SCIENCE CHINA
Information Sciences

• REVIEW •

August 2018, Vol. 61 081301:1–081301:25
https://doi.org/10.1007/s11432-017-9426-4

Overview of 5G security technology

Xinsheng JI, Kaizhi HUANG*, Liang JIN, Hongbo TANG, Caixia LIU, Zhou ZHONG, Wei YOU, Xiaoming XU, Hua ZHAO, Jiangxing WU & Ming YI

National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002*, China*

Received 15 November 2017/Revised 10 February 2018/Accepted 26 February 2018/Published online 9 July 2018

Abstract The 5th-generation mobile communication system (5G) has higher security requirements than previous systems. Accordingly, international standard organizations, operators, and equipment manufacturers are focusing extensively on 5G security technology. This paper analyzes the security requirements of 5G business applications, network architecture, the air interface, and user privacy. The development trends of 5G security architecture are summarized, with a focus on endogenous defense architecture, which represents a new trend in 5G security development. Several incremental 5G security technologies are reviewed, including physical layer security, lightweight encryption, network slice security, user privacy protection, and block chain technology applied to 5G.

Keywords 5G security, endogenous defense, mimic defense, physical layer security, lightweight encryption, network slice security, user privacy preservation, block chain

Citation Ji X S, Huang K Z, Jin L, et al. Overview of 5G security technology. Sci China Inf Sci, 2018, 61(8): 081301, https://doi.org/10.1007/s11432-017-9426-4

1 Introduction

To achieve a true "Internet of everything", the new generation of mobile communication technology, the 5th-generation (5G) mobile communication system, will be used for human-to-human communication and for human-to-machine and machine-to-machine communication. The International Standards Organization of the 3rd Generation Partnership Project (3GPP) has defined more than 70 kinds of 5G SA1 files required in this respect [1] and which can be divided into three kinds of scenarios: enhanced mobile broadband (eMBB), massive machine type communication (mMTC), and ultra-reliable low latency communication (uRLLC). Correspondingly, the key technologies that need to be developed for 5G are: massive multiple-input multiple-output (MIMO), filter bank based multicarrier (FBMC), full duplex, ultra-dense networking (UDN), software-defined networking (SDN), and network function virtualization (NFV) [2].

With the continuous development of new traffic, new architecture, new technologies, and new application scenarios in 5G, researchers of 5G security technology are consistently facing new challenges. The industry also anticipates the use of new approaches to promote developments related to architecture and endogenous security technology research, and to overcome problems when security and communication are separated from each other and security is maintained by patching; thereby achieving the vision of building 5G with a safety gene [3].

* Corresponding author (email: huangkaizhi@tsinghua.org.cn)

This paper first introduces research related to 5G security technology, and then combs 5G security requirements from a 5G development perspective, including aspects of traffic application, core network, air interfaces, and user privacy. In this respect, security challenges facing the current security architecture of mobile communications are analyzed. The authors propose that it is necessary to excavate endogenous security elements from the network architecture and electromagnetic transmission mechanism, and to introduce new security increments in the development of a 5G endogenous safety network. Finally, considering security recourses and characteristics relating to the 5G network and air-interference technology, recent advances and future trends of 5G security incremental supporting technologies are comprehensively reviewed, including the applications of physical layer security, lightweight encryption, network slice security, user privacy preservation, and block chain in 5G.

2 5G security technology research

Since the launch of 5G international standardization, 5G network security has become the focus of research attention. In February 2016, the 3rd Generation Partnership Project Service and System Aspects (3GPP SA) [1, 4] Technical Specifications Group began approving 5G security research projects, and the 3GPP SA3 research report TR 33.899, "Study on the security of the next generation system" represents the basis of the group's 5G security standardization work. The latest version V1.3.0 of TR33.899 presents a total of 106 solutions for 97 key issues, including 17 security areas that basically cover all 5G security requirements, and lists both time arrangements for solving issues and the key problems of each issue [4].

However, the International Telecommunication Union-Telecommunication Study Group 17 (ITU-T SG17) has grave concerns about 5G security issues involving mobile virtual operations, telecommunications fraud, the Internet of things, the Internet of vehicles, and the software definition network[1)]. In its 5G security white paper, the 5G Public Private Partnership (PPP) Security Working Group introduced research on security architecture, access control, privacy protection, trust models, security monitoring and management, network slicing security isolation, and other aspects [5]. The next generation mobile networks (NGMN) showed concerns about aspects of user authentication, user privacy protection, network security, and other aspects within their white paper [6]. Furthermore, the European Telecommunications Standards Institute (ETSI) organized 5G security seminars in June 2017, to emphatically discuss NFV Network security monitoring, management, and security problems in practical application[2)].

China also deployed security technology research at the beginning of 5G studies. In 2014, the FuTURE Mobile Communications Forum released the first Chinese 5G technology white paper[3)], which summarized the direction of security technology research from the perspective of air interface security, network security, application security, and network security. Subsequently, the National High-Tech R&D Program (863 Program) began implementation of the second phase of the 5G major project, and established a 5G network security mechanism research topic named "future wireless access physical layer and system security communication technology research" in January 2015. In 2017, National Science and Technology major projects known as the "New Generation Broadband Wireless Mobile Communications Network" established a project called "5G Security Overall Architecture Research and Standardization". Furthermore, the China Communications Standards Association (CCSA)[4)] TC5 WG5 and TC8 WG2 mainly relate to domestic 5G security standardization studies and work relating to docking in accordance with international standards, and provide several panel discussions on 5G security threats, security requirements, and solutions. In 2016, the CCSA proposed "5G Security Technology" as a research subject [7], and set up an industrial standard project named "5G Security Technology Requirements" in 2017 [8], which aims to promote Chinese 5G security standardization work.

The IMT-2020(5G) Promotion Group is a 5G technology research and promotion organization that is dominated by China. Many leading companies and research institutes have been recruited to pro-

1) ITU-T. http://www.itu.int/md/T13-SG17-160829/sum/enen.
2) ETSI. http://etsi.org/etsi-security-week-2017/5g-security.
3) FuTURE Mobile Communication Forum. http://www.future-forum.org/.
4) China Communications Standards Association (CCSA). http://www.ccsa.org/.

vide domestic information in the communication field, including Huawei, ZTE, Datang Telecom, and China Mobile Research Institute. The IMT-2020(5G) Promotion Group released the latest version of the 5G white paper "5G Network Security Requirements and Architecture White Paper" in June 2017[5)], proposing its 5G security architectural design vision. From the time schedule and the study content, it is evident that current 5G security research in China is based on implementing standardization guidelines from international organizations.

Domestic and foreign enterprises are conducting 5G security technology studies and are participating whole-heartedly in its standardization work. For example, in June 2015, Ericsson released the white paper "5G Security: Scenarios and Solutions" [9], presenting a vision of 5G network security architecture, and stating that the foundations of 5G are security and privacy. In December 2015, Datang Telecom Technology Industry Group analyzed the three core elements of 5G network security (trusted identity, trusted Internet, and trusted entity) in "Building a Safe and Secure Cyberspace: 5G Network Security White Paper" [10]. In 2015, Huawei Technologies Co., Ltd. released "5G: Security Requirements and Principles Huawei White Paper" [11], which analyzed the new security requirements and challenges of 5G and proposed an overall vision of 5G security. In November 2016, Huawei also released the "5G Scenarios and Security Design" [12], in which they analyzed different security requirements and challenges of eMBB, mMTC, and uRLLC, the three application scenarios of 5G, and proposed differentiated security abilities, strategies, and solutions. In December 2016, at the "2016 Future Mobile Communications Technology Summit", Nokia and Shanghai Bell stated that 5G new security solutions need to meet three basic requirements: robustness (where viability must be enhanced); flexibility (where different security requirements can be satisfied with different security mechanisms and solutions); and adaptive arrangements and management. In June 2017 at the security seminar organized by the EISI, Huawei summarized the security challenges for NFV and summarized security challenges, security control, the architectural model, and security model design; and Nokia introduced 5G security architecture elements from the perspective of 5G cloud environment deployment, including SDN security, NFV security, and network slicing security [13]. Although domestic and foreign enterprises are independent from each other, and they have their own features and advantages, together they form a complete 5G safety research ecology that is complementary and supportive.

3 5G security requirements

Overall, 5G requires the use of many new types of security, due to the new business applications, new architectures, new technologies, and new scenarios involved. In this respect, new business applications, which are represented by the Internet of things, pose unprecedented challenges to security [14], and open and shared network architectures, with cloud, virtualization, and pooling technology traits are expected to substitute closed-type network architectures entirely in traditional mobile networks, thereby bringing new security challenges that currently have limited security means to combat them [15]. The development and evolution of air interface technologies not only involve higher requirements of wireless secure transmission, but also create better conditions to fundamentally resolve information leakage problems due to the openness of wireless broadcasts [16]. Finally, the diverse scenarios applied in 5G will make it more difficult to provide adequate user privacy protection [17].

3.1 Security requirements of new business applications

5G needs to use protection mechanisms in accordance with different security requirements for the three application scenarios, eMBB, mMTC, and uRLLC [18], where eMBB focuses on businesses that have a high demand for bandwidth and user experience such as HD video, virtual reality, and augmented reality, and each business has a different security protection strength requirement [19]; mMTC focuses on high-density scenarios, such as smart traffic, hydrological monitoring, and smart meters (terminals have energy consumption limit characteristics, topological dynamic changes, and are data centric; therefore,

5) IMT-2020(5G) Promotion Group. 2017. http://www.imt-2020.cn/zh/documents/1.

lightweight security algorithms and efficient security protocols are required [20, 21]); and uRLLC focuses on communication services with low latency and high security, such as real-time medical services, vehicle networking, and automatic industrial control (which need to ensure high-level security measures without adding additional communication delays of identity authentication, data encryption and decryption, or security context transmissions [22]).

In addition to mMTC and uRLLC, networks need to support a connection density of 1 million/km^2 with an end-to-end delay of less than 1 ms, which means that huge numbers of nodes will be joining and exiting the network at the same time. Communication nodes have characteristics of a dense distribution, high concurrent communication, low communication delay, and dynamic migration. The network will be confronted with many problems, such as the real-time generation and management of key distribution between massive communication nodes, which also brings new challenges to providing security for traditional wireless communications [23–26].

In summary, use of 5G involves massive access nodes, low latency, high reliability, and node dynamic access and exit. In addition, computational resources and sizes and power consumption are limited, and there are thus extreme challenges to providing 5G security. However, studies exploring 5G endogenous security mechanisms are moving in a promising direction.

3.2 Security requirements of new network architecture

Traditional mobile network security relies mainly on a relationship built on trust between communication equipment and communication networks. However, as communication equipment is the irreplaceable core function execution entity that tightly couples hardware with software, hidden backdoors and political considerations are often important factors that need to be negotiated in the game of trust. Traditionally, the trust relationship with respect to communication networks is based on a closed-operation network environment. Together with the flourishing development of the mobile internet, network integration and openings are inevitable development trends. As such, it is difficult to maintain the traditional trust relationship because many serious and wide-influencing loopholes have now been uncovered [15, 27].

SDN/NFV technologies are introduced into new 5G network architectures, thereby decoupling the control and data planes of the equipment [28, 29], which creates favorable conditions for building new device trust relationships based on general IT hardware platforms from multiple manufacturers. The concept of being more open, and cloudy/pooling architecture designs also promote many security challenges [15,27,30]. In addition, security boundaries and protection modes in the traditional closed management mode are undergoing profound changes, and the openness of a business, the user's customization, and the ability to visualize the application of resources bring unprecedented challenges to providing security and credibility to cloud platforms [31]. Furthermore, the sharing of computing, storage, and network resources introduces problems, such as virtual machine security, the security of virtualization software, and data security [32]. Finally, due to centralized deployment, common hardware causes viruses to spread rapidly in the centralized deployment area, and hardware loopholes can be more easily detected and exploited by attackers [33].

In summary, 5G characteristics, including the general hardware platform, the open source software platform, network function virtualization, and unified orchestration and management of resources will cause an increasing number of previously unseen security threats, and traditional protection modes based on the prior knowledge are not suitable for use with 5G development. It is therefore necessary to make full use of the advantages of 5G network architecture, including software and hardware decoupling, virtualization, and dynamization, and to excavate endogenous security properties and develop endogenous security key technologies to build a high reliable and secure 5G network based on untrusted network components.

3.3 Security requirements of new air interface technology

Cryptographic technologies employed in 2G, 3G, and 4G are implemented at upper layers and ignore the securing of wireless broadcasting signals on the air interface, which causes severe threats to wireless

communication security that emphasize the content encryption but neglect the signal hiding [34].

It is expected that 5G will have a broader bandwidth, a denser number of users, lower latency, and that it will provide more reliable transmission [35]. However, to ensure that the key performance indicator (KPI) requirements grow at the correct orders of magnitude, it is necessary to design a secure mechanism to provide high level security without affecting network performance [36,37]. This mechanism is expected to be independent of computational complexity, to be flexible with respect to load regulation, and to suit different application scenarios.

In the traditional authentication and data integrity protection mechanism (e.g., AKA, EPS AKA), the principal approach used to prevent signal-based wireless attacks (such as message tampering, impersonation, man-in-the-middle, and replay attacks) is to tag the signaling and data with user identity information determined by an identity key [38,39]. However, authentication data is invalidated once the identity key is compromised or exposed, enabling attackers to eavesdrop on the authentication process and derive subsequent session keys, thereby threatening the security of the network. Subjected to the contradiction between the data rate and computational complexity, current mobile networks lack appropriate solutions to tackle the protection problem of ensuring the integrity of business data because of the rapid and sustainable increase in the mobile communication rate [37,40–42]. Therefore, it is necessary to urgently develop defense methods that can quickly determine and resist active attacks launched by attackers from unknown locations in typical 5G scenarios that can also satisfy multi-level security requirements in different communication scenarios.

3.4 Higher security requirements for user privacy

In addition to all the user privacy data relating to traditional networks (subscriber information, location, trajectory, communication content, communication behavior, communication relationships, and account number), 5G carries further privacy data, such as personal data relating to different industries (health information, service types, and service content) and industry users' privacy data (such as mechanical and production controls). These data tend to have higher sensitivity, which raises new challenges for preserving user privacy [7].

As a complex ecosystem, the 5G network will be used by many types of participants, including infrastructure providers, mobile communication network operators, and virtual operators. The storage, transmission, and processing of user data within a complex network composed of multiple access technology, multi-layer networks, multiple devices, and participants interacting with each other may lead to user privacy data being scattered in every corner of the network [17]. In addition, with respect to the spread of privacy data, data mining technology will enable third parties to analyze a greater amount of user privacy information [43]. In addition, although the introduction of virtualization technology in 5G networks brings flexibility, it will make network security boundaries more obscure [44]. User privacy data will be more vulnerable to attack, particularly with respect to multi-tenant sharing of computing resources [9]. Therefore, compared to traditional networks, the influence from the leakage of privacy in a 5G network will be wider and more harmful [45].

Therefore, enhanced protection of user privacy needs to be designed in the 5G network to protect users' sensitive information from being leaked in the progress of storage, transmission, and access.

4 5G security architecture

In summary, 5G requires a considerable amount of security for new application scenarios, new network architecture, new air interface technologies, all of which are radically different from those in the existing 4G network. In particular, security is required to authenticate massive equipment, provide high availability, low latency, low energy consumption, and other changes brought by IoT application scenarios. The introduction of SDN/NFV, virtualization, mobile edge computing, and other new technologies also brings certain changes and security risks. However, the existing 4G network security architecture and security key technologies cannot solve these new security issues, which poses new challenges for 5G security

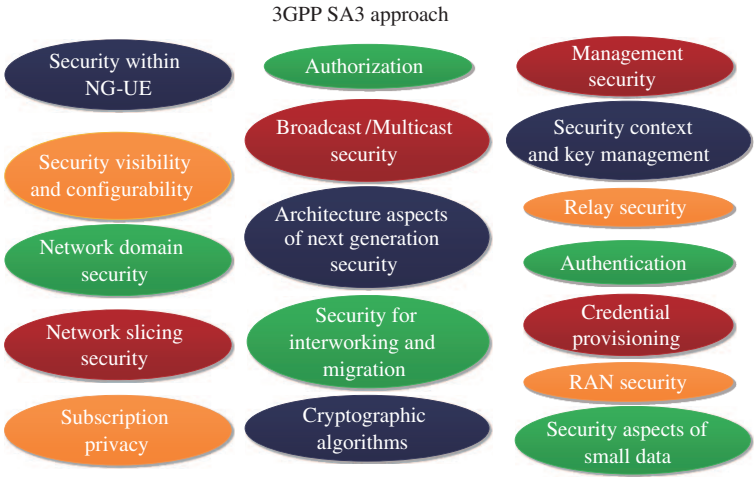

Figure 1 (Color online) The security area.

architecture design, not only with respect to solving security issues brought by multi-application scenarios and new technologies, but also with respect to providing differentiated security mechanisms for different scenarios. 5G security architecture needs to support multiple application scenarios and include a unified authentication framework, service certification, network slice security, and user privacy protection. In addition, security function instances need to be initiated and terminated flexibly, to provide differentiated security services to different services.

The 3GPP Working Group, SA3, is responsible for 5G network security architecture design, and has determined that security architecture design should consider the areas shown in Figure 1 [1].

Based on these design principles, 5GPP [5], ETSI, China's Future Mobile Communications Forum, the IMT-2020 (5G) Promotion Group, Ericsson (Ericsson) [9], Nokia [13], the Datang Telecom Technology Industry Group, Huawei Technologies Co., Ltd. [11,12], and other domestic and foreign enterprises have proposed their respective security architecture designs.

In summary, the solutions above are much the same in the capability logic function level of 5G security architecture; they basically follow the functional logical framework of 4G security architecture. It is also necessary to provide solutions for solving security issues with respect to the architecture, and to change security boundaries and separate the control plane from the forward plane. Furthermore, flexible security mechanisms need to be designed that fit the slice network, and which reserve resources and scalable interfaces for special and emergency scenarios, and which provide alert and defense mechanisms for big data security. In this respect, at the capability deployment level of 5G security architecture, although a variety of innovative ideas have not yet been converged, endogenous security has become a remarkable development trend.

4.1 Logic architecture for 5G security capability

To enable a differentiation protection mechanism between the user plane and the control plane in 5G security, and to support data security protection, embody a unified authentication framework, provide service authentication, fulfill the openness of capabilities, and support the protection mechanism for both slices and applications security, a 5G security architecture was proposed by the China IMT-2020 (5G) Promotion Group in June 2017 from the viewpoint of user equipment (UE), access network, serving network, home environment, and service applications. There are eight major domains for this 5G security architecture, as shown in Figure 2, as follows: (1) network access security: security of user data should be guaranteed and this includes confidentiality and integrity of both signaling (i.e., signaling in both the access network and the core network) and user data between the UE and network in control plane (CP)/user plane (UP); (2) network domain security: the secure exchange of both signaling and user data between different network entities, including RAN and service network public nodes, service

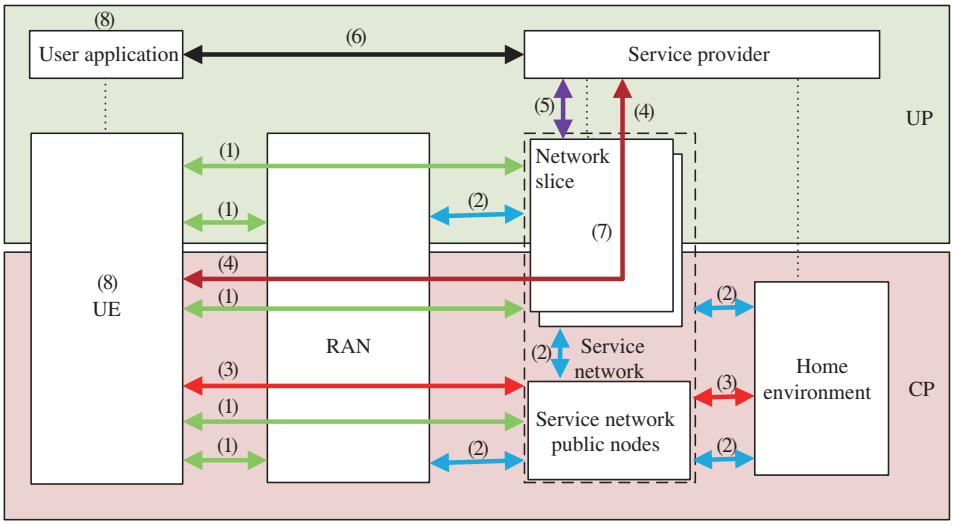

Figure 2 (Color online) 5G security architecture proposed by China IMT-2020 (5G) Promotion Group.

network public nodes and home environment, service network public nodes and network slices, and home environment and network slices; (3) initial authentication and key management: various mechanisms for authentication and key management should be included that embody the unified authentication framework, including operator-security-credentials based security credential authentication between UE and 3GPP networks, as well as the key management of user data protection after successful authentication; (4) re-authentication and key management: service authentication and relevant key management between UE and the external data network (i.e., service provider); (5) security capability openness: the openness of security capability between the 5G network entity and external service provider should be supported; (6) applications security: secure communications between UE and the service provider should be supported; (7) slices security: the security of slices should be guaranteed, including authorization and isolation; (8) security visualization and configurability: both the execution state of security characteristics and the capability of security characteristics to guarantee service security should be perceived. In conclusion, the first six domains describe the security requirements between different components, while the last two security domains (slices security, and security visualization and configurability) describe the security requirements of the network slice and the user equipment/user application themselves.

Compared with Figure 1, it can be concluded that the China IMT-2020 (5G) Promotion Group conducts 5G security architecture design from the perspective of realization, while 3GPP Working Group SA3 studies 5G security architecture design from the perspective of theoretical specification and guidance. The specific research contents in Figures 1 and 2 are essentially consistent, as all the specific research contents in Figure 1 can be found inside the eight domains presented in Figure 2.

4.2 Deployment architecture for 5G security capability

With respect to 5G security capability deployment levels, the current development trend is based on 5G security architecture that combines 5G network features of clouds, pooling, and virtualization to explore the mechanisms and deployment framework of endogenous security. This is also the current research focus of industry. In consideration of 5G security requirements and the system endogenous security mechanism, it is necessary to exploit endogenous security elements from the perspectives of the air interface and ground networks to develop new defense mechanisms. Furthermore, 5G endogenous security deployment architectures should be proposed, and research should focus on physical layer security, lightweight encryption, network slice security, mimic defense, user privacy protection, block chain, and the other key technologies that can be applied within the 5G network (as shown in Figure 3), to form a high-performance, high-confidence, integrated technology solution that defends against both known and unknown security risks and threats.

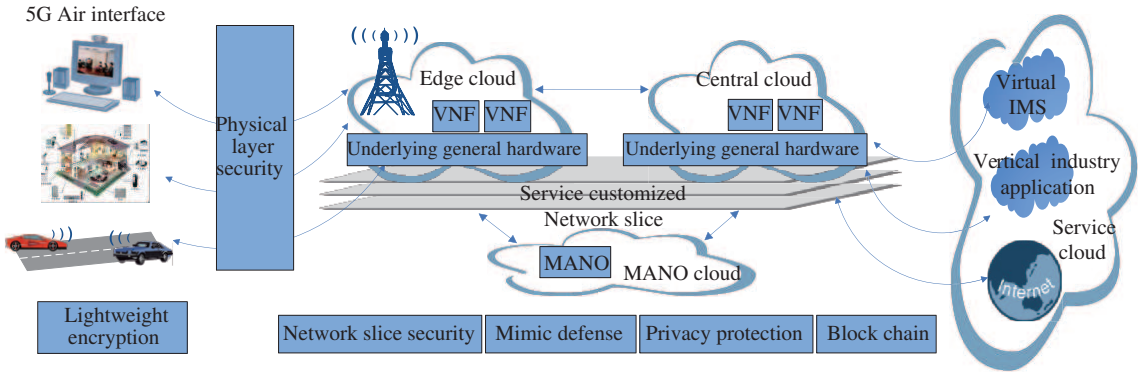

Figure 3 (Color online) 5G network endogenous defense security architecture.

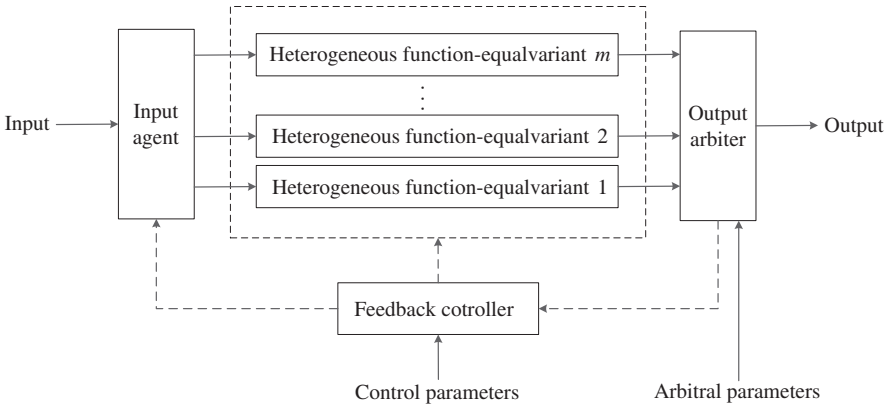

Figure 4 Abstract model of the mimic defense system.

From the perspective of the 5G security capability deployment level, a particularly noteworthy and typical architecture is that of the mimic defense system. Mimic defense [46, 47] is an active defense theory that was created by the Chinese Academy of Engineering, Wu Jiangxing academic team. It provides universal innovative defense theory and cyber space methods to deal with unknown vulnerabilities, back door viruses, Trojans, and other unknown threats in different areas within the relevant application level [48, 49].

An abstract model of the mimic defense system is shown in Figure 4, wherein the heterogeneous function-equal variant represents facilities with different levels and granularities, such as the network, platform, system, assembly unit, components, software implementation, hardware implementation, and the combined implementation of software and hardware.

To enable reliability and availability, the mimic defense system is suitable for use in situations that have both traditional and non-traditional security requirements. It needs the following conditions to be satisfied prior to application: (1) a standardized functional interface and protocol specification, (2) a functional input-output relationship, (3) possibility of being determined using a compound and consistency test, and (4) technical conditions of being processed multivariable or divertible.

The use of virtualization technology (in particular, newly-developed virtual container technology) can economically and flexibly set the mimicry scene to support the demand of diversified defense environment, which thus provides a very convenient condition for realizing a mimic defense mechanism, as shown in Figure 5.

Introducing the virtualization technology into the mimic defense scheme can enable implementation of a dynamic and randomized running environment. For example, the virtual container can support physical (logical) separation and partition of a heterogeneous and redundant function module, with the

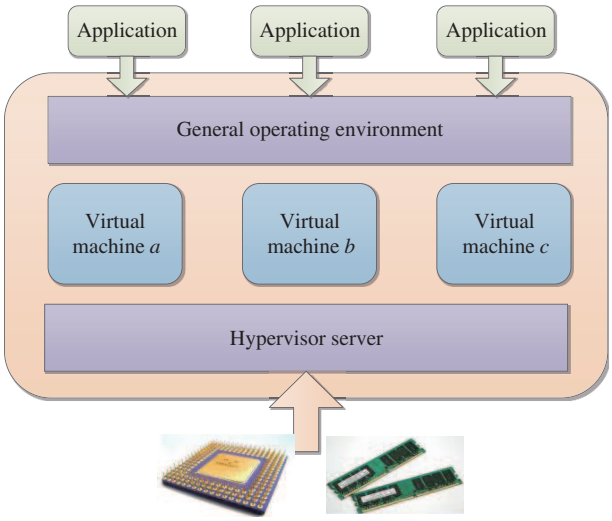

Figure 5 (Color online) Sketch map of virtual mimic defense scheme.

aim of managing and controlling the data and service functions. Meanwhile, through application of the virtual container, dynamic resource deployment and configuration can be achieved, and flexibility and utilization of resources can be improved. In terms of reducing the operating cost of the mimic situation, the virtualization scheme plays a significant role in declining the amount of physical modules and in screening the inner complexity, automatizing centralized management, simplifying the recovery process, and synchronizing operations, as well as enabling seamless migration of a multi-platform and cross-platform service.

The 5G core network using SDN/NFV-based open cloud architecture realizes the decoupling and separation of system function and hardware entity and provides unified scheduling, management, and controlling mechanisms for computing, storage, and communication resources, as well as providing the possibility of configuring dynamic heterogeneous resources. This naturally fits the concept of mimic defense. Therefore, the idea of mimic defense can be incorporated to establish 5G network endogenous defense security architecture. With the introduction of the functionally equivalent heterogeneous execution body in the network, a high security mimic defense system can be constructed based on a low-trusted infrastructure, thereby realizing the 5G network endogenous security mechanism and facilitating integration and design of network security and network services. An envisaged 5G network mimic defense system is shown in Figure 6; the entire system adds a mimic platform layer between the virtual layer and the application layer in the general 5G cloud service architecture, and also adds corresponding mimic scheduling management functions. The main added contents include: (1) a mimic platform layer that includes mimic proxy, feedback control proxy, scheduling proxy, resource monitoring, implementation of mimic virtual machine deployment, run-time monitoring, and information feedback; (2) a heterogeneous image library and management, generation, and registration of the heterogeneous image library, in addition to management of heterogeneous image modules for application-oriented virtual proxy, arbitrament and executable, respectively; (3) a mimic feedback controller consisting of a redundant controller, a heterogeneous controller, and a mimic interface controller, which is responsible for the corresponding security level requirements; (4) a mimic scheduler that includes the scheduling mechanism and cleaning strategy for receiving the mimic feedback controller instructions, and operating the mimic virtual machine dynamically based on the security strategy.

5 5G security key technologies

The 5G overall security architecture is supported by security key technologies. 5G's new business applications, new network frameworks, new air interface technologies, and higher user privacy security re-

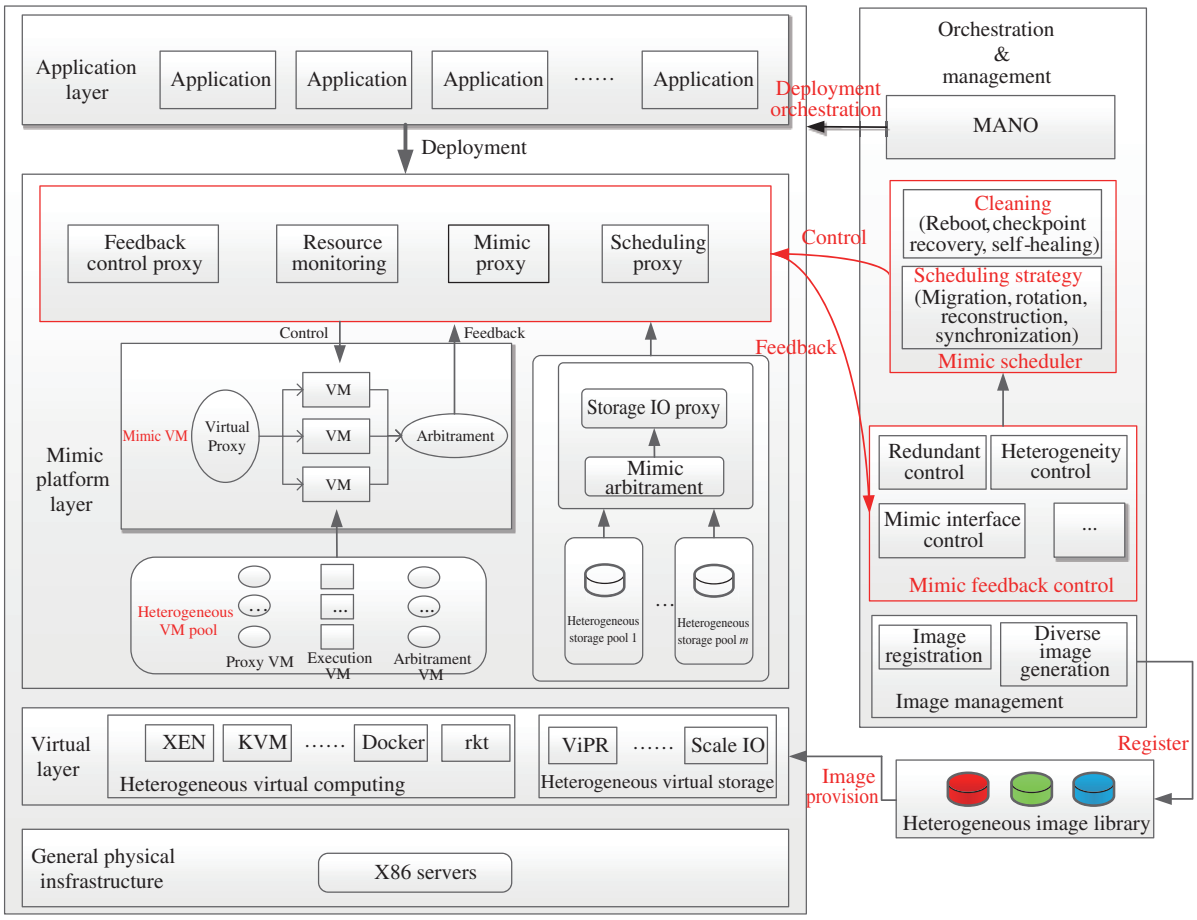

Figure 6 (Color online) 5G network mimic defense architecture.

quirements have also promoted the evolution and development of safety key technologies. The 5G eMBB scenario follows 4G end-to-end encryption algorithms such as AES, SNOW 3G, and ZUC. However, with the gradual maturity of quantum computer technology, AES, SNOW 3G and ZUC cryptographic algorithms using 128-bit key length in 4G will face security threats. Based on this, 3GPP SA3 has initiated the discussion of using a 128-bit key length and 256-bit key length symmetric cryptographic algorithm in 5G networks. AES and SNOW 3G natively support 256-bit key lengths. At present, the IMT 2020 (5G) promotion group is also conducting related evaluation of the ZUC-256 (256-bit key length) cryptographic algorithm, and actively promotes the ZUC-256 cryptographic algorithm to become an international standard. In the mIoT scenario, due to the limited security space provided by the device, algorithms such as AES, SNOW 3G, and ZUC cannot be effectively applied, and a lightweight algorithm needs to be introduced.

Overall, multi-domain, diversified, high-grade and lightweight security needs require multiple security measures and technologies to achieve. Next, the air interface physical layer security technology, lightweight encryption technology, network slice security technology, 5G user privacy protection technology and blockchain technology that are closely integrated with 5G new service applications, new network architectures, and new air interface technologies are introduced in detail.

5.1 Physical layer security with air interface

The use of physical layer security [50–52], which exploits the diversity and variability of wireless channels and the uniqueness and reciprocity of channels in legitimate communications, can be explored using the endogenous wireless communication security mechanism based on the characteristics of wireless propagation. Certain new air interference technologies adopted in 5G, such as massive MIMO, high frequency,

and large bandwidth communication, make it more convenient to extract security elements from wireless resources and to contribute to the application of physical layer security [53]. In addition, these security mechanisms are naturally based on communication processes and signal processing technologies and will evolve synchronously with the new air interface technologies in 5G.

Physical layer secure transmission technology, physical layer authentication technology, and physical layer key generation technology are three important research directions being conducted in physical layer security [16]. The methods used to employ endogenous security elements brought by 5G new air interface technologies to enhance these three technologies will be the major development trends in physical layer security [54]. Physical layer secure transmission technology, which utilizes significant differences between wireless channels created by 5G new air interference technologies to design signal transmission and processing mechanisms that are strongly associated with the location, can generate a private transport pipeline and achieve "physical isolation" in wireless communications [55]. In physical layer authentication technology, authentication parameter generation methods are studied from the signal perspective, and the authentication parameters are bound with the signal transmission path and channel characteristics. Therefore, the traditional identity and information authentication are transformed into channel authentication and new channel authentication mechanisms can be designed. Physical layer key generation technology employs the private channel characteristics of both communication sides to extract "fingerprint" features. It enables real time secret keys without key distribution to be obtained and to approach one-time pad communications [56–60]. These three technologies are interrelated with each other and form the unified entirety of physical layer security.

5.1.1 *Wireless channel characteristics based on secure transmission technology*

The "fingerprint" of wireless channels implies that they are strongly dependent on the spatial locations of transmitters and receivers. Based on 5G typical application scenarios and new air interface technologies, physical layer secure transmission technologies propose to convert the differences between wireless channels from different locations into an SINR difference. By applying signal processing methods, including artificial noise, MIMO beamforming, collaborative jamming, secrecy signal zero-forcing, and security coding, physical layer secure transmission technologies can enlarge the differences between wireless characteristics so that target users can demodulate signals while illegal users at other locations receive topsy-turvy signals and are unable to recover the information. Recently, many studies have applied physical layer secure transmission technologies into varied communication networks, such as heterogeneous cellular networks, cooperative relaying networks, D2D networks, massive MIMO networks, millimeter wave networks, and NOMA networks.

Wang et al. [61] and Lv et al. [62] designed artificial noise and MIMO beamforming to enhance the security of heterogeneous cellular networks. Dong et al. [63] and Zheng et al. [64], respectively exploited the spatial freedom degree of multi-relay in a collaborative relay network, and proposed the collaborative relay jamming scheme. Zhang et al. [65] and Chi et al. [66] studied a method to enable cooperation between D2D users and cellular network users, with respect to spectrum sharing and competition, to improve network security performance. In addition, Deng et al. [67] studied physical layer security gain based on the massive MIMO zero-forcing precoding technique in heterogeneous cellular networks. Furthermore, Zhu et al. [68] proposed a matched filter precoding and artificial noise scheme based on massive MIMO in multi-cell cellular communication, and analyzed the influence of different system parameters on network security performance. Zhu et al. [69] studied the influence of channel estimation and pilot contamination on the secrecy performance of massive MIMO network, based on the work of [68]. Kapetanovic et al. [70] showed that pilot contamination attacks seriously reduce the safety performance of massive MIMO networks and that they are difficult to detect. In order to enhance the network security of millimeter-wave communication network, Wang et al. [71, 72] proposed an analog beamforming scheme, which placed artificial noise into the orthogonal space of confidential signals based on the high directionality and narrow beam of millimeter-wave. The high directionality of the millimeter wave beam provides gains for physical layer security, but simultaneously causes the network to be more sensitive to beam alignment [73]. Qin

et al. [74] and Liu et al. [75] utilized natural interference caused by the non-orthogonal of the NOMA network, to decrease the received signal quality of the eavesdropper and improve the secrecy performance of the NOMA network. The NOMA network utilizes overlapping of the power domain and continuous interference cancellation techniques to cause effective interference for external eavesdroppers, but it cannot effectively resist the security threat of internal eavesdroppers. In addition, the security of NOMA network is susceptible to the effect of continuous interference cancellation. Islam et al. [76] researched the potential and challenges of enhancing physical layer security in NOMA networks.

In summary, in consideration of the new air interface technologies adopted by 5G, there are both opportunities and challenges in the development and evolution of physical layer secure transmission technologies that employ different wireless channel characteristics, and as such, these need further study.

5.1.2 *Physical layer authentication*

The basic principle of physical layer authentication is to add wireless channel characteristics that are strongly coupled with users' locations as new authentication parameters within traditional identity-based authentication. A "position stamp" is thus added onto user identity information, signaling, and data, which further expands the dimension of authentication security using spatial spectrum elements. It is feasible to build a double reinforced inherent security defensive system for the 5G system by combining it with traditional authentication mechanisms to effectively detect and resist wireless attacks from abnormal locations. Existing research on physical layer authentication mainly focuses on three aspects: channel fingerprints based physical layer authentication, challenge-response based physical layer authentication, and cross-layer authentication, which are presented as follows.

Channel fingerprints based physical layer authentication was first proposed by Patwari et al. [77] in 2008 and uses unique wireless channel characteristics decided by a user's location as a fingerprint to identify the user. Consecutive channel characteristics of successive data packets are then compared to determine whether the wireless link has been changed, and this further verifies the legitimacy of the user according to the channel correlation coefficient [77]. In the same year, Xiao et al. [78] demonstrated the feasibility of employing channel fingerprints to achieve authentication. In recent years, channel fingerprints based physical layer authentication has also been considered extensively in 5G new communication scenarios and wireless technologies. In [79,80], application of channel fingerprints based physical layer authentication was studied in the MIMO system and IoT system, respectively. Another study [81] analyzed the challenges of introducing such an authentication mechanism into the terahertz network, and further designed corresponding methods according to specific channel characteristics. In addition, to simplify the authentication procedure and reduce handover authentication latency and complexity, studies [82,83] applied channel fingerprints based physical layer authentication into SDN-based heterogeneous network, by extracting the channel characteristics as security context information.

Challenge-response based PLA was firstly proposed by Shan et al. [84] of the University of Michigan, using a challenge-response mechanism. Channel characteristics are exploited to mask the authentication challenge and secret key, with the aim of generating an authentication response. Only the legitimate node with the same channel can extract similar channel characteristics, and further recover the authentication response. This idea was also extended to the relay scenario in [85]. Wu et al. [86] also designed a similar approach to achieve physical layer authentication, where the wireless channel phase information is extracted to hide the key. To cope with the threat of channel characteristics being easily obtained by attackers in a slow-varying environment, the authors further proposed to inject artificial noises into the channel fingerprints to increase the randomness of the received signal, preventing attackers from forging [87]. To solve the problem of key leakages, Ji et al. [38] proposed to employ a fault-tolerant hash function at the physical layer to bind channel characteristics and the identity key. Even if channel information is obtained by attackers, they would be unable to irreversibly recover the secret key. The research group also used the National 863 Project to design a dual-authentication scheme, which involved combining identity and channel authentication to provide authentication and integrity protection for signaling in the control plane and business data in the user plane, thus preventing wireless attacks from

unknown locations.

To achieve enhanced authentication, cross-layer authentication combines physical layer authentication parameters and upper-layer authentication by enabling the interaction of information between the physical layer and upper layer. Wen et al. [88, 89] combined upper layer authentication and physical layer authentication to achieve cross-layer authentication in 5G vehicular networks, ad hoc networks, and intelligent meter systems. Wu et al. [90] embedded the physical layer authentication mechanism into the upper-layer AKA authentication to form a new security mechanism with double reinforcement in. To provide a closed protection tunnel for the transmission of AKA authentication data, another study [91] combined the physical layer authentication in [38] and the AKA mechanism, which improved the entropy of authentication information and security increments without introducing changes to the traditional authentication process.

5.1.3 *Physical layer secret key generation mechanism*

Physical layer based secret key generation is guaranteed by the intrinsic safety characteristics (i.e., randomness, time variation, and reciprocity) of the wireless channel. Specifically, the random wireless channel between legitimate transceivers provides common randomness, the time variation quality enables fast updates of the secret key, and furthermore, the reciprocal characteristics make it much easier to distribute and manage the secret key. This idea provides the foundations for physical layer secret key generation from the 5G air interface, which subsequently assists in achieving unconditional security from the perspective of information theory.

To distribute and manage the secret key among massive terminals, Maurer [92] first proposed a method to generate the secret key from common random information. Specifically, to distill strongly correlated information, the legitimate transceivers treat the shared common randomness as the source of the secret key; the consistent secret key is then extracted after completing the agreement procedure in the noiseless private channel. Based on this method, Ahlswede and Csiszar [56] proposed a basic model for wireless channel based secret key generation with noise considered. Aono et al. [58] studied the secret key generation method based on partially universal channel characteristics, the received signal strength index (RSSI), and evaluated the secrecy performance according to statistical results. Sayeed et al. [59] studied secret key generation from the channel impulse response (CIR). Jin et al. [93, 94] deduced a closed-form solution to the channel based secret key capacity over the uniform scattering environment, and also investigated the secret key capacity utilizing periodic sampling of the wireless channel. These results can all be utilized to quantitatively analyze factors such as the time difference of channel sampling, velocity, and additive noise, which affect the capacity of the secret key. In essence, these methods treat the wireless channel within the coherence time as different responses of different input signals in a linear time invariant system.

To improve the secret key generation rate, legitimate transceivers can explore ample degrees of freedom from multiple antennas. Therefore, 5G massive MIMO can radically increase the secret key generation rate [95, 96]. In 5G cooperative relay scenarios, the increase of both the cooperative nodes and antenna separation provides channel variations that are much richer. Lai et al. [97] utilized the channel between legitimate transceivers and relays as compound common randomness to generate the secret key. It was further demonstrated that the secret key rate grows linearly with an increase in the number of nodes. Wang et al. [98] investigated the secret key agreement scheme with three cooperative nodes and derived the upper and lower bound of the secret key rate. Furthermore, Chen et al. [99] investigated secret key generation in LTE-A networks.

These investigations provide possible solutions for the construction of secret key generation approaches in more practical communication scenarios.

5.1.4 *Current standardization situation*

From 2012, the EU Framework Program 7 (FP7) established PHYLAWS, DUPLO, PROPHYLAXE, and many other projects for research into physical layer security, with the main focus on investigating the

physical layer secure access mechanism on the air interface in mobile communications. Many outfield tests have been conducted with respect to these projects, using physical layer security technologies for 2G, 3G, 4G, WLAN and other communication systems [100].

For 5G physical layer security technology standardization, Celeno jointing VTT, Thales, Telecom Paris Tech, Imperial College, and many other enterprises and research institutions proposed two standards, in ITU-R66 and WRC-19d, respectively, for improving reliability and privacy within wireless communication [101] and security of the Internet of things [102]. In addition, Thales submitted three proposals to the SA3 working group of 3GPP: generation of a session key or temporary key using wireless channel features [103], generation of the link identifier instead of IMSI [104] and using the wireless channel, and developing network security architecture [105] based on physical layer security. In 2017, the CCSA proposed physical layer security research topics for the first time, with the aim of further standardizing the development and evolution of physical layer security technology in mobile communications networks.

5.2 Lightweight encryption

IoT is a critical application scenario in the 5G network and its security issues cannot be ignored. IoT nodes usually have limited hardware and signal processing abilities, limited memory storage, a compact overall dimension, and strict power constraints. Thus, a lightweight secure communication mechanism is preferred at IoT nodes, and lightweight security mechanisms need to be designed in consideration of such characteristics. From the perspective of traditional cryptography, it is possible to optimize the structure of existing encryption algorithms in terms of storage, hardware resources, and computational complexity, or to design a new lightweight cryptographic algorithm based on grouping, sequence, and hash. As such, resources and power costs can be reduced without degrading the security performance. In addition, it is also possible to employ the endogenous security property of the wireless channel to introduce new security elements that cannot be measured, restructured, or copied. Through the integrative design of security and communication, it is possible to achieve lightweight security without reducing the communication efficiency, particularly for massive access, small data transmission, and low delay scenarios.

5.2.1 *Lightweight encryption algorithm*

Hardware platforms have limited resources, and it is thus difficult to directly implement common symmetric cryptographic algorithms (such as AES and SHA-1) in IoT scenarios. Encryption algorithms may also be strictly limited by the performance of ROM, RAM, and the processor when implemented using software. The massive storage and computation costs both increase energy consumption and reduce the practicality of algorithms. Under these circumstances, an extensive amount of research into lightweight encryption algorithms is being conducted, and many have now emerged for use in different application environments.

In 2012, the American Bureau of Standard (ABS) formally promulgated the standard for lightweight encryption algorithms (ISO/IEC 29192) [106], in which Trivium, PRESENT, and CLEFIA were chosen as standards for lightweight sequence cipher and lightweight block cipher. Trivium is a lightweight block encryption algorithm that was designed by two famous cryptographers, Christophe De Canniere and Bart Preneel [107]. It is based on the idea of block cipher, uses three cascade-connected nonlinear feedback shift registers (NFSRs), and has a hardware cost of 2599 GEs [78]. PRESENT is a lightweight block encryption algorithm that was proposed by Bogdanov, a German researcher [108]; it has a hardware cost as large as 1570 GEs, but when utilized in a cascade way the cost can be optimized to less than 1000 GEs [79]. CLEFIA is a lightweight encryption algorithm designed by SONY Company [109]. The basic processing unit is as large as 128 bits, which accelerates the processing speed, and it can be used to complement PRESENT [80].

After 2012, cryptographers focused on problems such as low latency, the ability to resist side channel attacks, S-boxe optimization, and diffusion layer optimization. Several series of algorithms were then successively proposed, such as PRINCE, PICARO, Zorro, and PRIDE [110]. In 2013, NSA published two lightweight block encryption algorithms, SIMON and SPECK, for hardware and software implementation,

respectively [111]. Additionally, cryptographers from all over the world proposed several lightweight hash algorithms, such as Quark, PHOTON, SPONGENT, and GLUON [112]. In 2016, Bansod et al. [113] proposed an ultra-lightweight cipher named ANU, which is a 25-round lightweight cipher that supports 80/128 bits key scheduling. It only requires 934 GEs for 128 bits key, which is minimal compared to all existing ciphers. In addition, the design shows good resistance against basic and advanced attacks. Alshamsi et al. [114] designed a lightweight block cipher algorithm named LEA, which supports a key-length of 128/192/256 bits. The scheme supports flexible public key management through adopting identity-based encryption and does not require complex certificate handling. Furthermore, Peng et al. [115] proposed a lightweight, 8-round iteration block cipher algorithm for UANs communication based on chaotic theory and increased the key space by changing the numbers of iteration rounds.

In 2017, Win et al. [116] proposed a multi-receiver lightweight encryption scheme for device communications in IoT. Usman et al. [117] then proposed a lightweight encryption algorithm named SIT for use in IoT scenarios. The architecture of the algorithm is a mixture of the Feietel structure and a uniform substitution-permutation network; it provides substantial security in just five encryption rounds. In addition, Tahir et al. [118] proposed a novel searchable encryption scheme for client-server architecture. The scheme exploits modular inverse properties to facilitate searching over the secure inverted index table, which has the search function for encrypted data on the cloud.

5.2.2 *Lightweight security mechanisms for Internet of things*

Based on the wireless endogenous security mechanism, wireless channel "fingerprint" extraction and security enhancement technology not only meet security demands but can also reduce the expense of complex computing, key distribution, and management of the traditional cryptographic algorithm. Thus, they provide a promising solution for achieving high level and lightweight security within the 5G scenario, for example with mMTC and URLLC.

The PROPHULAXE project (2013.3-2015.8), hosted by Wunder, involved research conducted on physical layer security key generation for IoT nodes, where endogenous characters of the wireless channel were used to generate the shared key. In addition, new security architectures and physical layer security protocols have been proposed in IoT [119]. In their latest research, Wunder et al. [120] proposed a key generation method combining a random signal with the wireless channel, which has solved the problem of limited randomness of the wireless channel and a low-key generation rate under mobility limited scenarios. For smart wearable networks, the authors of [121] studied secret-key generation between sensors in the body area network, and verified that wireless channel changes rapidly with respect to movement of the body. Gungor et al. [122] extended physical layer key generation methods to vehicle networks, by generating a secret key from a fast-changing channel caused by the vehicle movement and protecting sensitive data (such as driving instructions and vehicle location) using the generated key. Wang et al. [123] extended the traditional TDD based wireless key security method to the FDD system; a key generation algorithm was proposed based on the reciprocity multipath angle and delay in the FDD system, which provided a solution for application of the wireless key security mechanism in FDD based NB-IoT. In consideration of the natural channel change in the heterogeneous and dense IoT being neither fast enough nor controllable, which leads to a low key generation rate and acts as an obstacle to meeting practical demands, Jin et al. [124] proposed a method combining a random signal and a secret key. Specifically, at the BS, the secret key is extracted from randomness of the channel and signal, while the security of the signal source is ensured by a secure transmission scheme. Simultaneously, the node side generates the key directly, based on the received signal.

In summary, the wireless endogenous security mechanism can achieve a fast secret key distribution and updating to reduce network signaling overhead, minimize delay, and provide a promising solution to secret key distribution and management with massive equipment. As such, it can satisfy the security requirements for lightweight realization at terminals in 5G IoT scenarios, provide highly efficient small data secure transmission, and offer integrity, confidentiality, and privacy protection.

5.3 Security of network slicing

Network slicing is a key feature of NFV applied to the 5G phase [125].

By using NFV technology, 5G network physical infrastructure resources could be virtualized into a number of independent parallel virtual network slices according to the needs of user cases; moreover, each slice could be custom-tailed to the network function, managed, and orchestrated using the corresponding network resource in accordance with needs of business scenarios and the business model. The network slicing instance can be regarded as an instantiated 5G end-to-end network architecture, where the operator can further segment virtual resources and create subnets when necessary.

The NGMN Alliance [126] analyzed the 5G network using network slicing technology, which may face security threats and own some security flaws, and listed 10 secure problems of concern for network slicing. These include (1) controlling communication between inter-network slices; (2) the instantiation time required for impersonation attacks against network slice manager or host (physical) platforms within an operator network; (3) impersonation attacks against a network slice instance within an operator network; (4) impersonation attacks against different network slice managers within an operator network; (5) different security protocols or policies in different slices; (6) denial of service to other slices; (7) exhaustion of security resources in other slices; (8) side-channel attacks across slices; (9) hybrid deployment models; and (10) sealing between slices when the UE is attached to several slices. Of these, the side-channel attack could be the most important problem, and it represents a security problem that cannot be ignored. It can be consider using two aspects of the test channel attack. The first simply relates to the isolation strength of virtual machines: observing or influencing how a code runs in one virtual machine should not allow an attacker to influence or deduce anything about how the code runs in another virtual machine on the same hardware. The second is to avoid co-hosting on the same hardware slices that have very different levels of sensitivity, or very different levels of vulnerability to influence by an attacker. For example, avoid co-hosting one slice that supports a particularly sensitive service and another slice that supports an application layer code being run on the same hardware.

With respect to the security of network slicing, 3GPP [127] will research this problem in two steps. The first stage involves consideration of key issues, such as securely isolating slices, having secure access to slices of the terminal, and providing the security of sensitive network elements. The second stage involves the use of independent security policies for slices, slice management security, and other key issues. In particular, the security requirements to enable isolation between network slices are proposed using a key-based solution. Although the same terminal can share the control plane key, different data plane keys are used in different slices. First, the terminal and the network are authenticated, and the security key system of the control plane is established following authentication. The entity responsible for the slice selection in the network then selects the appropriate slice for the terminal and requests SEAF (security anchor function) to generate a separate slice master key for the slice. In a low security level case, the security anchor function in the slice can use the master key to derive the various keys required for user plane encryption and integrity protection. When the security level is higher, the security anchor function in the slice interacts with the terminal and the third-party authentication authority to perform authentication and authorization of the terminal within the slice. It also uses key material provided by the third-party authentication authority to derive the slice master key and then further derives the various keys of user plane, thereby realizing the security of user plane within the slice without monitoring the operator.

China mobile, Huawei, Deutsche Telekom, and the Volkswagen group jointly issued a white paper on 5G service-guaranteed network slicing [128]. In terms of ensuring safety, the white paper focuses on the following three aspects of security, as follows. (1) Infrastructure security: as network slicing instances (NSIs) share the same infrastructure, proper isolation between NSIs must be enforced to avoid adverse cross-effects and information leakage, especially when the NFV (network function virtualization) is used. (2) Network management security: security risks exist in every phase of the NSI lifecycle management in the network management layer. Malicious attacks may use malware to compromise a network slice template, threatening all subsequent NSIs. Attacks may also pass through configuration interfaces during

the runtime phase of an NSI. However, confidential data could be obtained during the decommissioning phase, if the NSI is handled improperly. Therefore, security considerations should cover each single step of the lifecycle management of NSIs. (3) NSI security: to guarantee security for the network services provided by an NSI, it is necessary to embed the security mechanism and security provisioning entity (e.g., security anchors and security functions) into the logical network architecture of the NSI.

5.4 Privacy protection for user

In the research and standardization process of 5G network security mechanism, enabling user privacy protection is a primary and widespread concern. A number of specifications and research reports of the 3GPP relate to research on privacy issues. Of these, TR 33.849 [129] focuses on key privacy issues and methods of reducing risk; TR22.864 [130] relates to security requirements for contract data privacy; TR 22.891 [131] concerns user identity security; and TR 22.185 [132] focuses on the privacy needs of the Internet of Vehicles. NGMN showed that "endogenous privacy protection" should be a design principle within the 5G system. In addition, the 5G PPP project identifies 5G-Ensure privacy as one of the highest priorities of next-generation systems. CCSA also considers 5G privacy and security to be important and is conducting research in this respect. For example, contract data privacy and security content are included in "5G security technology" research topics [7], and the "5G security technical requirements" industry standard project proposal [8] includes three items on user data security research: privacy protection of identity, which involves signing by the user on a device; the secure storage and processing of signed documents and identity identification; and problems of confidentiality and completeness with user and signaling data.

An analysis of the content relating to 5G network privacy protection highlights at least three aspects that need addressing: (1) the traditional sense of user privacy data protection over mobile communication networks (for example, subscriber data, location, whereabouts, communication content, communication behavior, communication relations, and account number); (2) user privacy data protection in different industries (for example, the users' medical and health information, and sensitive information in the Internet of vehicles); and (3) critical data protection in sensitive industries (such as instruction data for mechanical and production controls). In addition, in consideration of threats to privacy data, research focusing on two aspects should be conducted on 5G privacy protection mechanisms and key technologies: first, the anti-leakage problem of privacy data in the procedure of provision, interaction, and use; and second, tamper-proofing, anti-destruction, and anti-theft problems relating to privacy data during procedures of storage, transmission, and use.

In the mobile communication network, industry is focusing on whether user identity can be effectively certified to protect user identity, location, and other privacy information from exposure to an unrelated network. From the earlier GSM to the recently commercial LTE mobile communication system, the wireless access network uses the temporary identity, TMSI, instead of the user's real identity identifier, IMSI, and encrypts transmission in wireless channels to protect the privacy of the user's identity information. However, there are still specific application scenarios that require the wireless channel to send IMSI as plaintext, and this problem has not yet been resolved prior to use with the 5G network. In the 5G standardization process, a relatively perfect user identity protection mechanism has been proposed in [4, 7]. The core idea of the related mechanism is to use the public key mechanism and transmit the encrypted user identity between the terminal and the user's home network, to ensure that the air interface and the service network do not leak the user's real IMSI.

The National Digital Switching System Engineering & Technological Research Center (NDSC) has proposed solutions with respect to the traditional meaning of user privacy data leakage problems in the mobile communication network. The core idea of the solutions is to adopt the active defense mechanism of "dynamic & hidden mapping," to effectively hide and dynamically change the association relation of user data, and to attempt to construct a dynamic, indefinite "user data association relation spectrum" in the uncontrollable communication process or communication device, so that user data can present characteristics of being incomplete, uncertain, unrelated, and unreal.

A considerable amount of research has also been conducted with respect to traditional user privacy protection, such as the use of user privacy data anti-leakage technologies in the release process, which includes data encryption technology, data distortion technology, and anonymous technology [133]. Typical anonymity methods include k-anonymity [134], l-diversity [135], t-closeness [136], differential privacy [137] and other methods.

In the process of data usage, location information is a key concern. The rise of the mobile location service (LBS) service provides a convenient way to query the users' location information, but security issues have caused widespread concern within the industry. There are three main ways to solve the LBS service location leakage: (1) restrict location information or the service attributes of a users' LBS query by establishing common privacy management rules and a trusted privacy agreement [138]; (2) modify or distort spatiotemporal information or service attributes before the LBS query is exposed to the LBS server so that the LBS server cannot obtain the exact location information or service attributes [139]; (3) use encryption technology to make the users' LBS query completely invisible to the LBS server, thereby achieving the purpose of privacy protection [140]. In addition, with rapid development of the mobile internet, a wide range of mobile application services have enabled the common leakage of user privacy information. Solutions for such privacy leakage have mainly focused on terminal vulnerability discovery and patches, such as the research on privacy protection technology for mobile application services based on the Android mobile terminal platform [141].

There are different privacy preserving requirements in the 5G network for different users, network elements, applications, and service scenarios. Therefore, the network is required to provide a differential privacy preserving ability and to exploit different technical measures to prevent user data leakage within the 5G network. In this respect, the content and scope of personal private information should first be clearly defined, and network entities and related operations that process and store private information should be explicitly revealed. Then, with respect to the air traffic, network, signaling interaction and application layer, the request, storage, transmission, and other manipulations of privacy information should be protected using technical and management measures that include data minimization, access control, anonymity, encryption protection, and user permissions [142].

5.5 Block-chain technology

There are huge numbers of massive entities within 5G cyberspace, the types of which are complex. In addition, the network environment is complex, and the virtual state and the physical state exist simultaneously. Therefore, it is necessary to determine how to realize the integrity protection of mutual information between the various network elements in a complex dynamic environment, and the non-repudiation of interactive behavior is a major challenge for the 5G network. Block-chain, is a distributed database that records all transactions from the genesis block to the current block of the block-chain and has characteristics of being decentralized, immutable, anonymous, and auditable. It is also able to provide solutions to the above challenges.

Since the block-chain was first proposed by Satoshi Nakamoto in 2009 [143], many companies and agencies have begun to study its application in the field of security. The Encrypto Telecom project is dedicated to developing encryption protocol for deploying block-chain technology, and establishing a decentralized system. Through blockchain-based secure communications infrastructure, it is possible to achieve privacy-oriented encrypted audio and video communication, new solutions for fraud management, identity as a service, and data management for the telecommunications industry, while building a secure network of the Internet of things for 5G[6]. NATO made an assessment of the use of block-chain technology in military applications, such as military logistics, procurement, finance, the Internet of things, and other military applications, with the aim of accelerating the application of advanced technologies, such as block-chain, to real-world solutions, and to support NATO C4ISR and network capability requirements. This assessment has now been submitted as a part of the 2016 innovation challenge[7]. The US Defense

6) Encypto Tel. http://ico.encryptotel.com/.

7) NCI Agency Innovation Challenge. https://www.ncia.nato.int/NewsRoom/Pages/160425_Innovation.aspx.

Advanced Research Projects Agency (DARPA) commissioned Galois to conduct research to build its block-chain application, guardtime keyless signature infrastructure (KSI), which verifies that the integrity monitoring system can build an unbreakable code form to improve key Weapon system security while KSI detects an advanced persistence threat (APT) hidden in the network [144].

Block-chain technology has attracted extensive attention in academic circles. Zyskind et al. [145] have proposed a decentralized personal data management system that ensures that users both own and control their data. Through the application of block-chain technology, signaling (which stores, queries, and shares data) is used as the ledger information (without a trusted third party) to achieve secure-access control management of data. Kravitz et al. [146] researched the privacy and security challenges of massive embedded devices, and used private chains to protect and manage these systems, thereby providing distributed management and flexible management of users and devices identity by satisfying basic needs (such as long-term, agile, and incremental adaptation). Lei et al. [147] proposed a new key management scheme for key transfer between security managers in a heterogeneous VCS (vehicular communication system) network, realizing secure transmission of the key by introducing block-chain technology. Furthermore, Cai et al. [148] proposed a trustworthy and private keyword search in encrypted decentralized storage to protect files and query confidentiality, while minimizing search latency.

Block-chain technology also has a broad application prospects in the area of the Internet of things. In 2015, IBM and Samsung conducted a cooperative project called ADEPT, and attempted to use block-chain as the underlying technology and apply it in applications of the Internet of things [149]. In 2016, IOTA, a new venture, also developed a new technology called "Tangle", to improve traditional block-chain technology applied to the Internet of things. In 2017, Alibaba Group, ZTE, China Unicom, and the Ministry of Industry announced that they would jointly build a block-chain framework specifically for the Internet of things, and together with the International Telecommunication Union (ITU) they aim to cope with problems of high connection costs, excessive concentration, uneasy expansion, network security vulnerabilities, and other issues inherent in IoT by block-chain technology. In September 2017, Tencent and the Wuxi High-tech Zone jointly announced the establishment of the TUSI Internet of things Joint Laboratory, and they are working together with Intel to develop block-chain technology. Progress has been made in the study of the Internet of things security, and FTSAFE, WATCHDATA, TENDYRON, and other intelligent hardware equipment manufacturers are also conducting research[8)].

6 Conclusion

A full range of future 5G security is required and will be based on more diverse application scenarios, multiple access methods, differentiated network services, and new network architectures, that provide high performance, high reliability, and high availability. In addition to providing inherent high-level security capabilities, future 5G security will also need to withstand known security risks and unknown security threats. At present, 5G standardization work has been fully launched, and 3GPP SA2 plans to complete the first version 5G technical standard formulation (Release 15) in 2018. It is thus necessary to clarify the security requirements of the 5G network as early as possible, and research on key 5G network technologies needs to be initially conducted. The endogenous security elements should be extracted from the network architecture and the electromagnetic propagation mechanism, and new defense mechanisms should be developed. Furthermore, if the security requirements of 5G are considered when the overall architecture, business processes, and algorithm in 5G are designed, we will be nearer the goal of building a more secure and reliable 5G endogenous security network.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grants Nos. 61521003, 61379006, 61471396, 61501516, 61601514, 61701538).

8) Tencent and the Wuxi High-tech Zone set up the first domestic TUSI Internet of Things Joint Laboratory. http://finance.sina.com.cn/roll/2017-09-10/doc-ifykuftz5907196.shtml.

References

1 3GPP SA. 3rd generation partnership project service and system aspects. http://www.3gpp.org/specifications-groups/

2 You X H, Pan Z W, Gao X Q, et al. The 5G mobile communication: the development trends and its emerging key techniques (in Chinese). Sin Chin Inform, 2014, 44: 551–563

3 Huang K Z, Jin L, Zhao H. Study on the security threat and protection technologies of 5G. Des Tech Post Telecommun, 2015, 6: 8–12

4 3GPP. 3rd generation partnership project; technical specification group services and system aspects; study on the security aspects of the next generation system (Release 14). TR 33.899 version 1.3.0, 2017

5 5GPP. 5G PPP phase1 security landscape produced by the 5G PPP security WG. 2017. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

6 NGMN. NGMN 5G white paper. http://ngmn.org/5g-white-paper.html

7 China Communications Standards Association (CCSA). Study on the 5G security technology. 2016. http://www.ccsa.org.cn/tc/meeting.php?meeting_id=5495

8 China Communications Standards Association (CCSA). Technical requirement on 5G security. 2017. http://www.ccsa.org.cn/tc/meeting.php?meeting_id=5693

9 Ericsson. 5G security: scenarios and solutions. 2015. http://www.ericsson.com/cn/res/docs/whitepapers/wp-5g-security.pdf

10 Datang Telecom Technology & Industry Group. Building a safe and secure cyberspace: 5G network security white paper (in Chinese). 2015

11 Huawei Technologies Co. Ltd. 5G: safety requirements and safety principles, Huawei white paper. 2015. https://max.book118.com/html/2017/0709/121290873.shtm

12 Huawei Technologies Co. Ltd. 5G scenarios and security design. 2016. https://www-file.huawei.com/-/media/CORPORATE/PDF/white%20paper/5g-scenarios-and-security-design.pdf

13 NOKIA Bell Labs. Securing 5G mobile networks built on distributed telco clouds. 2017. http://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/06_5GSECURITY/KEYNOTE_NOKIA_SCHNEIDER.pdf

14 Uher J, Harper J, Mennecke R G, et al. Investigating end-to-end security in the fifth generation wireless capabilities and IoT extensions. In: Proceedings of Cyber Sensing, International Society for Optics and Photonics, Baltimore, 2016

15 Tao X F, Han Y, Xu X D, et al. Recent advances and future challenges for mobile network virtualization. Sci China Inf Sci, 2017, 60: 040301

16 Liu Y L, Chen H H, Wang L M. Physical layer security for next generation wireless networks: theories, technologies, and challenges. IEEE Commun Surv Tutorials, 2017, 19: 347–376

17 Duan X Y, Wang X B. Authentication handover and privacy protection in 5G hetnets using software-defined networking. IEEE Commun Mag, 2015, 53: 28–35

18 Future Forum 5G SIG. 5G: rethink mobile communications for 2020+ white paper. 2014. https://www.ncbi.nlm.nih.gov/pubmed/26809577

19 Prasad A, Benjebbour A, Bulakci O, et al. Agile radio resource management techniques for 5G new radio. IEEE Commun Mag, 2017, 55: 62–63

20 Sun Y H, Zhao M, Zhang S H, et al. Aggregation transmission scheme for machine type communications. Sci China Inf Sci, 2017, 60: 100305

21 Jayawickrama B A, He Y, Dutkiewicz E, et al. Scalable spectrum access system for massive machine type communication. IEEE Netw, 2018, 32: 154–160

22 Lien S Y, Hung S C, Deng D J, et al. Optimum ultra-reliable and low latency communications in 5G new radio. In: Mobile Networks and Applications. Berlin: Springer, 2017

23 Pratas N K, Pattathil S, Stefanović Č, et al. Massive machine-type communication (mMTC) access with integrated authentication. In: Proceedings of IEEE International Conference on Communications, Paris, 2017

24 Mathur C N, Subbalakshmi K P. A light weight enhancement to RC4 based security for resource constrained wireless devices. Int J Netw Secur, 2007, 5: 205–212

25 Hamamreh J M, Basar E, Arslan H. OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services. IEEE Access, 2017, 5: 25863–25875

26 Hoymann C, Astely D, Stattin M, et al. LTE release 14 outlook. IEEE Commun Mag, 2016, 54: 44–49

27 Ni J B, Zhang A Q, Lin X D, et al. Security, privacy, and fairness in fog-based vehicular crowdsensing. IEEE

Commun Mag, 2017, 55: 146–152
28 Open Networking Foundation. Software defined networking: the new norm for networks. 2013. https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf
29 ETSI. Network function virtualization: architectural framework. 2013. http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf
30 Xu D Y, Ren P Y, Du Q H, et al. Towards win-win: weighted-Voronoi-diagram based channel quantization for security enhancement in downlink cloud-RAN with limited CSI feedback. Sci China Inf Sci, 2017, 60: 040303
31 Pfaff B, Scherer J, Hock D, et al. SDN/NFV-enabled security architecture for fine-grained policy enforcement and threat mitigation for enterprise networks. In: Proceedings of the SIGCOMM Posters and Demos, Los Angeles, 2017
32 Petroulakis N E, Fysarakis K, Askoxylakis I, et al. Reactive security for SDN/NFV-enabled industrial networks leveraging service function chaining. Trans Emerg Telecomun Technol, 2017, 27: 3269
33 Ordonez-Lucena J, Ameigeiras P, Lopez D, et al. Network slicing for 5G with SDN/NFV: concepts, architectures, and challenges. IEEE Commun Mag, 2017, 55: 80–87
34 Rhee M Y. Cryptography and Secure Communications. New York: McGraw-Hill, 1993
35 Zhang X W, Kunz A, Schröder S. Overview of 5G security in 3GPP. In: Proceedings of IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, 2017. 181–186
36 Soderi S, Mucchi L, Hämäläinen M, et al. Physical layer security based on spread-spectrum watermarking and jamming receiver. Trans Emerg Telecommun Technol, 2017, 28: 3142
37 Li L M, Wang D M, Niu X K, et al. mmWave communications for 5G: implementation challenges and advances. Sci China Inf Sci, 2018, 61: 021301
38 Ji X S, Yang J, Huang K Z, et al. Physical layer authentication scheme based on Hash method. J Electron Inf Technol, 2016, 38: 2900–2907
39 Yang J. Research on authentication schemes based on physical layer security. Dissertation for Master Degree. Zhengzhou: PLA Information Engineering University, 2016
40 Akpakwu G A, Silva B J, Hancke G P, et al. A survey on 5G networks for the internet of things: communication technologies and challenges. IEEE Access, 2018, 6: 3619–3647
41 Zhang J, Ge X H, Li Q, et al. 5G millimeter-wave antenna array: design and challenges. IEEE Wirel Commun, 2017, 24: 106–112
42 Gandotra P, Jha R K. A survey on green communication and security challenges in 5G wireless communication networks. J Netw Comput Appl, 2017, 96: 39–61
43 Roiger R J. Data Mining: a Tutorial-Based Primer. Boca Raton: CRC Press, 2017
44 Gupta A, Jha R K. A survey of 5G network: architecture and emerging technologies. IEEE Access, 2015, 3: 1206–1232
45 Kumar T, Liyanage M, Ahmad I, et al. User privacy, identity and trust in 5G. In: A Comprehensive Guide to 5G Security. Hoboken: Wiley, 2018
46 Wu J X. Research on network space mimicry defense technology. Cyber Secur, 2016, 1: 1–10
47 Hu H C, Chen F C, Wang Z P. Several issues and performance evaluation of pseudo mimicry defense DHR model. Cyber Secur, 2016, 1: 40–51
48 Wu J X. A brief introduction to cyberspace mimicry defense principle. Civil Mil Integration, 2017, 2: 30–35
49 Wu J X. Nextwork space mimicry defense technology (in Chinese). Secrecy Sci Technol, 2014, 10: 4–9
50 Ji X S, Huang K Z, Wen H, et al. Achieving strong security based on fountain code with coset pre-coding. IET Commun, 2014, 8: 2476–2483
51 Li X Y, Wang X, Xu X, et al. A distributed implementation algorithm for physical layer security based on untrusted relay cooperation and artificial noise. ETRI J, 2014, 36: 183–186
52 Ji X S, Kang X, Huang K Z, et al. The full-duplex artificial noise scheme for security of a cellular system. China Commun, 2015, 12: 150–156
53 Yang N, Wang L F, Geraci G, et al. Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun Mag, 2015, 53: 20–27
54 Wang C X, You X H, Wang J, et al. Special focus on 5G wireless communication networks. Sci China Inf Sci, 2016, 59: 020300
55 Zhong Z. Reseach on secure coding and transmission mechanism under equivalent channel feature variable model. Dissertation for Ph.D. Degree. Zhengzhou: PLA Information Engineering University, 2013
56 Ahlswede R, Csiszar I. Common randomness in information theory and cryptography. Part I: Secret sharing. IEEE Trans Inf Theory, 1993, 39: 1121–1132

57 Huang Y, Jin L, Li N, et al. Secret key generation based on private pilot under man-in-the-middle attack. Sci China Inf Sci, 2017, 60: 100307

58 Aono T, Higuchi K, Ohira T, et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. IEEE Trans Antenn Propag, 2005, 53: 3776–3784

59 Sayeed A, Perrig A. Secure wireless communications: secret keys through multipath. In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas, 2008. 3013–3016

60 Chen C, Jensen M A. Secret key establishment using temporally and spatially correlated wireless channel coefficients. IEEE Trans Mobile Comput, 2011, 10: 205–215

61 Wang H M, Zheng T X, Yuan J, et al. Physical layer security in heterogeneous cellular networks. IEEE Trans Commun, 2016, 64: 1204–1219

62 Lv T J, Gao H, Yang S S. Secrecy transmit beamforming for heterogeneous networks. IEEE J Sel Areas Commun, 2015, 33: 1154–1170

63 Dong L, Han Z, Petropulu A P, et al. Improving wireless physical layer security via cooperating relays. IEEE Trans Signal Process, 2010, 58: 1875–1888

64 Zheng G, Choo L C, Wong K K. Optimal cooperative jamming to enhance physical layer security using relays. IEEE Trans Signal Process, 2011, 59: 1317–1322

65 Zhang R Q, Cheng X, Yang L Q. Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks. IEEE Trans Wirel Commun, 2016, 15: 5651–5663

66 Xu C, Zeng P, Liang W, et al. Secure resource allocation for green and cognitive device-to-device communication. Sci China Inf Sci, 2018, 61: 029305

67 Deng Y S, Wang L F, Wong K K, et al. Safeguarding massive MIMO aided hetnets using physical layer security. In: Proceedings of IEEE International Conference on Wireless Communications & Signal Processing, Nanjing, 2015

68 Zhu J, Schober R, Bhargava V K. Secure transmission in multicell massive MIMO systems. IEEE Trans Wirel Commun, 2014, 13: 4766–4781

69 Zhu J, Schober R, Bhargava V K. Linear precoding of data and artificial noise in secure massive MIMO systems. IEEE Trans Wirel Commun, 2016, 15: 2245–2261

70 Kapetanovic D, Zheng G, Rusek F. Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks. IEEE Commun Mag, 2015, 53: 21–27

71 Wang C, Wang H M. Physical layer security in millimeter wave cellular networks. IEEE Trans Wirel Commun, 2016, 15: 5569–5585

72 Zhu Y X, Wang L F, Wong K K, et al. Secure communications in millimeter wave Ad hoc networks. IEEE Trans Wirel Commun, 2017, 16: 3205–3217

73 Xiao M, Mumtaz S, Huang Y M, et al. Millimeter wave communications for future mobile networks. IEEE J Sel Areas Commun, 2017, 35: 1909–1935

74 Qin Z J, Liu Y W, Ding Z G, et al. Physical security for 5G non-orthogonal multiple access in large-scale networks. In: Proceedings of IEEE International Conference on Communications, Kuala Lumpur, 2016

75 Liu Y W, Qin Z J, Elkashlan M, et al. Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. IEEE Trans Wirel Commun, 2017, 16: 1656–1672

76 Islam S M, Zeng M, Dobre O A. Noma in 5G systems: existing possibilities for enhancing spectral efficiency. 2017. ArXiv:1706.08215

77 Patwari N, Kasera S K. Temporal link signature measurements for location distinction. IEEE Trans Mobile Comput, 2011, 10: 449–462

78 Xiao L, Greenstein L J, Mandayam N B, et al. Fingerprints in the ether: using the physical layer for wireless authentication. In: Proceedings of IEEE International Conference on Communications, Glasgow, 2007. 4646–4651

79 Xiao L, Chen T H, Han G A, et al. Game theoretic study on channel-based authentication in MIMO systems. IEEE Trans Veh Technol, 2017, 66: 7474–7484

80 Caparra G, Centenaro M, Laurenti N, et al. Energy-based anchor node selection for IoT physical layer authentication. In: Proceedings of IEEE International Conference on Communications, Kuala Lumpur, 2016

81 Rahman M M U, Abbasi Q H, Chopra N, et al. Physical layer authentication in Nano networks at terahertz frequencies for biomedical applications. IEEE Access, 2017, 5: 7808–7815

82 Wang X B, Hao P, Hanzo L. Physical-layer authentication for wireless security enhancement: current challenges and future developments. IEEE Commun Mag, 2016, 54: 152–158

83 Duan X Y, Wang X B. Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information.

In: Proceedings of IEEE International Conference on Communications, Kuala Lumpur, 2016
84 Shan D, Zeng K, Xiang W D, et al. PHY-CRAM: physical layer challenge-response authentication mechanism for wireless networks. IEEE J Sel Areas Commun, 2013, 31: 1817–1827
85 Du X R, Shan D, Zeng K, et al. Physical layer challenge-response authentication in wireless networks with relay. In: Proceedings of IEEE International Conference on Computer Communications, Toronto, 2014. 1276–1284
86 Wu X F, Yang Z. Physical-layer authentication for multi-carrier transmission. IEEE Commun Lett, 2015, 19: 74–77
87 Wu X F, Yang Z, Ling C, et al. Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission. IEEE Trans Wirel Commun, 2016, 15: 6611–6625
88 Wen H, Ho P H, Gong G. A novel framework for message authentication in vehicular communication networks. In: Proceedings of IEEE International Conference on Global Telecommunications, Honolulu, 2009
89 Wang Y F, Zhou L, Zhu X P, et al. Physical layer assist authentication technique for smart meter system. IET Commun, 2013, 7: 189–197
90 Wu X F, Yan Z, Ling C, et al. A physical-layer authentication assisted scheme for enhancing 3GPP authentication. Mathematics, 2015. ArXiv:1502.07565
91 Yang J, Ji X S, Huang K Z, et al. AKA-PLA: enhanced AKA based on physical layer authentication. KSII Trans Int Inf Syst, 2017, 11: 3747–3765
92 Maurer U M. Secret key agreement by public discussion from common information. IEEE Trans Inf Theory, 1993, 39: 733–742
93 Wang X, Jin L, Song H W, et al. Physical layer security key capacity based on wireless channel parameters. J Electron Inf Technol, 2016, 38: 2612–2618
94 Wang X, Jin L, Liu L, et al. Analysis of physical layer security key capacity in uniform scattering environment. J Commun, 2016, 37: 75–81
95 Furqan H M, Hamamreh J M, Arslan H. Secret key generation using channel quantization with SVD for reciprocal MIMO channels. In: Proceedings of IEEE International Symposium on Wireless Communication Systems, Poznan, 2016. 597–602
96 Taha H, Alsusa E A. Secret key exchange using private random precoding in MIMO FDD and TDD systems. IEEE Trans Veh Technol, 2017, 66: 4823–4833
97 Lai L F, Liang Y B, Du W L. Cooperative key generation in wireless networks. IEEE J Sel Areas Commun, 2012, 30: 1578–1588
98 Wang N, Zhang N, Gulliver T A. Cooperative key agreement for wireless networking: key rates and practical protocol design. IEEE Trans Inf Foren Secur, 2014, 9: 272–284
99 Chen K, Natarajan B, Shattil S. Secret key generation rate with power allocation in relay-based LTE-A networks. IEEE Trans Inf Foren Secur, 2015, 10: 2424–2434
100 Ngassa C L K, Moliére R, Delaveau F, et al. Secret key generation scheme from WiFi and LTE reference signals. Analog Integ Circ Signal Process, 2017, 91: 277–292
101 ITU. New proposal about requirement and evaluation criteria of technologies to enhance security and privacy of radio communications. ITU-R66 WRC-19, 2016
102 ITU. Proposal for studies related to the security of machine-type communications and internet of things. ITU-R66 WRC-19, 2016
103 Thales. Enhanced protections using physical layer security. 3GPP TSG SA WG3 #82 S3-160267, 2016
104 Thales. PCR for adding solution for key issues #7.4 and #7.7: effective generation of temporary or short-time identifiers based on channel estimation. 3GPP TSG SA WG3 #85 S3-161639, 2016
105 Thales. Study on architecture and security for nest generation system. 3GPP TSG SA WG3 #82 S3-160278, 2016
106 ISO/IEC 29192. Information technology-security techniques-lightweight cryptography – part 1: general / part 2: block ciphers / part 3: stream ciphers / part 4: mechanisms using asymmetric techniques. 2016
107 Cannière C, Preneel B. Trivium: a stream cipher construction inspired by block cipher design principles. In: Proceedings of International Conference on Information Security, Samos, 2006. 171–186
108 Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: an ultra-lightweight block cipher. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems, Vienna, 2007. 450–466
109 Shirai T, Shibutani K, Akishita T, et al. The 128-bit blockcipher CLEFIA. In: Proceedings of the 14th international conference on Fast Software Encryption, Luxembourg, 2007. 181–195
110 Albrecht M R, Driessen B, Kavun E B, et al. Block ciphers-focus on the linear layer. In: Proceedings of International Cryptology Conference, Santa Barbara, 2014. 57–76

111 Beaulieuand R, Shors D, Smith J, et al. Performance of the SIMON and SPECK Family of Lightweight Block Ciphers. National Security Agency Technical Report, 2014

112 Berger T P, Hayer J D, et al. The GLUON family; a lightweight Hash function family based on FCSRs. In: Proceedings of International Conference on Cryptology in Africa, Ifrance, 2012. 306–323

113 Bansod G, Patil A, Sutar S, et al. An ultra lightweight encryption design for security in pervasive computing. In: Proceedings of the 2nd International Conference on Big Data Security on Cloud, New York, 2016. 79–84

114 Alshamsi A Z, Barka E S, Serhani M A. Lightweight encryption algorithm in wireless body area network for e-health monitoring. In: Proceedings of the 12th International Conference on Innovations in Information Technology, Al-Ain, 2016. 144–150

115 Peng C Y, Du X J, Li K Q, et al. An ultra-lightweight encryption scheme in underwater acoustic networks. J Sensor, 2016, 2016: 1–10

116 Win E K, Yoshihisa T, Yoshimasa I, et al. A lightweight multi-receiver encryption scheme with mutual authentication. In: Proceedings of the 41st Annual Computer Software and Applications Conference, Turin, 2017. 491–497

117 Usman M, Ahmed I, Aslam M I, et al. SIT: a lightweight encryption algorithm for secure internet of things. Int J Adv Comput Sci Appl, 2017, 8: 1–10

118 Tahir S, Ruj S, Rahulamathavan Y, et al. A new secure and lightweight searchable encryption scheme over encrypted cloud data. IEEE Trans Emerg Top Comput, 2017. doi: 10.1109/TETC.2017.2737789

119 Zenger C T, Chur M J, Posoclck J F, et al. A novel key generating architecture for wireless low-resource devices. In: Proceedings of IEEE International Conference on Secure Internet of Things Workshop, Taipei, 2014. 26–34

120 Fritschek R, Wunder G. On-the-fly secure key generation with deterministic models. In: Proceedings of IEEE International Conference on Communications, Paris, 2017

121 Shi L, Yuan J W, Yu S C, et al. MASK-BAN: movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks. IEEE Int Things J, 2015, 2: 52–62

122 Gungor O, Chen F Z, Koksal C E. Secret key generation via localization and mobility. IEEE Trans Veh Technol, 2015, 64: 2214–2230

123 Wang W J, Jiang H Y, Xia X G, et al. A wireless secret key generation method based on Chinese remainder theorem in FDD systems. Sci China Inf Sci, 2012, 55: 1605–1616

124 Lou Y M, Jin L, Zhong Z, et al. Secret key generation scheme based on MIMO received signal spaces (in Chinese). Sin Chin Inform, 2017, 47: 362–373

125 IMT-2020 (5G) Propulsion Group. 5G network technology framework. 2015. http://www.imt-2020.cn/zh/documents/1

126 NGMN. 5G security recommendations package #2: network slicing. 2016. http://ngmn.org/5g-white-paper.html

127 3GPP. 3rd generation partnership project; technical specification group services and system aspects; study on the security aspects of the next generation system (Release 14). TR 33.899 Version 1.1.0, 2017

128 China Mobile Communications Corporation, Huawei Technologies Co., Ltd., Deutsche Telekom AG, Volkswagen. 5G service-guaranteed network slicing white paper. 2017. https://www.huawei.com/ch-en/industry-insights/outlook/mbb-2020/trends-insights/5g-service-guaranteed-network-slicing-whitepaper

129 3GPP. Study on subscriber privacy impact in 3GPP (Release 14). TR 33.849 Version 2.0.0, 2016

130 3GPP. Feasibility study on new services and markets technology enablers for network operation (Release 15). TR 22.864 Version 15.0.0, 2016

131 3GPP. Study on new services and markets technology enablers (Release 9). TR 22.891 Version 14.2.0, 2016

132 3GPP. Service requirements for V2X services (Release 14). TS 22.185 Version 14.3.0, 2017

133 Zhou S G, Li F, Tao Y F, et al. Privacy preservation in database applications: a survey. Chin J Comput, 2009, 32: 847–861

134 Sweeney L. K-anonymity: a model for protecting privacy. Int J Uncertain Fuzz Knowl-Based Syst, 2002, 10: 557–570

135 Machanavajjhala A, Kifer D, Gehrke J. L-diversity: privacy beyond k-anonymity. In: Proceedings of the 22nd International Conference on Data Engineering, Atlanta, 2006

136 Li N H, li T C, Venkatasubramanian S. T-closeness: privacy beyond k-anonymity and l-diversity. In: Proceedings of the 23rd International Conference on Data Engineering, Istanbul, 2007. 106–115

137 Dwork C. Differential privacy: a survey of results. In: Proceedings of the 5th International Conference on Theory and Applications of Models of Computation, Xi'an, 2008

138 Internet Engineering Task Force. Representation of uncertainty and confidence in the presence information data format location object (PIDF-LO). IETF standard RFC 7459-2015. https://buildbot.tools.ietf.org/html/rfc7459

139 Dewri R. Local differential perturbations: location privacy under approximate knowledge attackers. IEEE Trans Mobile Comput, 2013, 12: 2360–2372

140 Yao B, Li F F, Xiao X K. Secure nearest neighbor revisited. In: Proceedings of the 29th IEEE Internation Conference on Data Engineering, Brisbane, 2013. 733–744

141 Stach C, Mitschang B. Privacy management for mobile platforms – a review of concepts and approaches. In: Proceedings of the 14th IEEE International Conference on Mobile Data Management, Milan, 2013. 305–313

142 Future-Forum. The 2nd conference of future forum information security group. 5G security white paper framework recommendations. 2017. http://www.future-forum.org/2009cn/download_list.asp?classid=%B9%A4%D7%F7%D7%E9%CE%C4%B5%B5

143 Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2008. https://bitcoin.org/en/bitcoin-paper

144 Ruubel M. Guardtime federal and galois awarded darpa contract to formally verify blockchain-based integrity monitoring system. https://guardtime.com/blog/galois-and-guardtime-federal-awarded-1-8m-darpa-contract-to-formally-verify-blockchain-based-inte

145 Zyskind G, Nathan O, Pentland A S. Decentralizing privacy: using blockchain to protect personal data. In: Proceedings of IEEE Security and Privacy Workshops, San Jose, 2015. 180–184

146 Kravitz D W, Cooper J. Securing user identity and transactions symbiotically: IoT meets blockchain. In: Proceedings of IEEE Global Internet of Things Summit, Geneva, 2017

147 Lei A, Cruickshank H, Cao Y, et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Int Things J, 2017, 4: 1832–1843

148 Cai C J, Yuan X L, Wang C. Towards trustworthy and private keyword search in encrypted decentralized storage. In: Proceedings of 2017 IEEE International Conference on Conmunications, Paris, 2017

149 IBM Institute for Business Value. Device democracy: saving the future of the internet of things. http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/