ultrawideband and Ultrashort Impulse Signals. Sevastopol, Ukraine, 2006: 142 – 144. DOI: 10.1109/uwbus.2006.307182

[26] LIN Z Y, WEI P. Pulse Amplitude Modulation Direct Sequence Ultra Wideband Sharing Signal for Communication and Radar Systems [C]//7th International Symposium on Antennas, Propagation & EM Theory. Guilin, China, 2006. DOI: 10.1109/isape.2006.353326

[27] FRANKEN G E A, NIKOOKAR H, GENDEREN P. Doppler Tolerance of OFDM-Coded Radar Signals [C]//European Radar Conference. Manchester, UK, 2006: 108 – 111.DOI: 10.1109/eurad.2006.280285

[28] STURM C, ZWICK T, WIESBECK W. An OFDM System Concept for Joint Radar and Communications Operations [C]//VTC Spring 2009—IEEE 69th Vehicular Technology Conference. Barcelona, Spain, 2009. DOI: 10.1109/vetecs.2009.5073387

[29] TIGREK R F, DE HEIJ W J A, GENDEREN PV. Multi-Carrier Radar Waveform Schemes for Range and Doppler Processing [C]//IEEE Radar Conference. Pasadena, USA, 2009: 2 – 6. DOI: 10.1109/radar.2009.4976986

[30] LELLOUCH G, TRAN P, PRIBIC R, et al. OFDM Waveforms for Frequency Agility and Opportunities for Doppler Processing in Radar [C]//IEEE Radar Conference. Rome, Italy, 2008. DOI: 10.1109/radar.2008.4720798

[31] TIGREK R F, DE HEIJ W J A, GENDEREN PV. Solving Doppler Ambiguity by Doppler Sensitive Pulse Compression Using Multi-Carrier Waveform [C]//5th European Radar Conference. Amsterdam, Netherlands, 2008: 72 – 75

[32] GENDEREN V. Recent Advances in Waveforms for Radar, Including Those

with Communication Capability [C]//European Radar Conference. Rome, Italy, 2009: 318 – 325
[33] GENDEREN V. A Communication Waveform for Radar [C]//8th International Conference on Communications. Bucharest, Romania, 2010: 289 – 292. DOI: 10.1109/iccomm.2010.5509110
[34] BERGER C R, DEMISSIE B, HECKENBACH J, et al. Signal Processing for Passive Radar Using OFDM Waveforms [J]. IEEE Journal of Selected Topics in Signal Processing, 2010, 4(1): 226 – 238. DOI: 10.1109/jstsp.2009.2038977
[35] STURM C, PANCERA E, ZWICK T, et al. A Novel Approach to OFDM Radar Processing [C]//IEEE Radar Conference. Pasadena, USA, 2009: 9 – 12. DOI: 10.1109/radar.2009.4977002
[36] STURM C, BRAUN M, ZWICK T, et al. A Multiple Target Doppler Estimation Algorithm for OFDM Based Intelligent Radar Systems [C]//7th European Radar Conference. Paris, France, 2010: 73 – 76
[37] BRAUN M, STURM C, JONDRAL F K. Maximum Likelihood Speed and Distance Estimation for OFDM Radar [C]//IEEE Radar Conference. Arlington, USA, 2010: 256 – 261.DOI:10.1109/radar.2010.5494616
[38] BRAUN M, STURM C, JONDRAL F K. On the Single-Target Accuracy of OFDM Radar Algorithms [C]//IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications. Toronto, Canada, 2011: 794 – 798. DOI: 10.1109/pimrc.2011.6140075
[39] YATTOUN I, LABIA T, PEDEN A, et al. A Millimetre Communication System for IVC2007 [C]//7th International Conference on ITS Telecommunications. Sophia Antipolis, France, 2007: 281 – 286.DOI: 10.1109/ITST.2007.4295879
[40] ZHANG H, LI L, WU K. 24GHz Software-Defined Radar System for Automotive Applications [C]//European Conference on Wireless Technologies. Munich, Germany, 2007: 138 – 141.DOI: 10.1109/ecwt.2007.4403965
[41] YU J G, GONG M J, ZHANG M. RoF Communication Technology and Its Application Prospect [J]. ZTE Communcations, 2009, 7(3): 12 – 15
[42] JUNG D H, PARK S O. Ku-Band Car-Borne FMCW Stripmap Synthetic Aperture Radar [C]//International Symposium on Antennas and Propagation (ISAP). Phuket, Thailand, 2017. DOI: 10.1109/isanp.2017.8228895
[43] ALIZADEH P, PARINI C, RAJAB K Z. A Low-Cost FMCW Radar Front End for Imaging at 24 GHz to 33 GHz [C]//Loughborough Antennas & Propagation Conference (LAPC). Loughborough, United Kingdom, 2015: 24 – 27. DOI: 10.1109/lapc.2015.7366007
[44] CHENG P, WANG Z, XIN Q, et al. Imaging of FMCW MIMO Radar with Interleaved OFDM Waveform [C]//12th International Conference on Signal Processing. Hangzhou, China, 2014: 1944 – 1948.DOI: 10.1109/ICOSP.2014.7015332
[45] GANIS A, NAVARRO E M, SCHOENLINNER B, et al. A Portable 3-D Imaging FMCW MIMO Radar Demonstrator with a 24× 24 Antenna Array for Medium-Range Applications [J]. IEEE Transactions on Geoscience and Remote Sensing, 2018, 56(1): 298 – 312. DOI: 10.1109/tgrs.2017.2746739
[46] SCHEIBLHOFER W, FEGER R, HADERER A, et al. Simultaneous Localization and Data-interrogation Using a 24-GHz Modulated-Reflector FMCW Radar System [C]//IEEE MTT-S International Microwave Symposium (IMS). Honolulu, USA, 2017: 67 – 70.DOI: 10.1109/mwsym.2017.8058669
[47] PENG Z Y, RAN L X, LI C Z. A K-Band Portable FMCW Radar with Beamforming Array for Short-Range Localization and Vital-Doppler Targets Discrimination [J]. IEEE Transactions on Microwave Theory and Techniques, 2017, 65 (9): 3443 – 3452. DOI: 10.1109/tmtt.2017.2662680
[48] MASKELL D L, WOODS G S. A Frequency Modulated Envelope Delay FSCW Radar for Multiple-Target Applications [J]. IEEE Transactions on Instrumentation and Measurement, 2000, 49(4): 710 – 715. DOI: 10.1109/19.863911
[49] MASKELL D L, WOODS G S. A Multiple-Target Ranging System Using an FM Modulated FSCW Radar [C]//Microwave Conference. Munich, Germany, 1999: 888 – 891.DOI: 10.1109/APMC.1999.833736
[50] NICOLAESCU I, GENDEREN PVAN, DONGEN K WVAN, et al. Stepped Frequency Continuous Wave Radar Data Preprocessing [C]//Advanced Ground Penetrating Radar. Nantes, France, 2003: 14 – 16. DOI: 10.1109/AGPR.2003.1207315
[51] ZHU D K, LIU Y X, HUO K, et al. A Novel High-Precision Phase-Derived-Range Method for Direct Sampling LFM Radar [J]. IEEE Transactions on Geoscience and Remote Sensing, 2016, 54(2): 1131 – 1141. DOI: 10.1109/tgrs.2015.2474144
[52] SHI P F, GUO J M, LV P, et al. The Chirp-based Analog to Information Conversion in the LFM Pulse Compression Radar [C]//CIE International Conference on Radar (RADAR). Guangzhou, China, 2016. DOI: 10.1109/radar.2016.8059317
[53] KURDZO J M, CHEONG B L, PALMER R D, et al. Optimized NLFM Pulse Compression Waveforms for High-Sensitivity Radar Observations [C]//International Radar Conference. Lille, France, 2014. DOI: 10.1109/radar.2014.7060249
[54] XIONG Y, CHENG M, GAO Y, et al. Simulation Research on the Use of Phase Encoding Algorithm in Correcting Range Ambiguity for Doppler Weather Radar [C]//International Conference on Information Science and Technology. Nanjing, China, 2011: 761 – 765.DOI: 10.1109/icist.2011.5765356
[55] NUNN J, WRIGHT L J, SÖLLER C, et al. Large-Alphabet Time-Frequency Entangled Quantum Key Distribution by Means of Time-to-Frequency Conversion [J]. Optics Express, 2013, 21(13): 15959. DOI: 10.1364/oe.21.015959
[56] PETTERSSON M. Multifrequency Complementary Phase-Coded Radar Signal [J]. Radar, Sonar and Navigation, 2000, 147(6): 1 – 22. DOI: 10.1049/ip-rsn: 20000734
[57] DONNET B, LONGSTAFF I. Combining MIMO Radar with OFDM Communications [C]//European Radar Conference. Manchester, UK, 2006. DOI: 10.1109/eurad.2006.280267
[58] SINGH U K, BHATIA V, MISHRA A K. Multiple Target Detection and Estimation of Range and Doppler for OFDM-RADAR System [C]//4th International Conference on Signal Processing and Integrated Networks (SPIN). Noida, India, 2017: 27 – 32.DOI: 10.1109/spin.2017.8049910
[59] NUSS B, SIT L, FENNEL M, et al. MIMO OFDM Radar System for Drone Detection [C]//18th International Radar Symposium. Prague, Czech, 2017: 1 – 9.
[60] GARMATYUK D, KAUFFMAN K. Radar and Data Communication Fusion with UWB-OFDM Software-Defined System [C]//IEEE International Conference on Ultra-Wideband. Vancouver, Canada, 2009: 454 – 458.DOI: 10.1109/icuwb.2009.5288748
[61] WANG F, SHI S, SCHNEIDER G J, et al. Photonic Microwave Generation with High-Power Photodiodes [C]//IEEE Photonics Conference. Bellevue, UAS, 2013: 350 – 351.DOI: 10.1109/IPCon.2013.6656581
[62] LIN B, PAN B W, ZHENG Z, et al. A Review of Photonic Microwave Generation [C]//IEEE Optoelectronics Global Conference (OGC). Shenzhen, China, 2016. DOI: 10.1109/ogc.2016.7590480
[63] ZHANG F Z, PAN S L. Microwave Photonic Signal Generation for Radar Application [J]. Electromagnetics: Applications and Student Innovation Competition (iWEM), 2016, 2: 2 – 4
[64] GHELFI P, LAGHEZZA F, SCOTTI F, et al. A Fully Photonics-Based Coherent Radar System [J]. Nature, 2014, 507(7492): 341 – 345. DOI: 2014.10.1038/nature13078
[65] LI R M, LI W Z, WEN Z L, et al. Synthetic Aperture Radar Based on Photonic-Assisted Signal Generation and Processing [C]//Opto-Electronics and Communications Conference (OECC) and Photonics Global Conference (PGC). Singapore, Singapore, 2017. DOI: 10.1109/oecc.2017.8114844
[66] GHELFII P, LAGHEZZA F, SCOTTI F, et al. Photonic Generation of High Fidelity RF Sources for Mobile Communications [J]. Journal of Lightwave Technology, 2017, 35(18): 3901 – 3908. DOI: 10.1109/JLT.2017.2707411
[67] INOUEI T, IKEDA K, KAKUBARI Y, et al. Millimeter-Wave Wireless Signal Generation and Detection Using Photonic Technique for Mobile Communication Systems [C]//IEEE International Topical Meeting on Microwave Photonics (MWP). Long Beach, USA, 2016: 55 – 58
[68] MAYER W, GRONAU A, MENZEL W, et al. A Compact 24 GHz Sensor for Beam-Forming and Imaging [C]//9th International Conference on Control, Automation, Robotics and Vision. Singapore, Singapore, 2006: 1 – 6. DOI: 10.1109/icarcv.2006.345160
[69] ANDRES M, FEIL P, MENZEL W. 3D-Scattering Center Detection of Automotive Targets Using 77 GHz UWB Radar Sensors [C]//6th European Conference on Antennas and Propagation (EUCAP). Prague, Czech, 2012: 3690 – 3693. DOI: 10.1109/eucap.2012.6206580
[70] ZHANG H K, WANG S W, JIA S, et al. Experimental Generation of Linearly Chirped 350 GHz Band Pulses with a Bandwidth beyond 60 GHz [J]. Optics Letters, 2017, 42(24): 5242. DOI: 10.1364/ol.42.005242
[71] YU X, CHEN Y, GALILI M, et al. The Prospects of Ultra-Broadband THz Wireless Communications [C]//16th International Conference on Transparent Optical Networks (ICTON 2014). Graz, Austria, 2014. DOI: 10.1109/ICTON.2014.6876675

[72] YU X, JIA S, HU H, et al. 160 Gbit/s Photonics Wireless Transmission in the 300-500 GHz Band [J]. APL Photonics, 2016, 1(8): 081301. DOI: 10.1063/1.4960136
[73] YU X B, ASIF R, PIELS M, et al. 400-GHz Wireless Transmission of 60-Gb/s Nyquist-QPSK Signals Using UTC-PD and Heterodyne Mixer [J]. IEEE Transactions on Terahertz Science and Technology, 2016, 6(6): 765 – 770. DOI: 10.1109/tthz.2016.2599077
[74] JIA S, PANG X, OZOLINS O, et al. 0.4THz Photonic-Wireless Link with 106Gbit/s Single Channel Bitrate [J]. Journal of Lightwave Technology, 2018, 36(2): 610 – 616, 2018
[75] JIA S, YU X B, HU H, et al. 120 Gb/s Multi-Channel THz Wireless Transmission and THz Receiver Performance Analysis [J]. IEEE Photonics Technology Letters, 2017, 29(3): 310 – 313. DOI: 10.1109/lpt.2016.2647280

Biographies

GAO Xiang received the B.S. degree from Zhejiang Sci-Tec University, China in 2017. He is currently working towards the M.S. degree at the School of Electronic science and technology, Zhejiang University. His current research interest is terahertz imaging.

Saqlain MUHAMMAD received the M.S. degree in electronics communication engineering from the University of Nottingham, Malaysia Campus in 2013. He has been a Ph.D. student at the College of Information Science and Electronic Engineering, Zhejiang University since 2017. His research interests are terahertz communication and channel impairments.

CAO Xiaoxiao received the B.S. degree from Anhui University, China in 2017. She is currently working towards the M.S. degree at the School of Electronic science and technology, Zhejiang University. Her current research interest is terahertz imaging.

WANG Shiwei received the B.S. degree in electronics science and technology from Harbin Institute of Technology, China in 2016. He is currently working towards the Ph.D. degree in electronics science and technology at Zhejiang University. His current research interests are in the areas of terahertz/microwave photonics and terahertz communications.

LIU Kexin received the B.S. degree from Sun Yat-sen University, China in 2016. She received the M.S. degree from the College of Information Science and Electronic Engineering, Zhejiang University in 2019. Her research interest is terahertz communications.

ZHANG Hangkai received the B.S. and M.S. degrees from the College of Information Science and Electronic Engineering from Zhejiang University, China in 2018. His research interest is terahertz/microwave photonics.

YU Xianbin (xyu@zju.edu.cn) received his Ph.D. degree in 2005 from Zhejiang University, China. From 2005 to 2007, he was a postdoctoral researcher at Tsinghua University, China. Since November 2007, he has been with the Technical University of Denmark, Kongens Lyngby, Denmark, as a Postdoctoral and Assistant Professor, and was promoted to a Senior Researcher in 2013. He is currently a Research Professor with Zhejiang University, China. He has authored or coauthored two book chapters and more than 150 peer-reviewed international journal and conference papers in the area of microwave photonics and optical communications. His current research interests are in the areas of terahertz/microwave photonics, optical fiber communications, ultrafast photonic wireless signal processing, and ultrahigh frequency wireless access technologies.

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 3000 to 8000, 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 in-text 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
- Inspec
- Ulrich's Periodicals Directory
- Wanfang Data

ZTE COMMUNICATIONS
Vol. 18 No. 1 (Issue 69)
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
Online Submission: https://mc03.manuscriptcentral.com/ztecom

Annual Subscription: RMB 80
Printed by:
Hefei Tiancai Color Printing Company

Publication Date: March 25, 2020

Publication Licenses: ISSN 1673-5188
CN 34-1294/ TN