8-2017

Security for 5G Mobile Wireless Networks

Dongfeng Fang
University of Nebraska-Lincoln, dongfeng.fang@huskers.unl.edu

Yi Qian
University of Nebraska-Lincoln, yqian2@unl.edu

Rose Qingyang Hu
Utah State University, rose.hu@usu.edu

Security for 5G Mobile Wireless Networks

Dongfeng Fang, Yi Qian, and Rose Qingyang Hu

***Abstract*—The advanced features of 5G mobile wireless network systems yield new security requirements and challenges. This paper presents a comprehensive survey on security of 5G wireless network systems compared to the traditional cellular networks. The paper starts with a review on 5G wireless networks particularities as well as on the new requirements and motivations of 5G wireless security. The potential attacks and security services with the consideration of new service requirements and new use cases in 5G wireless networks are then summarized. The recent development and the existing schemes for the 5G wireless security are presented based on the corresponding security services including authentication, availability, data confidentiality, key management and privacy. The paper further discusses the new security features involving different technologies applied to 5G such as heterogeneous networks, device-to-device communications, massive multiple-input multiple-output, software defined networks and Internet of Things. Motivated by these security research and development activities, we propose a new 5G wireless security architecture, based on which the analysis of identity management and flexible authentication is provided. As a case study, we explore a handover procedure as well as a signaling load scheme to show the advantage of the proposed security architecture. The challenges and future directions of 5G wireless security are finally summarized.**

***Index Terms*—5G wireless network systems, security, authentication, availability, confidentiality, key management, privacy, heterogenous networks, device-to-device communications, massive multiple-input multiple-output, software defined networks, Internet of Things, 5G wireless security architecture.**

I. Introduction

5TH generation wireless systems, or 5G, are the next generation mobile wireless telecommunications beyond the current 4G/International Mobile Telecommunications (IMT)-Advanced Systems [1]. 5G wireless system is not only an evolution of the legacy 4G cellular networks, but also a system with many new service capabilities [2]. 5G research and development aim at various advanced characteristics, such as higher capacity than current 4G, higher density of mobile broadband users, and supporting device-to-device (D2D) communications and massive machine-type communications [3]. 5G planning also aims at lower latency and lower energy consumption, for better implementation of Internet of Things (IoT) [4]. More specifically, there are eight advanced features of 5G wireless systems, 1-10 Gbps connections to end points in the field, 1 millisecond latency, 1000x bandwidth per unit area, 10-100x number of connected devices, 99.999% availability, 100% coverage, 90% reduction of network energy usage and up to ten years battery life for low power devices [5]. To achieve these performance requirements, various technologies [6] are applied to 5G systems, such as heterogenous networks (HetNet), massive multiple-input multiple-output (MIMO), millimeter wave (mmWave) [7], D2D communications [8], software defined network (SDN) [9], network functions visualization (NFV) [10] and networking slicing [11]. The standardization process for 5G wireless systems is just at the very beginning. Fig. 1 illustrates a generic architecture of 5G wireless systems. 5G wireless systems can provide not only traditional voice and data communications, but also many new use cases, new industry applications, and a multitude of devices and applications to connect society at large [12]. Different 5G use cases are specified such as vehicle-to-vehicle and vehicle-to-infrastructure communications, industrial automation, health services, smart cities, smart homes and so on [13]. It is believed that 5G wireless systems can enhance mobile broadband with critical services and massive IoT [14]. The new architecture, new technologies, and new use cases in 5G wireless systems will bring new challenges to security and privacy protection [15].

Due to the broadcast nature and the limited bandwidth of wireless communications, it is possible but difficult to provide security features such as authentication, integrity and confidentiality. There are various security issues in current cellular networks at media access control layer (MAC) and physical layer (PHY) in terms of possible attacks, vulnerabilities and privacy concerns [16]. The security protections of voice and data are provided based on traditional security architectures with security features as user identity management, mutual authentications between the network and user equipment (UE), securing communication channel and so on. In the legacy cellular networks - Long Term Evolution (LTE), a high level of security and trustworthiness for users and network operators are provided [12]. Besides encryption of user traffic, mutual authentication is achieved between a UE and a base station. In addition, the security of the access and the mobility management of LTE are ensured by a key hierarchy and handover key management mechanism [17]. There are also research work on security related to the technologies applied to LTE [18] [19]. However, new security requirements are needed to support a variety of new use cases and the new networking paradigms [20]. The security mechanisms are needed to comply with the overall 5G advanced features such as low latency and high energy efficiency (EE) [20]. The Next Generation Mobile Networks (NGMN) Alliance highlights the security requirements of 5G wireless networks shown in Table. I. Moreover, unlike the legacy cellular networks, 5G wireless networks are going to be service-oriented which has a special emphasis on security and privacy requirements from the perspective of services [15].

Fig. 2 illustrates the main drives for 5G wireless security.

This work was supported by the National Science Foundation under the grants ECCS-1307580, ECCS-1308006, EARS-1547312, and EARS-1547330.

D. Fang, and Y. Qian are with the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Omaha, NE 68182. E-mail: dongfeng.fang@huskers.unl.edu; yqian2@unl.edu.

R. Q. Hu is with the Department of Electrical and Computer Engineering, Utah State University, Logan, UT 84321. E-mail: rose.hu@usu.edu.

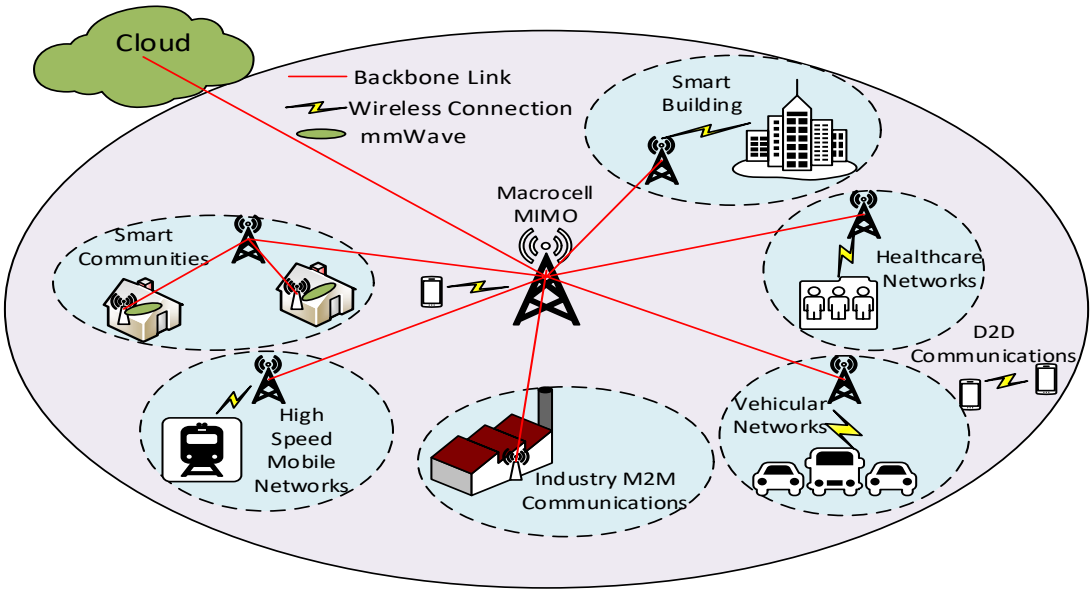


Fig. 1: A generic architecture for 5G wireless systems

TABLE I: Security requirements for 5G wireless networks [21]

Requirements respect to 4G	Improve resilience and availability of the network against signaling based threats including overload caused maliciously or unexpectedly
	Specific security design for use cases which require extremely low latency
	Comply with security requirements defined in 4G 3GPP standards. Need to apply especially to a virtualized implementation of the network
	Provide Public Safety and Mission Critical Communications (resilience and high availability)
Requirements from radio access perspective	Improve system robustness against smart jamming attacks
	Improve security for 5G small cell nodes

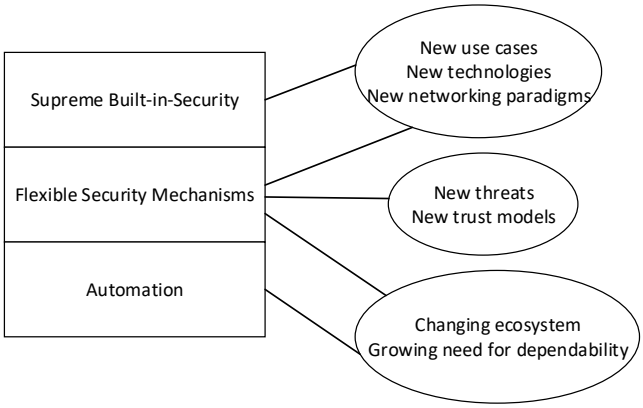


Fig. 2: Major drives for 5G wireless security

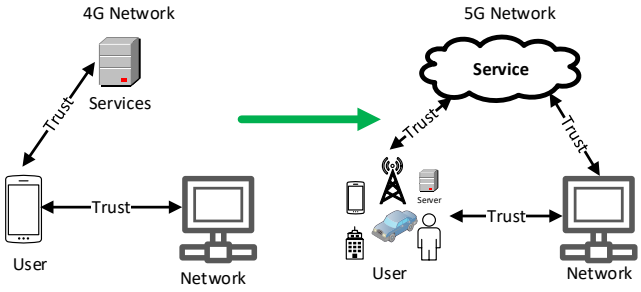


Fig. 3: Trust model of 4G and 5G wireless networks

The new use cases can have a variety of specific requirements such as ultra-low latency in the user communications. New technologies not only yield advanced service capabilities but also open door to vulnerabilities and thus impose new security requirements in 5G [22][23]. In HetNet, different access technologies may have different security requirements, and multi-network environment may need high frequent authentications with stringent delay constraints [24]. Massive MIMO has been deemed an important 5G technique to achieve higher spectral efficient and energy efficiency. It is also considered as a valuable technique against passive eavesdropping [25]. Furthermore, SDN and NFV in 5G will support new service delivery models and thus require new security aspects [26] [27]. With the advent of 5G networking paradigms, new security architecture is needed [28]. To address these issues, security must be considered as an integral part of the overall architecture and should be integrated into the system design at the very beginning. To support various use cases and new trust models in an optimal way, flexible security mechanisms are needed. The trust models of the legacy cellular networks and 5G wireless networks are presented in Fig. 3 [15]. Authentications are required not only between subscribers and the two

operators (the home and serving networks) but also among service parties in 5G wireless networks. Moreover, for the vertical industries use case, the security demands can be significantly different among different applications. For instance, mobile devices require lightweight security mechanisms as its power resource constraint, while high-speed services require efficient security services with low latency. Therefore, the general flexibility for 5G security mechanisms is another key requirement [29]. The authentication management in 5G is more complex due to various types of and a massive number of devices connected. For different applications, different authentication models can be implemented. In Fig. 3, user authentication can be done by the network provider, or by the service provider, or by both. Besides the flexibility requirement of 5G security, security automation is also a key element. It combines automated holistic security management with automated and intelligent security controls [20]. Since more personal information is used in various applications such as surveillance applied over 5G wireless networks, privacy concerns escalate. Moreover, various services in 5G can be tied closer than before. As an example, the fixed telephone line, internet access, and TV service can be terminated simultaneously due to the outage of a major network [15]. Therefore, security automation is needed to make the 5G system robust against various security attacks.

Security attacks can be classified into two types, namely, passive attacks and active attacks [30]. For a passive attack, attackers attempt to learn or make use of the information from the legitimate users but do not intend to attack the communication itself. The popular passive attacks in a cellular network are two kinds, i.e., eavesdropping and traffic analysis. Passive attacks aim to violate data confidentiality and user privacy. Unlike passive attacks, active attacks can involve modification of the data or interruption of legitimate communications. Typical active attacks include man-in-the-middle attack (MITM), replay attack, denial of service (DoS) attack, and distributed denial of service (DDoS) attack.

The mechanisms used to tackle security attacks can be mainly divided into two categories: cryptographic approaches with new networking protocols and physical layer security (PLS) approaches. The cryptographic techniques are the most commonly used security mechanisms, which are normally deployed at the upper layers of the 5G wireless networks with new networking protocols. The modern cryptography consists of symmetric-key cryptography and public-key cryptography. Symmetric-key cryptography refers to the encryption methods in which a secret key is shared between a sender and a receiver. Public-key cryptography or asymmetric cryptography uses two different keys, one is used as the public key for encryption and the other one is used as the secret key for decryption. The performance of a security service depends on the key length and computational complexity of the algorithms. The management and distribution of the symmetric keys are well protected in the traditional cellular networks. Due to more complex protocols and heterogeneous network architectures in 5G, the management and distribution of symmetric keys may encounter new challenges [31].

Due to the limited progress on practical wiretap codes and

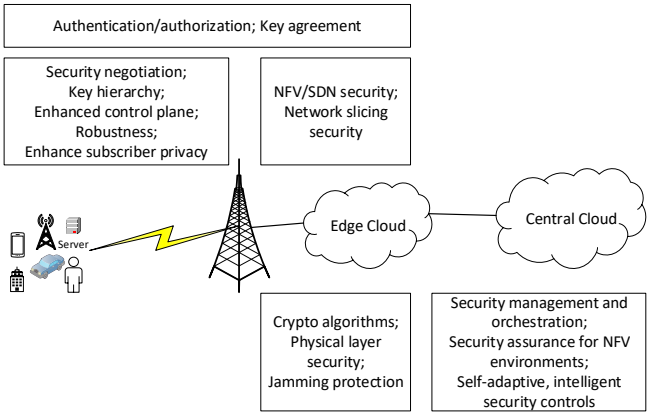


Fig. 4: Elements in a 5G security architecture [20]

on strictly positive secrecy capacity in the 1970s and 1980s, the application of PLS has been hampered. At that time, most contemporary security schemes adopted the public-key cryptography [32]. The interest on using PLS quickly mounted after [33] proved that it is still possible for a legitimate user with a worse channel than the eavesdropper to generate a secret key over an insecure public channel. There have been extensive PLS research done recently in 5G wireless systems. Unlike conventional approaches that provide security mainly through cryptographic techniques, PLS is identified as a promising security strategy to provide secure wireless transmissions by exploiting the unique wireless physical layer medium features [34]. Compared to cryptography, PLS demonstrates advantages in two aspects, namely, low computational complexity and high scalability, which make PLS an ideal candidate technique for cryptographic key distribution in 5G wireless networks. In [31], authors summarized the existing PLS techniques and grouped them into five major categories based on their theoretical security capacity, power, code, channel, and signal approaches.

Besides PLS and cryptographic techniques, there have been some research work on security architecture [35], vulnerability assessment mechanisms [36], and intrusion detection mechanisms based on data analysis [37]. These security mechanisms need to comply with the 5G performance requirements such as extremely low latency and high degree of EE. The 5G security requirements thus need to consider the legacy security features, new use cases, and new networking paradigms altogether. Fig. 4 presents the typical elements in a 5G security architecture. Edge cloud is applied to improve the network performance by reducing the communication delay. Central cloud is used to connect the edge clouds for data sharing and centralized control.

The main contributions of this paper are summarized as follows. We first discuss various attacks as well as the state-of-the-art solutions in 5G wireless networks based on security services. The new security concerns on the technologies applied to 5G wireless network systems are then presented. Motivated by these security research and development activities, we further propose a new 5G wireless security architecture, based on which the analysis of identity management and flexible

authentication is provided. As a case study, we examine a handover procedure as well as a signaling load scheme to show the advantage of the proposed security architecture. The challenges and future directions of 5G wireless network security are finally summarized.

The rest of this paper is organized as follows. The attacks and security services in 5G wireless networks are introduced in section II. In section III, recent development and current solutions in 5G wireless security are discussed. In section IV, security issues for different technologies applied to 5G are elaborated. In section V, we propose a 5G wireless security architecture. The analysis of identity management and flexible authentication based on the new security architecture is presented. A handover procedure and signaling load analysis are studied to show the advantage of the proposed security architecture. In section VI, challenges and future directions for 5G wireless security are introduced. In section VII, conclusion is presented.

II. Attacks and Security Services in 5G Wireless Networks

Due to the broadcast nature of the wireless medium, wireless information transmission is vulnerable to various malicious threats. In this section, we discuss four types of attacks, i.e., eavesdropping and traffic analysis, jamming, DoS and DDoS, and MITM, in 5G wireless networks. We also introduce four security services including authentication, confidentiality, availability, and integrity.

A. Attacks in 5G Wireless Networks

Fig. 5 illustrates all four attacks, each of which is individually discussed in the following three aspects, type of the attack (passive or active), security services provided to fight against this attack, and the corresponding methods applied to avoid or prevent this attack. We focus on security attacks at the PHY layer and MAC layer, where the key difference on security between wireless and wire-line networks occur.

1) Eavesdropping and Traffic Analysis: Eavesdropping is an attack that is used by an unintended receiver to intercept a message from others. Eavesdropping is a passive attack as the normal communication is not affected by eavesdropping, as shown in Fig. 5a. Due to the passive nature, eavesdropping is hard to detect. Encryption of the signals over the radio link is most commonly applied to fight against the eavesdropping attack. The eavesdropper can not intercept the received signal directly due to the encryption. Traffic analysis is another passive attack that an unintended receiver uses to intercept information such as location and identity of the communication parties by analyzing the traffic of the received signal without understanding the content of the signal itself. In other word, even the signal is encrypted, traffic analysis can still be used to reveal the patterns of the communication parties. Traffic analysis attack does not impact the legitimate communications either.

Encryption method used to prevent eavesdropping is heavily dependent on the strength of the encryption algorithm and also on the computing capability of the eavesdropper. Due to the quick escalation of computing power and booming of advanced data analysis technologies, eavesdropper can take the advantage of the new technologies in theirs attacks. The existing mechanisms to tackle eavesdropping face a big challenge as many of them assume a small number of simultaneous eavesdroppers with low computing capability and low data analysis capability. Moreover, some technologies applied to 5G wireless networks such as HetNet may further increase the difficulty to fight against eavesdroppers. In general the new characteristics of 5G wireless networks lead to many more complicated scenarios to cope with eavesdroppers, for example, in [38], eavesdroppers with multiple antennas are considered. As cryptographic methods to tackle eavesdropping have been extensively investigated in the past and are considered rather mature, most recently, PLS research to tackle eavesdropping has been paid more and more attentions.

2) Jamming: Unlike eavesdropping and traffic analysis, jamming can completely disrupt the communications between legitimate users. Fig. 5b is an example for jamming attack. The malicious node can generate intentional interference that can disrupt the data communications between legitimate users. Jamming can also prevent authorized users from accessing radio resources. The solutions for active attacks are normally detection based.

Spread spectrum techniques such as direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) are widely used as a secure communication method to fight against jamming at the PHY layer by spreading the signals over a wider spectral bandwidth. However, DSSS and FHSS based anti-jamming schemes may not fit into some applications in 5G wireless networks. In [39], a pseudorandom time hopping anti-jamming scheme is proposed for cognitive users to improve the performance compared to FHSS. Due to the characteristics of jamming, detection is possible. In [40], a resource allocation strategy is proposed between a fusion center and a jammer. Resource allocation is applied to improve the detection to achieve a better error rate performance.

3) DoS and DDoS: DoS attacks can exhaust the network resources by an adversary. DoS is a security attack violation of the availability of the networks. Jamming can be used to launch a DoS attack. DDoS can be formed when more than one distributed adversary exists. Fig.5c shows a DDoS model. DoS and DDoS are both active attacks that can be applied at different layers. Currently, detection is mostly used to recognize DoS and DDoS attacks. With a high penetration of massive devices in 5G wireless networks, DoS and DDoS will likely become a serious threat for operators [21]. DoS and DDoS attacks in 5G wireless networks can attack the access network via a very large number of connected devices. Based on the attacking target, a DoS attack can be identified either as a network infrastructure DoS attack or a device/user DoS attack [21]. A DoS attack against the network infrastructure can strike the signaling plane, user plane, management plane, support systems, radio resources, logical and physical resources [21]. A DoS attack against device/user can target on battery, memory, disk, CPU, radio, actuator and sensors [21].

4) MITM: In MITM attack, the attacker secretly takes control of the communication channel between two legitimate par-

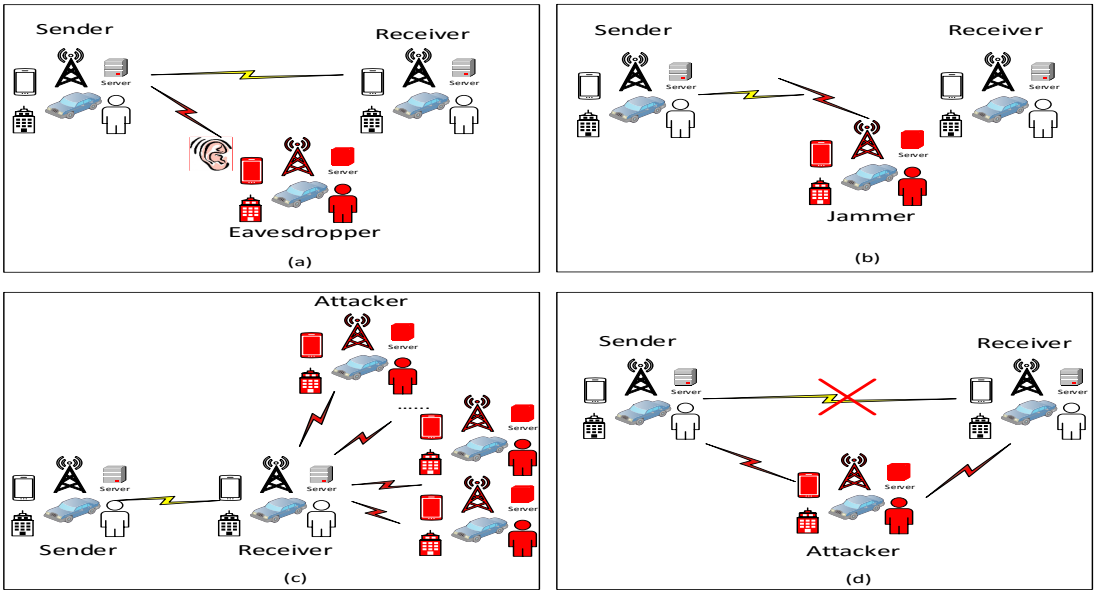


Fig. 5: Attacks in 5G wireless networks (a). Eavesdropping; (b). Jamming; (c). DDoS; (d). MITM

ties. The MITM attacker can intercept, modify, and replace the communication messages between the two legitimate parties. Fig. 5d shows a MITM attack model. MITM is an active attack that can be launched in different layers. In particular, MITM attacks aim to compromise data confidentiality, integrity, and availability. Based on the Verizon's data investigation report [41], MITM attack is one of the most common security attacks. In the legacy cellular network, false base station based MITM is an attack that the attacker forces a legitimate user to create a connection with a fake base transceiver station [42]. Mutual authentication between the mobile device and the base station is normally used to prevent the false base station based MITM.

B. Security Services in 5G Wireless Networks

The new architecture, new technologies, and use cases in 5G wireless networks bring in new features and requirements of security services. In this section, we primarily introduce four types of security services: authentication (entity authentication, message authentication), confidentiality (data confidentiality, privacy), availability, and integrity.

1) Authentication: There are two kinds of authentications, namely, entity authentication and message authentication. Both entity authentication and message authentication are important in 5G wireless networks to tackle the previous mentioned attacks. Entity authentication is used to ensure the communicating entity is the one that it claims to be. In the legacy cellular networks, mutual authentication between user equipment (UE) and mobility management entity (MME) is implemented before the two parties communicating to each other. The mutual authentications between UE and MME is the most important security feature in the traditional cellular security framework. The authentication and key agreement (AKA) in 4G LTE cellular networks is symmetric-key based. However, 5G requires authentication not only between UE and MME but also between other third parties such as service providers. Since the trust model differs from that used in the traditional cellular networks, hybrid and flexible authentication management is needed in 5G. The hybrid and flexible authentication of UE can be implemented in three different ways: authentication by network only, authentication by service provider only, and authentication by both network and service provider [15]. Due to the very high speed data rate and extremely low latency requirement in 5G wireless networks, authentication in 5G is expected to be much faster than ever. Moreover, the multi-tier architecture of the 5G may encounter very frequent handovers and authentications between different tiers in 5G. In [43], to overcome the difficulties of key management in HetNets and to reduce the unnecessary latency caused by frequent handovers and authentications between different tiers, a SDN enabled fast authentication scheme using weighted secure-context-information transfer is proposed to improve the efficiency of authentication during handovers and to meet 5G latency requirement. To provide more security services in 5G wireless networks, in [44][45], a public-key based AKA is proposed.

With the various new applications in 5G wireless networks, message authentication becomes increasingly important. Moreover, with the more strict requirements on latency, spectrum efficiency (SE), and EE in 5G, message authentication is facing new challenges. In [46] an efficient Cyclic Redundancy Check (CRC) based message authentication for 5G is proposed to enable the detection of both random and malicious error without increasing bandwidth.

2) Confidentiality: Confidentiality consists of two aspects, i.e., data confidentiality and privacy. Data confidentiality protects data transmission from passive attacks by limiting the data access to intended users only and preventing the access from or disclosure to unauthorized users. Privacy prevents controlling and influencing the information related to legitimate users, for example, privacy protects traffic flows from

any analysis of an attacker. The traffic patterns can be used to diagnose sensitive information, such as senders/receivers location, etc. With various applications in 5G, there exist massive data related to user privacy, e.g., vehicle routing data, health monitoring data, and so on.

Data encryption has been widely used to secure the data confidentiality by preventing unauthorized users from extracting any useful information from the broadcast information. Symmetric key encryption technique can be applied to encrypt and decrypt data with one private key shared between the sender and the receiver. To share a key between the sender and the receiver, a secure key distribution method is required. Conventional cryptography method is designed based on the assumption that attackers have limited computing capabilities. Thus it is hard to fight against attackers who are equipped with powerful computing capabilities. Rather than relying solely upon generic higher-layer cryptographic mechanisms, PLS can support confidentiality service [47] against jamming and eavesdropping attacks. Besides the data services of 5G, users start to realize the importance of privacy protection service. Privacy service in 5G deserves much more attention than in the legacy cellular networks due to the massive data connections [12]. Anonymity service is a basic security requirement in many user cases. In many cases, privacy leakage can cause serious consequences. For examples, health monitoring data reveals the sensitive personal health information [45]; vehicle routing data can expose the location privacy [44]. 5G wireless networks raise serious concerns on privacy leakage. In HetNets, due to the high density of small cells, the association algorithm can reveal the location privacy of users. In [48], a differential private algorithm is proposed to protect the location privacy. In [49], the privacy in group communications is secured by the proposed protocol. In [44], cryptographic mechanisms and schemes are proposed to provide secure and privacy-aware real-time video reporting service in vehicular networks.

3) Availability: Availability is defined as the degree to which a service is accessible and usable to any legitimate users whenever and wherever it is requested. Availability evaluates how robust the system is when facing various attacks and it is a key performance metric in 5G. Availability attack is a typical active attack. One of the major attacks on availability is DoS attack, which can cause service access denial to legitimate users. Jamming or interference can disrupt the communication links between legitimate users by interfering the radio signals. With massive unsecured IoT nodes, 5G wireless networks face a big challenge on preventing jamming and DDoS attacks to ensure the availability service.

For the availability at PHY, DSSS and FHSS are two classical PLS solutions. DSSS was first applied to the military in 1940s. A pseudo noise spreading code is multiplied with the spectrum of the original data signal in DSSS. Without knowledge on the pseudo noise spreading code, a jammer needs a much higher power to disrupt the legitimate transmission. For FHSS, a signal is transmitted by rapidly switching among many frequency channels using a pseudorandom sequence generated by a key shared between transmitter and receiver. Dynamic spectrum is applied to D2D communications and cognitive radio paradigm to improve the SE in 5G. In [39], the authors pointed out that FHSS can cause bad performance with the jamming attack. A pseudorandom time hopping spread spectrum is proposed to improve the performance on jamming probability, switching probability, and error probability. Resource allocation is adopted to improve the detection of the availability violation [40].

4) Integrity: Although message authentication provides the corroboration of the source of the message, there is no protection provided against the duplication or modification of the message. 5G aims to provide connectivity anytime, anywhere, and anyhow, and to support applications closely related to human being daily life such as metering for the quality of the drinking water and scheduling of the transportation. The integrity of data is one of the key security requirements in certain applications.

Integrity prevents information from being modified or altered by active attacks from unauthorized entities. Data integrity can be violated by insider malicious attacks such as message injection or data modification. Since the insider attackers have valid identities, it is difficult to detect these attacks. In use cases such as smart meters in smart grid [50], data integrity service needs to be provided against manipulation. Compared to voice communications, data can be more easily attacked and modified [51]. Integrity services can be provided by using mutual authentication, which can generate an integrity key. The integrity service of personal health information is required [45]. Message integrity can be provided in the authentication schemes [44].

III. State-of-the-Art in 5G Wireless Security

In this section, we summarize the state-of-the-arts including recent development and current solutions for security in 5G wireless network systems. As indicated in the previous section, cryptography and PLS are two major security solutions.

Many new PHY technologies in 5G wireless networks launched considerable research work in PLS. Most PLS research work are based on resource allocation. In [52] a security-oriented resource allocation scheme is considered in ultra-dense networks (UDNs). The authors presented several resource dimensions with the influence of security transmission. The main resource dimensions mentioned are power allocation, relay selection, frequency allocation, time allocation, and beamforming. The open issues and future directions in PLS are discussed, including interference management, substitute for dedicated jammer, security over mobility management, and handing the heterogeneity. A case study for cross layer cooperation scheme in HetNet is presented when considering multiple users and SBSs in UDNs. For better understanding the PLS, two metrics used to evaluate the security performance are introduced as secrecy capacity and secrecy outage probability. The secrecy capacity C_s is defined as:

$$C_s = C_m - C_e; \tag{1}$$

where the C_m is the main channel capacity of the legitimate user, and the C_e is the channel capacity of the eavesdropper. The secrecy outage probability is defined as the instantaneous

secrecy capacity is less than a target secrecy rate R_t, where $R_t > 0$, and:

$$P_{out}(R_s) = P(C_s < R_t); \quad (2)$$

Besides these two metrics, with the consumed power, in [53], secrecy EE is defined as the ratio between the system achievable secrecy rate and the corresponding consumed power.

The new development and solutions in cryptography have mainly targeted at new applications. There have been development and proposed solutions on the security services including authentication, availability, confidentiality, and key management. Due to the escalated privacy concerns in 5G wireless networks, we further separate the confidentiality solutions into data confidentiality based and privacy based.

A. Authentication

Authentication is one of the most important security services in 5G wireless networks. In the legacy cellular networks, an authentication scheme is normally symmetric-key based. The implementation of the authentication scheme can deliver several security requirements. In the third generation (3G) cellular networks, the mutual authentication is implemented between a mobile station and the network. Following the authentication, a cipher key and an integrity key are generated to ensure both data confidentiality and integrity between the mobile station and the base station.

Due to the low latency requirement of 5G networks, authentication schemes are required to be more efficient in 5G than ever before. To leverage the advantages of SDN, in [43], a fast authentication scheme in SDN is proposed, which uses weighed secure-context-information (SCI) transfer as a non-cryptographic security technique to improve authentication efficiency during high frequent handovers in a HetNet in order to address the the latency requirement. Compared with the digital cryptographic authentication methods, the proposed method is hard to be totally compromised since it is based on the user-inherent physical layer attributes. There are more than one physical layer characteristics used in SCI to improve the authentication reliability for applications requiring a high level of security. The SDN enabled authentication model is shown in Fig. 6. The SDN controller implements an authentication model to monitor and predict the user location in order to prepare the relevant cells before the user arrival. This helps achieve seamless handover authentication. Physical layer attributes are used to provide unique fingerprints of the user and to simplify authentication procedure. Three kinds of fingerprints are used as the user-specific physical layer attributes. The validated original attributes are obtained after a full authentication. The observations are collected through constantly sampling multiple physical layer attributes from the received packets at the SDN controller. Both the original file and observation results contain the mean value of the attributes and variance of the chosen attributes. Then the mean attribute offset can be calculated based on the validated original attributes and observed attributes. If the attribute offset is less than a pre-determined threshold, the user equipment is considered legitimate. The detection probability is presented in the paper. To evaluate the performance of the proposed method, a SDN network

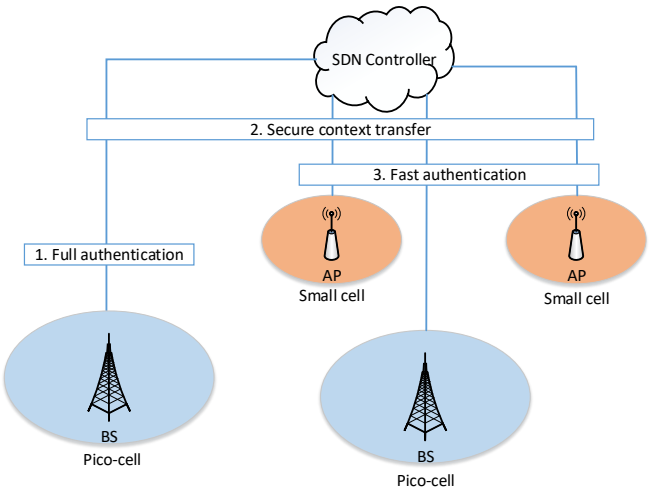


Fig. 6: A SDN enabled authentication model [43]

model using priority queuing is proposed. The arriving traffic is modeled as a Pareto distribution. Authentication delay is compared among different network utilization scenarios. The proposed fast authentication protocol includes full authentication and weighted SCI transfer based fast authentication. As shown in Fig. 6, after the first full authentication in one cell, it can be readily applied in other cells with MAC address verification, which only needs local processing. Moreover, full authentication can even be done without disrupting the user communication. A valid time duration parameter is used to flexibly adjust the secure level requirement. The simulation results compared the delay performance between the SDN enabled fast authentication and the conventional cryptographic authentication method. The SDN enabled fast authentication has a better delay performance owing to SDN flexibility and programmability in 5G networks.

To address the issues caused by the lack of a security infrastructure for D2D communications, in [54], a security-scoring based on continuous authenticity is developed to evaluate and improve the security of D2D wireless systems. The principle of legitimacy patterns is proposed to implement continuous authenticity, which enables attack detection and system security scoring measurement. For the legitimacy pattern, a redundant sequence of bits is inserted into a packet to enable the attack detection. The simulation results show the feasibility of implementing the proposed security scoring using legitimacy patterns. The authors pointed out that legitimacy patterns considering technical perspectives and human behaviors could improve the performance.

Combining the high security and utmost efficiency in bandwidth utilization and energy consumption in 5G, in [46], the authors proposed a new cyclic redundancy check (CRC)-based message authentication which can detect any double-bit errors in a single message. The CRC codes based cryptographic hash functions are defined. A linear feedback shift register (LFSR) is used to efficiently implement the CRC encoding and decoding. The message authentication algorithm outputs an authentication tag based on a secret key and the message.

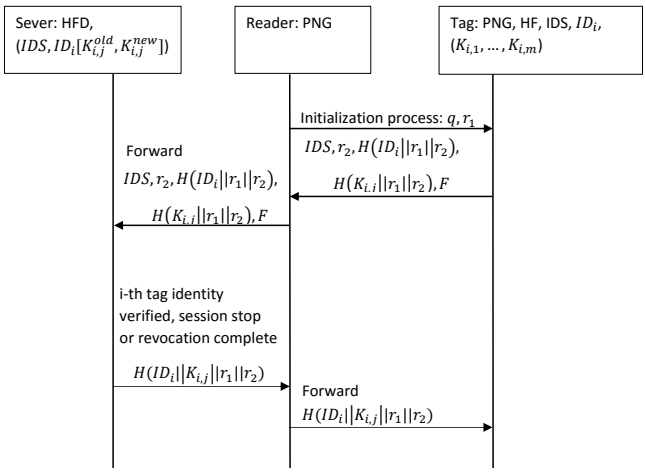


Fig. 7: The authentication process of the RFID secure application revocation scheme [55]

It is assumed that the adversary has the family of hash functions but not the particular polynomial $g(x)$ and the pad s that are used to generate the authentication tag. The generator polynomial is changed periodically at the beginning of each session and pad s is changed for every message. The new family of cryptographic hash functions based on CRC codes with generator polynomials in $g(x) = (1 + x)p(x)$ are introduced, where $p(x)$ is a primitive polynomial. The proposed CRC retains most of the implementation simplicity of cryptographically non-secure CRCs. However, the applied LFSR requires re-programmable connections.

Radio frequency identification (RFID) has been widely applied and a single RFID tag can integrate multiple applications. Due to various limitations in low-cost RFID tags, the encryption algorithms and authentication mechanisms applied to RFID systems need to be very efficient. Thus simple and fast hash function are considered for the authentication mechanisms. Moreover, with multiple applications of single RFID, the revocation should be taken consideration into the authentication scheme. In [55], the authors proposed a revocation method in the RFID secure authentication scheme in 5G use cases. A hash function and a random number are used to generate the corresponding module through a typical challenge-response mechanism. Fig. 7 shows the authentication process of the RFID secure application revocation scheme. The reader contains a pseudo-random number generator (PNG) and the sever holds a hash function and a database (HFD). The server establishes a tag record for each legitimate tag as (IDS, ID_i) and a group of corresponding application records as $(K_{i,j}^{old}, K_{i,j}^{now})$. q is the authentication request generated by the reader. r_1 is the first random number generated by the PNG in reader. After receiving the authentication request, the tag generates the second random number r_2 and calculates two hash authentication messages M_1, M_2, and value of XOR authentication information $F = E \bigoplus K_{i,j}$, where E is the current value of the status flag information, which is used to determine whether to revoke or to certify the application. The security and complexity results are presented, which show that

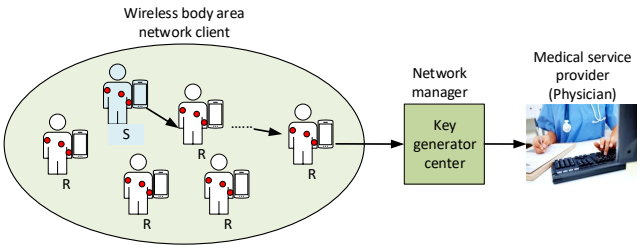


Fig. 8: A m-health system model [45]

the proposed scheme has a higher level of security and the same level of complexity compared with existing ones.

Considering the open nature of D2D communications between medical sensors and the high privacy requirements of the medical data, in [45], by utilizing certificate-less generalized signcryption (CLGSC) technique, the authors proposed a light-weight and robust security-aware (LRSA) D2D-assist data transmission protocol in a m-health system. The m-health system is modeled in Fig. 8, where S indicates the source node, and R represents the relay node. The anonymous and mutual authentication is implemented between the client and the physician in a wireless body area network to protect the privacy of both the data source and the intended destination. The signcryption of the message μ_S and encryption of its identity e_H^S are applied to the source client to authenticate the physician. A certificated-less signature algorithm is applied to the source client data before it is sent out. The source data identity can only be recovered by the intended physician who has the private key (x_H, z_H). The cipher text μ_S should be decrypted after the source identity is recovered with the right session key. Therefore, even the private key is leaked out, without the session key, the ciphertext is still safe. On the other hand, by verifying the signcryption μ_S, the physician can authenticate the source client. The relay nodes can verify the signature and then forward the data with their own signatures. The computational and communication overheads of the proposed CLGSC are compared with other four schemes. Simulation results show that the proposed CLGSC scheme has a lower computational overhead than the other four schemes.

Compared to IEEE 802.11p and the legacy cellular networks, 5G is a promising solution to provide real-time services for vehicular networks. However, the security and privacy need to be enhanced in order to ensure the safety of transportation. In [44], a reliable, secure, and privacy-aware 5G vehicular network supporting real-time video services is presented. The system architecture is shown in Fig. 9, which includes a mobile core network (MCN), a trusted authority (TA), a department of motor vehicles (DMV), and a law enforcement agency (LEA). D2D communications and mmWave techniques are adopted in the 5G vehicular communications. As shown in Fig. 9, HetNet is applied to expand network capacity and achieve high user data rates. The cloud platform provides massive storage and ubiquitous data access. The proposed cryptographic mechanisms include a pseudonymous authentication scheme, a public key encryption with keyword search, a ciphertext-policy attribute-based encryption, and threshold schemes based

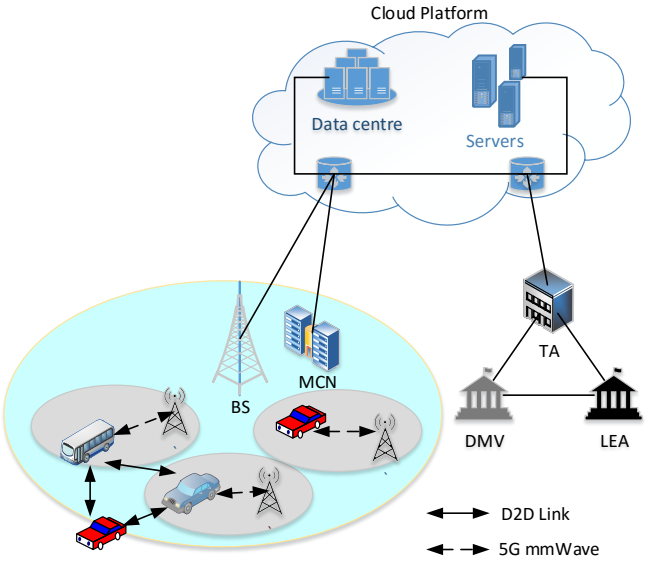


Fig. 9: A 5G-enabled vehicular network [44]

on secret sharing. The pseudonymous authentication scheme with strong privacy preservation [56] is applied to optimize the certification revocation list size, which is in a linear form with respect to the number of revoked vehicles so that certification verification overhead is the lowest. The authentication requirements include vehicle authentication and message integrity, where vehicle authentication allows the LEA and official vehicles to check the sender authenticity. The authentication is achieved by using a public-key-based digital signature that binds an encrypted traffic accident video to a pseudonym and to the real identity of the sender. The pseudonymous authentication technique can achieve the conditional anonymity and privacy of the sender.

B. Availability

Availability is a key metric to ensure the ultra-reliable communications in 5G. However, by emitting wireless noise signals randomly, a jammer can degrade the performance of the mobile users significantly and can even block the availability of services. Jamming is one of the typical mechanisms used by DoS attacks. Most of the anti-jamming schemes use the frequency-hopping technique, in which users hop over multiple channels to avoid the jamming attack and to ensure the availability of services.

In [57], the authors proposed a secret adaptive frequency hopping scheme as a possible 5G technique against DoS based on a software defined radio platform. The proposed bit error rate (BER) estimator based on physical layer information is applied to decide frequency blacklisting under DoS attack. Since the frequency hopping technique requires that users have access to multiple channels, it may not work efficiently for dynamic spectrum access users due to the high switching rate and high probability of jamming.

To reduce the switching rate and probability of jamming, in [39], a pseudorandom time hopping anti-jamming scheme is

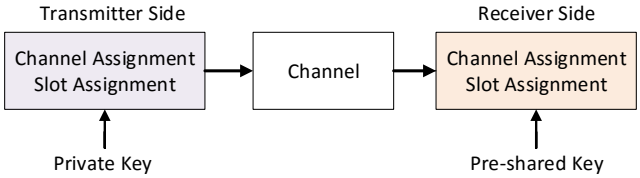


Fig. 10: A pseudorandom time hopping system block diagram [39]

proposed for cognitive users in 5G to countermeasure jamming attacks. The impact of spectrum dynamics on the performance of mobile cognitive users is modeled with the presence of a cognitive jammer with limited resources. The analytical solutions of jamming probability, switching rate, and error probability are presented. The jamming probability relates to delay performance and error probability. The jamming probability is low when the jammer lacks the access opportunities. Switching probability of time-hopping system outperforms the frequency-hopping system. With the same average symbol energy per joule, time-hopping has a lower error probability than frequency-hopping, and the performance gain saturates at a certain symbol energy level. The authors pointed out that the proposed time-hopping technique is a strong candidate for D2D links in 5G wireless networks due to its good EE and SE performance as well as its capability in providing jamming resilience with a small communication overhead. However, a pre-shared key is required for the time-hopping anti-jamming technique. The pseudorandom time hopping system block diagram is shown in Fig. 10. Both frequency hopping and time hopping require a pre-shared key to determine the hopping sequence.

Considering the limited computational capabilities at certain nodes, in [40], a fusion center is used to defend these nodes from a malicious radio jamming attack over 5G wireless network. A noncooperative Colonel Blotto game is formulated between the jammer and the fusion center as an exercise in strategic resource distribution. Fig. 11 shows the resource allocation model between fusion center and the malicious jammer. The jammer aims to jeopardize the network without getting detected by distributing its power among the nodes intelligently. On the other hand, the fusion center as a defender aims to detect such an attack by a decentralized detection scheme at a certain set of nodes. The fusion center can allocate more bits to these nodes for reporting the measured interference. A hierarchal degree is assigned to each node based on its betweenness centrality. Once the attack is detected, the fusion center will instruct the target node to increase its transmit power to maintain a proper SINR for normal communications. The simulation results show that error rate performance improves significantly with the fusion center having more bits to allocate among the nodes. The proposed resource allocation mechanism outperforms the mechanism that allocates the available bits in a random manner.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2779146, IEEE Access

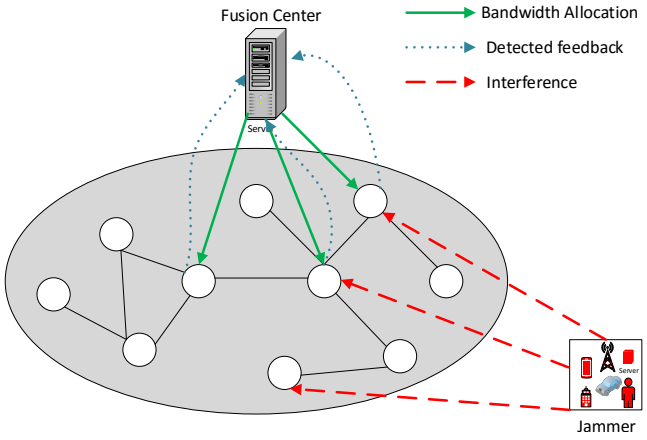


Fig. 11: The resource allocation model [40]

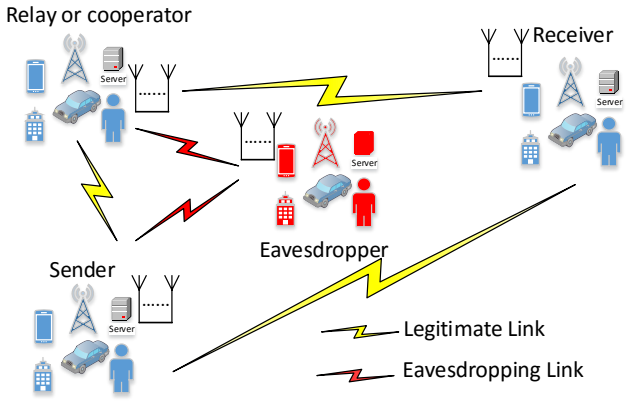


Fig. 12: A general system model with eavesdropping attacks

C. Data Confidentiality

Data confidentiality service is commonly required to tackle eavesdropping attacks. The general system model with eavesdropping attacks is shown in Fig.12. The specific system models can be different in the number of transmitter/receiver/eavesdropper antennas and in the number of eavesdroppers/relays/cooperators. The relays or cooperators are optional in the system. In this subsection, we discuss data confidentiality based on power control, relay, artificial noise, signal processing, and cryptographic methods.

1) Power Control: Power control for security aims to control the transmit power to ensure that the eavesdropper can not recover the signal. Based on the most simple eavesdropping attack model with a single eavesdropper armed with a single antenna, in [58], the authors proposed a distributed algorithm to secure D2D communications in 5G, which allows two legitimate senders to select whether to cooperate or not and to adapt their optimal power allocation based on the selected cooperation framework. Fig. 12 shows a general system model with eavesdropping attacks. In the system model in [58], the sender, relay or cooperator, receiver, and eavesdropper are named as Alice, John, Bob, and Eve, respectively. Each user has a single antenna. A shared bi-directional link is applied between Alice and John. The problem is formulated to maximize the achievable secrecy rates for both Alice and John as follows [58]

$$C_a = \max\left(R_{ajb} - R_{ae}\right), \tag{3}$$

$$s.t. P_j + P_{jb} \leq P_J; \tag{4}$$

$$C_j = \max\left(R_{jab} - R_{je}\right), \tag{5}$$

$$s.t. P_a + P_{ab} \leq P_A, \tag{6}$$

where C_a and C_j represent the secrecy rates of Alice and John respectively. R_{ajb} and R_{jab} are the achievable rates of Alice and John respectively with helping to relay data for each other. R_{ae} and R_{je} are the achievable rates of eavesdropper from Alice and from John respectively. Eq. 4 and Eq. 6 represent the transmit power limitation of the two legitimate senders. Two cooperation scenarios are considered, namely cooperation with relay and cooperation without relay. In the cooperation with relay scenario, Alice and John can help relay data of each other using the shared bi-directional link. In cooperation without relay, Alice and John coordinate their respective transmission power to maximize the secrecy rate of the other one. The optimization problem of noncooperation scenario is also presented for comparison. The distance between the legitimate transmitter and the eavesdropper is given a constraint to avoid distance attacks as the eavesdropper may have a better received signal quality on the transmitted message than the legitimate receiver. Simulation results show that achievable secrecy rates of Alice and John are improved by relaying data for each other. With the increase of distance between the transmitter and the receiver, the benefit from cooperation decreases and at some point non-cooperation could become more beneficial to the legitimate transmitter.

With no relay or cooperation, based only on power control and channel access, in [59], the authors developed a Stackelberg game framework for analyzing the achieved rate of cellular users and the secrecy rate of D2D users in 5G by using PLS. The system model includes one base station (BS), a number of cellular users, one D2D link, and one eavesdropper, as shown in Fig. 13. The utility function of cellular user achieved rates and D2D user secrecy rates are expressed as functions of channel information and transmission power [59]:

$$u_{c,i} = \log_2(1 + SINR_{c,i}) + \alpha\beta P_D h_{dc}, \tag{7}$$

$$u_d = [\log_2(1+SINR_d) - \log_2(1+SINR_e)] - \alpha P_D h_{dc}, \tag{8}$$

where α is the price factor and β is the scale factor. The first term in $u_{c,i}$ represents the data rate of the i^{th} cellular user, and the second term compensates the interference from the D2D link, where P_D is the transmit power of the D2D user and h_{dc} is the channel gain from the D2D user to cellular users. The utility function of D2D user includes the secrecy data rate and the payment for the interference to cellular users. The game strategy of cellular users depends on the price factor α and game strategy of D2D user depends on the transmission power P_D. The Stackelberg game is formed to maximize cellular utility function at the first stage and then the utility function of D2D user at the second stage.

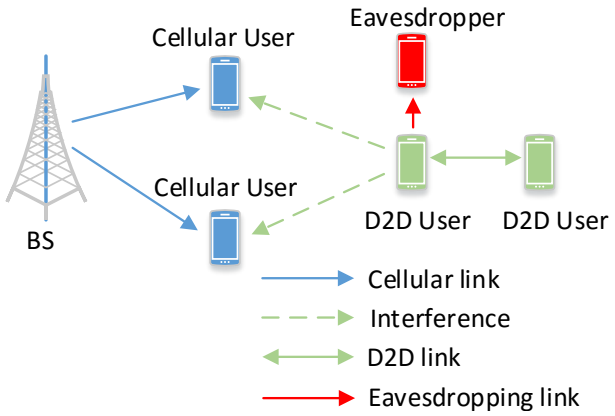


Fig. 13: The system model with D2D link and an eavesdropper [59]

Power control is also one of the normally used mechanisms to improve the EE of the network. In [60], the authors studied the trade-off between PLS and EE of massive MIMO in an HetNet. An optimization model is presented to minimize the total power consumption of the network while satisfying the security level against eavesdroppers by assuming that the BS has imperfect channel knowledge on the eavesdroppers. The simulation results show that a highly dense network topology can be an effective solution to achieve high capacity, high cellular EE, and reliable and secure communication channels.

2) Relay: As shown in Fig.12, cooperation with relay can be used to help the sender to secure the signal transmission. In [61], two relay selection protocols, namely optimal relay selection (ORS) and partial relay selection (PRS), are proposed to secure an energy harvesting relay system in 5G wireless networks. The system model is shown in Fig. 12, which consists of multiple relay nodes and assumes there is no direct link between sender and receiver. The power beacon is armed with multiple antennas, which can be used to strengthen the energy harvested. The ORS chooses the aiding relay to maximize the secrecy capacity of the system by assuming the source has full knowledge of channel state information (CSI) on each link. The PRS selects the helping relay based on partial CSI. The system includes a power beacon with multiple antennas, several relays, a destination node and an eavesdropper with a single antenna. Two energy harvesting scenarios that aim to maximize energy harvesting for source and selected relay are investigated. The analytical and asymptotic expressions of secrecy outage probability for both relay selections protocols are presented. The numerical results show that ORS can significantly enhance the security of the proposed system model and can achieve full secrecy diversity order while PRS can only achieve unit secrecy diversity order regardless of the energy harvest strategies. PRS that maximizes energy harvesting for relay strategy has a better secrecy performance than the one based on the maximizing energy harvesting for source. Moreover, the results show that the secrecy performance of the considered system is impacted significantly by the duration of energy harvest process.

To tackle the complexity issue of relay selection in 5G large-scale secure two-way relay amplify-and-forward (TWR-AF) systems with massive relays and eavesdroppers, in [62], the authors proposed a distributed relay selection criterion that does not require the information of sources SNR, channel estimation, or the knowledge of relay eavesdropper links. The proposed relay selection is done based on the received power of relays and knowledge of the average channel information between the source and the eavesdropper. The system model includes two source nodes, a number of legitimate relay nodes and multiple passive eavesdroppers. Each node has a single antenna. The cooperation of eavesdroppers is considered. In TWR-AF, the received signals from the two sources at the eavesdropper in each time slot are overlapped, where one source's signal acts as the jamming noise. The analytical results show that the number of eavesdroppers has a severe impact on the secrecy performance. The simulation results show that the performance of the proposed low-complexity criterion is very close to that of the optimal selection counterpart.

Considering eavesdroppers and relay with both single and multiple antennas, in [63], the transmission design for secure relay communications in 5G networks is studied by assuming no knowledge on the number or the locations of eavesdroppers. The locations of eavesdroppers form a homogeneous Poisson Point Process. A randomize-and-forward relay strategy is proposed to secure multi-hop communications. Secrecy outage probability of the two-hop transmission is derived. A secrecy rate maximization problem is formulated with a secrecy outage probability constraint. It gives the optimal power allocation and codeword rate. Simulation results show that the secrecy outage probability can be improved by equipping each relay with multiple antennas. The secrecy throughput is enhanced and secure coverage is extended by appropriately using relaying strategies.

3) Artificial Noise: Artificial noise can be introduced to secure the intended signal transmission. With the artificial-noise-aided multi-antenna secure transmission under a stochastic geometry framework, in [24], the authors proposed an association policy that uses an access threshold for each user to associate with the BS so that the truncated average received signal power beyond the threshold is maximized and it can tackle randomly located eavesdroppers in a heterogeneous cellular network. The tractable expression of connection probability and secrecy probability for a randomly located legitimate user are investigated. Under the constraints of connection and secrecy probabilities, the network secrecy throughput and minimum secrecy throughput of each user are presented. Numerical results are presented to verify the analytical accuracy.

Assuming the sender is armed with multiple antennas, in [64], an artificial noise transmission strategy is proposed to secure the transmission against an eavesdropper with a single antenna in millimeter wave systems. Millimeter wave channel is modeled with a ray cluster based spatial channel model. The sender has partial CSI knowledge on the eavesdropper. The proposed transmission strategy depends on directions of the destination and the propagation paths of the eavesdropper. The secrecy outage probability is used to analyze the transmission scheme. An optimization problem based on minimizing the

secrecy outage probability with a secrecy rate constraint is presented. To solve the optimization problem, a closed-form optimal power allocation between the information signal and artificial noise is derived. The secrecy performance of the millimeter wave system is significantly influenced by the relationship between the propagation paths of destination and eavesdropper. The numerical results show that the secrecy outage is mostly occurred if the common paths are large or the eavesdropper is close to the transmitter.

To improve EE of the security method using artificial noise, in [53], an optimization problem is formulated to maximize the secrecy EE by assuming imperfect CSI of eavesdropper at transmitter. The system is modeled with one legitimate transmitter with multiple antennas, and one legitimate receiver and one eavesdropper, each with a single antenna. Artificial noise is used at the transmitter. Resource allocation algorithms are used to solve the optimization problem with correlation between transmit antennas. With the combination of fractional programming and sequential convex optimization, the first-order optimal solutions are computed with a polynomial complexity.

4) Signal Processing: Besides the three methods above to provide data confidentiality, in [38], the authors proposed an original symbol phase rotated (OSPR) secure transmission scheme to defend against eavesdroppers armed with unlimited number of antennas in a single cell. Perfect CSI and perfect channel estimation are assumed. The BS randomly rotates the phase of original symbols before they are sent to legitimate user terminals. The eavesdropper can not intercept signals, only the legitimate users are able to infer the correct phase rotations recover the original symbols. Symbol error rate of the eavesdropper is studied, which proves that the eavesdropper can not intercept the signal properly as long as the base station is equipped with a sufficient number of antennas.

Considering multiple eavesdroppers in [65], the authors analyzed the secure performance on a large-scale downlink system using non-orthogonal multiple access (NOMA). The system considered contains one BS, M NOMA users and eavesdroppers randomly deployed in an finite zone. A protected zone around the source node is adopted for enhancing the security of the random network. Channel statistics for legitimate receivers and eavesdroppers and secrecy outage probability are presented. User pair technique is adopted among the NOMA users. Analytical results show that the secrecy outage probability of NOMA pairs is determined by the NOMA users with poorer channel conditions. Simulation results show that secrecy outage probability decreases when the radius of the protected zone increases and secrecy outage probability can be improved by reducing the scope of the user zone as the path loss decreases.

In [66], the authors proposed a dynamic coordinated multipoint transmission (CoMP) scheme for BS selection to enhance secure coverage. Considering co-channel interference and eavesdroppers, analysis of the secure coverage probability is presented. Both analytical and simulation results show that utilizing CoMP with a proper BS selection threshold the secure coverage performance can be improved, while secure coverage probability decreases with the excessive cooperation. The proposed CoMP scheme has a better performance to resist more eavesdroppers than the no-CoMP scheme.

In [25], massive MIMO is applied to HetNets to secure the data confidentiality in the presence of multiple eavesdroppers. The tractable upper bound expressions for the secrecy outage probability of HetNet users are derived, which show that massive MIMO can significantly improve the secrecy performance. The relationship between the density of picocell base station and the secrecy outage probability of the HetNet users is discussed.

5) Cryptographic Methods: Besides the PLS solutions introduced above, cryptographic methods are also used for implementing data confidentiality by encrypting data with secret keys. Asymmetric cryptography can be applied to key distributions. To reduce the cost of encryption, symmetric cryptography is adopted for data encryption.

In [44], a participating vehicle can send its random symmetric key, which is encrypted using TA's public key. The symmetric key is used to encrypt the message between TA, DMV, and participating vehicles. A one-time encryption key is also encrypted by a public key. The one-time encryption key is used to encrypt the video. In [45], an initial symmetric session key is negotiated between the client and a physician after they establish the client/server relationship. The symmetric key is then used for the data transmission between the client and the physician.

D. Key Management

Key management is the procedure or technique that supports the establishment and maintenance of keying relationships between authorized parties, where the keying relationship is the way common data is shared between communication entities. The common data can be public or secret keys, initialization values, and other non-secret parameters.

To provide flexible security, in [67], three novel key exchange protocols, which have different levels of computational time, computational complexity, and security, for D2D communications are proposed based on the Diffie-Hellman (DH) scheme. Details of the key exchange schemes are shown in Fig. 14. The threat analysis of all three proposed protocols under common brute force and MITM attacks is presented. Performance study is provided for the proposed protocols to evaluate the confidentiality, integrity, authentication, and non-repudiation of security services based on theoretical analysis. The analysis proves that the proposed protocols are feasible with reasonable communication overhead and computational time.

For D2D group use cases, in [49], a group key management (GKM) mechanism to secure the exchanged D2D message during the discovery and communication phases is proposed. There are five security requirements in the proposed GKM, namely forward secrecy (users that have left the group should not have access to the future key), backward secrecy (new users joining the session should not have access to the old key), collusion freedom (fraudulent users could not deduce the current traffic encryption), key independence (keys in one group should not be able to discover keys in another

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2779146, IEEE Access

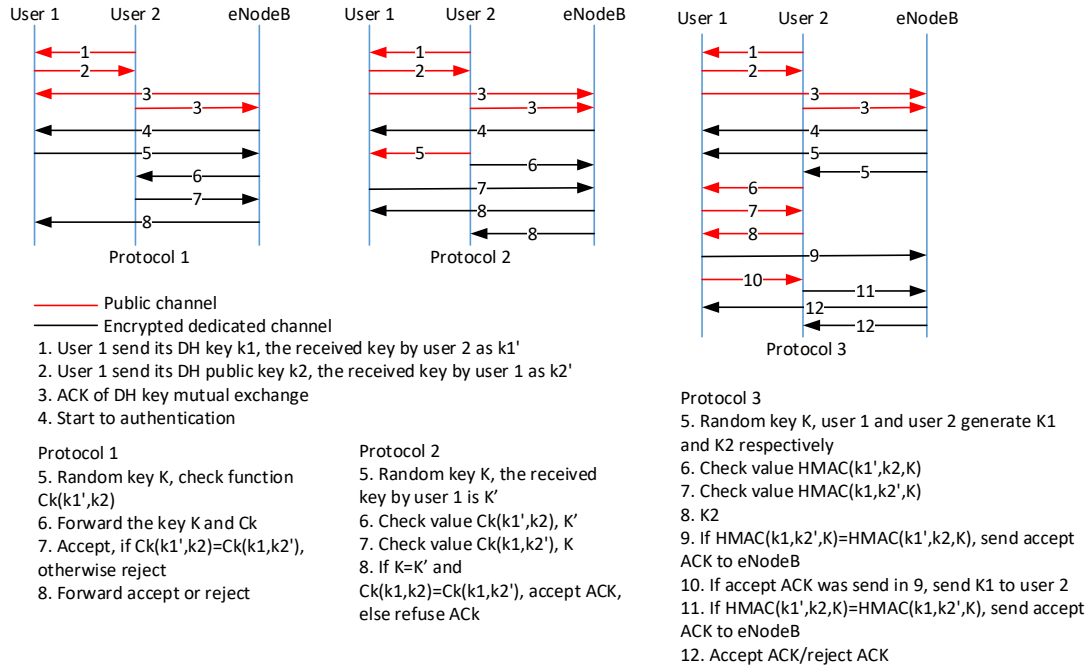


Fig. 14: Three key exchange schemes in [67]

group), and trust relationship (do not reveal the keys to any other part in the same domain or any part in a different domain). ID-based cryptography (IBC) scheme based on Elliptic Curve Cryptography (ECC) for securing multicast group communications is presented. The steps of the proposed protocol include secret key generation, elliptic curve digital signature algorithm, signature verification, group formation procedure, key generation, join process, and leave process. The master key and private key generations are based on IBC and ECC schemes. The overhead for communications, re-keying message, and key storage are assessed. The weakness of the IBC scheme and the ways of creating and using GKM are compared. The overall performance comparisons show that the proposed GKM has an enhancement in both the protocol complexity and security level compared with other works.

ECC is also adopted for the proposed LRSA protocol in [45]. The network manager generates a partially private and partially public key for the client and the physician after the registration. And once the client and the physician establish the client/server relationship, an initial systematic session key can be set up for the data transmission.

E. Privacy

As discussed in the previous sections, 5G wireless networks raise serious concerns on privacy leakage when supporting more and more vertical industries such as m-health care and smart transportation [15]. The data flows in 5G wireless networks carry extensive personal privacy information such as identity, position, and private contents. In some cases, privacy leakage may cause serious consequences. Depending on the privacy requirements of the applications, privacy protection is a big challenge in 5G wireless networks. There have already been research work considering location privacy and identity privacy.

Regarding location privacy, in [48], to protect the location and preferences of users that can be revealed with associated algorithms in HetNets, a decentralized algorithm for access point selection is proposed based on a matching game framework, which is established to measure the preferences of mobile users and base stations with physical layer system parameters. Differentially private Gale-Shapley matching algorithm is developed based on differential privacy. Utilities of mobile users and access points are proposed based on packet success rate. Simulation results show that the differentially private algorithm can protect location privacy with a good quality of service based on utility of the mobile users. In [37], a location-aware mobile intrusion prevention system (mIPS) architecture with privacy enhancement is proposed. The authors presented the mIPS requirements, possible privacy leakage from managed security services.

In [45], contextual privacy is defined as the privacy of data source and destination. The identity of the source client is encrypted by a pseudo identity of the source client with the public key of the physician using certificateless encryption mode. Meanwhile, the identity of the intended physician is also encrypted with the public key of the network manager. Through these two encryption steps, the contextual privacy can be achieved. For the proposed reporting service in [44], privacy is an essential requirement to gain acceptance and participation of people. The identity and location information of a vehicle should be preserved against illegal tracing. Meanwhile, a reporting vehicle should be able to reveal its identity to the authorities for special circumstances. The pseudonymous authentication schemes are applied to achieve the conditional

anonymity and privacy.

IV. Security for Technologies Applied to 5G Wireless Network Systems

In this section, we present the security research activities from the perspectives of technologies applied to 5G. First we briefly introduce the technologies applied to 5G. Then the security activities of each technology are presented. The technologies applied to 5G wireless networks discussed in this section are HetNet, massive MIMO, D2D, SDN, and IoT.

A. HetNet

HetNet is a promising technique to provide blanket wireless coverage and high throughput in 5G wireless networks. It is a multi-tier system in which nodes in different tier have different characteristics such as transmission power, coverage size, and radio access technologies. With the heterogeneous characteristics, HetNet achieves higher capacity, wider coverage and better performance in EE and SE. However, HetNet architecture, compared to single-tier cellular network, makes UE more vulnerable to eavesdropping [24]. Moreover, with the high density of small cells in HetNet, traditional handover mechanisms could face significant performance issues due to too frequent handovers between different cells [43]. The privacy issue in HetNet also faces a big challenge. Location information becomes more vulnerable due to the high density of small cells. The conventional association mechanism can disclose the location privacy information [48].

To tackle the eavesdropping attacks in HetNet, a secret mobile association policy is proposed based on the maximum truncated average received signal power (ARSP). The maximum ARSP should be higher than a pre-set access threshold in order for mobile to keep active. Otherwise, the mobile device remains idle. In [24], the authors analyzed the user connection and secrecy probability of the artificial-noise-aided secure transmission with the proposed association policy, which is based on an access threshold. The secrecy throughput performance can be significantly enhanced with a proper access threshold used in the association policy.

For enhancing communication coverage in HetNet, coordinated multipoint transmission (CoMP) can be applied [66]. However, CoMP can increase the risk of being eavesdropped for the legitimate users. In [66], multiple BSs are selected to transmit the message. A dynamic BS selection scheme is proposed based on the secure coverage probability. Based on the theoretical and simulation results, the authors concluded that the proper BS selection threshold for CoMP can improve the secure coverage performance.

Security-based resource management has been used to implement security in HetNet. In [52], the authors studied a case to improve the existing jamming and relaying mechanisms by proposing a cross-layer cooperation scheme with the aid of SBSs for protecting the confidentiality of macro cell user communications. The SBSs are motivated by monetary or resource bonus to become jammers to assist the secure communications under the constraints of the QoS of their own users.

Due to the high density of small cells, the knowledge of the cell an user is associated with can easily reveal the location information of that user. In [48], the authors investigated the location privacy based on physical layer of association algorithms in 5G. A differential private Gale-Shapley algorithm is proposed to prevent the leakage of location information with certain QoS for users. The evaluation of the algorithm based on different privacy levels is presented with the influence on utility of users.

The intrusion detection based approach is considered as one way to provide secure communications. In [68], intrusion detection techniques for mobile cloud computing in heterogeneous 5G are introduced. Several detection methodologies are studied as signature-based detection, anomaly-based detection, specification-based detection, stateful protocol analysis, hybrid intrusion detections with principles of these approaches. Traditional password-based authentication and biometric authentication are discussed for providing different levels of security.

B. D2D

In D2D communications, devices can communicate with each other without going through BSs. D2D communications enable efficient spectrum usage in 5G. Moreover, D2D communications can effectively offload traffic from BSs. However, the lack of a D2D security infrastructure makes the D2D communications less secure than the device to network communications [54][69]. To improve the SE, dynamic spectrum access is usually adopted for D2D links, which can yield security threats such as jamming [39]. The security issue becomes a major concern for direct radio communications and large-scale deployment of D2D groups [49].

Cooperation between D2D nodes is a popular way to secure the D2D communications against eavesdroppers. The legitimate transmitters with a common receiver can improve their reliable transmission rate through cooperation. In [58], the authors proposed a cooperation scheme to secure D2D communications considering distance. Before the cooperation, devices can check the distance to test whether cooperation can improve the security of the communications. The distance constraints can be used to determine cooperation jointly, cooperation from one side, or no cooperation to maximize the achievable secrecy rate. With no specific requirements for the D2D communications, the proposed scheme can be applied to all D2D communications scenarios.

Besides cooperation, power control and channel access are also considered in securing D2D communications. In [59], optimal power control and channel access of D2D link are proposed to maximize the achievable rate of cellular users and the physical layer secrecy rate of D2D links. The system model is shown in Fig. 13. The utility function of a single D2D user is modeled by considering PLS requirement and payment of interference from other D2D users. A Stackelberg game approach is used, where the price from cellular users are leaders and transmission power of D2D users are followers. The channel access problem of D2D links is discussed to maximize the achievable secrecy rate of D2D links and to minimize the interference to the cellular users.

To provide a measurement for security level, continuous authenticity with legitimacy patterns is proposed in [54] to enable wireless security scoring. Security scoring based on probability of attack detection is applied to prevent, react, and detect attacks. The continuous legitimacy pattern is inserted into packets to authenticate the integrity and authenticity of transmissions.

Considering the assistance of the network, in [67], key exchange protocols involved with the two D2D users and eNodeB are proposed. Two scenarios are considered. For the traffic offload scenario, D2D users are connected to the same eNodeB. For the social networking scenario, D2D link is required for the applications in each D2D user. Public channel and encrypted dedicated channel are applied to the process of key exchange. The eNodeB is involved in the initial key exchange and mutual authentication of the D2D users. Based on the role of eNodeB in the authentication process, three different key exchange protocols are proposed with different computational time and complexity.

The security algorithms and solutions for public cellular systems are not adapted to the short radio range D2D communications. The security issues in both proximity service discovery and communication phases for D2D communications are presented and addressed by proposing a group key management mechanism using IBC [49]. Key distributions and key revocations are two problems in group key management (GKM). Five security requirements of GKM are defined and corresponding solutions are provided. A key graph is applied by dividing a group of members into subgroups to reduce the complexity of join process and leave process.

With the development of D2D technique, m-health applications are adopted to improve efficiency and quality of healthcare services. The security requirements for D2D communications used in m-health system are analyzed in [45]. The protocol needs to secure the data that is not accessed by relays and to achieve mutual authentication between the source and the intended physician without interaction. It also requires light weight for mobile terminals with energy and storage constraints and needs to be robust enough to fight against threats as part of the keys can be exposed. A certificateless public key cryptography is applied to achieve the security requirements. The private key of a user is generated by both key generator center and the user, which makes the key generator center unaware about user's private key. Authentication is achieved by recognizing the public key. Security objectives of m-health network are defined as data confidentiality and integrity, mutual authentication, anonymity to anyone except intended physician, unlinkability, forward security and contextual privacy.

C. Massive MIMO

By utilizing a large number of antennas at BSs, massive MIMO can provide high EE and SE to support more users simultaneously. The large number of antennas at BSs can significantly improve the throughput, EE performance, and shift the most of signal processing and computation from user terminals to BSs [38]. Moreover, massive MIMO can improve the security of communications. In [25] the authors considered PLS for a downlink K-tier HetNet system with multiple eavesdroppers. Each MBS is armed with large antenna arrays using linear zero-forcing beamforming. Both theoretical analysis and simulation results show that massive MIMO can significantly enhance the secrecy outage probability of the macrocell users.

However, eavesdropper can utilize massive MIMO to attack the legitimate communications. In the system model [38], the authors considered massive MIMO at both BS and the eavesdropper. The antenna arrays of the eavesdropper are far more powerful. The OSPR approach is introduced. Theoretical and simulation analysis shows that the antenna number at the BS can significantly impact the security performance. With the number of antennas at the BS is sufficiently high, the massive MIMO eavesdropper fails to decode the majority of the original symbols while the legitimate users are able to recover the original symbols with only a limited number of antennas. Compared to other approaches involved in jamming, the proposed method has a higher EE.

D. SDN

By decoupling the control plane from the data plane, SDN enables centralized control of the network and brings promising methods to make the network management simpler, more programmable, and more elastic [9]. Information can be shared between cells by using SDN. SDN can provide three key attributes, namely logically centralized intelligence, programmability, and abstraction [70] so that scalability and flexibility of the network can be greatly improved and cost can be significantly reduced. A survey of software-defined mobile network (SDMN) and its related security problems are provided in [26].

In [9], the authors discussed the pros and cons of the SDN security. The pros of SDN security over traditional networks are shown in Table. II. Besides the pros of the SDN brought to 5G wireless networks, the new security issues caused by SDN are presented in Table. III, together with possible countermeasures.

In [22], the authors discussed the limitations in present mobile networks. A SDMN architecture consisting of an application, control plane, and data plane is proposed, which integrates SDN, NFV and cloud computing. The security mechanisms in legacy cellular networks are presented with their limitations. The expected security advantages of SDMN are introduced. The security perspectives that can be improved through SDMN are listed. Besides the advantages of SDMN, threat vectors for SDMN architecture are also presented. In [35], the open issues of 5G security and trust based on NFV and SDN are elaborated. Corresponding security and trust frameworks are proposed, which use NFV Trust Platform as a service, security function as a service and trust functions as a service.

To address the threats in SDMN, in [36], security attack vectors of SDN are presented. The authors modeled the network attacks by using attack graph. Analytic hierarchy process and technique are applied to calculate the node minimal effort for SDMN. A case study based on MobileFow architecture

TABLE II: The pros of SDN security over traditional networks [9]

SDN characteristic	Attributed to	Security use
Global network view	Centralization Traffic statistics collection	Network-wide intrusion detection Detection of switch's malicious behavior Network forensics
Self-healing mechanisms	Conditional rules Traffic statistics collection	Reactive packet dropping Reactive packet redirection
Increased control capabilities	Flow-based forwarding scheme	Access control

TABLE III: New security issues that SDN networks are exposed to along with possible countermeasures [9]

Targeted level	Malicious behavior	Caused by	Possible countermeansures
Forwarding plane	Switch DoS	Limited forwarding table storage capacity Enormous number of flows Limited switchs buffering capacity	Proactive rule caching Rule aggregation Increasing switchs buffering capacity Decreasing switch-controller communication delay
	Packet encryption and tunnel bypassing	Invisible header fields	Packet type classification based on traffic analysis
Control plane	DDoS attack	Centralization Limited forwarding table storage capacity Enormous number of flows	Controller replication Dynamic master controller assignment Efficient controller placement
	Compromised controller attacks	Centralization	Controller replication with diversity Efficient controller assignments
Forwarding-control Link	MITM attacks	Communication message sent in clear Lack of authentication	Encryption Use of digital signatures
	Replay attacks	Communication message sent in clear Lack of time stamping	Encryption Time stamp inclusion in encrypted messages

is presented as an example to test the proposed vulnerability assessment mechanism.

Due to the high density of small cells in 5G, key management is difficult with user frequently joining and leaving the small cells. Moreover, speeding up the authentication process is essential to ensure the low latency requirement in 5G. In [43], SDN is introduced into the system model to enable the coordination between different heterogeneous cells. A SDN controller is used to monitor and predict the user locations. The multiple physical layer characteristics are constantly sampled by the SDN controller to show the performance of the multiple SCI combination. The weighted SCI design and decision rules are proposed. The SDN mode uses the priority queuing and arriving traffic is modeled as a Pareto distribution. The latency performance of the SDN based authentication is shown to be better than the performance of traditional cryptographic methods based on different load situations. By pre-shared SCI over SDN, security framework can have a higher tolerance level to deal with failures of the network.

E. IoT

Due to the limited computation capability of IoT nodes, security services in 5G IoT devices need to be efficient and lightweight. Relaying has been considered as an effective mechanism in IoT networks to save the power of IoT nodes and also to extend the transmission coverage.

In [40], a fusion center is used to protect IoT nodes with limited computation power from jammer. Each IoT node is equipped with a sensor to detect the interference. The betweenness centrality of each IoT node is taken consideration to measure the importance of the node over the network. The decentralized interference measurements are collected at the fusion center in regular intervals on a common control channel. A certain level threshold and aggregated received interference power level are used to determine whether a jamming attack exists or not. The authors assumed that the jammer knows the topology of the network and correspondingly allocates certain interference power to the IoT nodes to decrease their SINR. The fusion center can also allocate bandwidth to certain nodes to measure the interference level in order to detect the jammer attack. Therefore, a non-cooperative Colonel Blotto game between the jammer and the fusion center is formed as a resource distribution problem.

In [63], the security of relay communications in IoT networks is introduced by considering power allocation and codeword rate design over two-hop transmission against randomly distributed eavesdroppers. The problem is formulated to maximize the secrecy rate. Both single- and multiple-antenna cases at relays and eavesdroppers are considered. It is shown that proper relay transmission can extend secure coverage and the increase of the number of antennas at relay nodes can improve the security level.

RFID is an automatic identification and data capture technology widely used in IoT networks. In [55], a RFID secure application revocation scheme is proposed to efficiently and securely use multi-application RFID and revoke applications in the tag. Based on theoretical analysis, the proposed scheme can achieve a higher level of security than other existing schemes.

V. Proposed 5G Wireless Security Architecture

In this section, we present the proposed 5G wireless network security architecture. First we illustrate a 5G wireless network architecture, based on which we further propose a corresponding security architecture. Identity management and flexible authentication based on the proposed 5G security architecture are analyzed. A handover procedure and signaling

load analysis are studied to illustrate the advantages of the proposed 5G wireless security architecture.

A. 5G Wireless Network Architecture

In this subsection, we introduce a 5G wireless network architecture. As shown in Fig. 15, the illustrated general 5G wireless network architecture includes a user interface, a cloud-based heterogeneous radio access network, a next generation core, distributed edge cloud and central cloud. The cloud-based heterogeneous radio access network can combine virtualization, centralization and coordination techniques for efficient and flexible resource allocation. Based on different use cases, 3GPP classifies more than 70 different use cases into four different groups such as massive IoT, critical communications, network operation, and enhanced mobile broadband [71]. In the cloud-based heterogeneous access network, besides the 3GPP access and non-3GPP access, other new radio technologies will be added for more efficient spectrum utilization. In the first stage of 5G, the legacy evolved packet core (EPC) will still be valid. Network slicing is applied to enable different parameter configurations for the next generation core according different use cases. New flexible service-oriented EPC based on network slicing, SDN, and NFV will be used in the next generation core as virtual EPC (VEPC) shown in the Fig .15. The VEPC is composed of modularized network functions. Based on different use cases, the network functions applied to each VEPC can be various. In the VEPC, control plane and user plane are separated for flexibility and scalability of the next generation core. Edge cloud is distributed to improve the service quality. Central cloud can implement global data share and centralized control.

Compared with the legacy cellular networks, 5G wireless networks introduce some new perspectives and changes. (1) User equipment and services are not limited to regular mobile phone and regular voice and data services. Based on different use cases and requirements, user interfaces are classified into four different groups such as massive IoT, critical communications, network operation, and enhanced mobile broadband. Every use case can affect the radio access selection and VEPC functions. (2) In addition to 3GPP access and non-3GPP access in the cloud-based heterogeneous radio access network, 5G access network includes other new radios, which build the foundation of wireless standards for the next generation mobile networks for higher spectrum utilization. The new radios can support the performance and connectivity requirements of various use cases in 5G wireless networks. Moreover, there are many technologies applied to the access network to improve the network performance, such as massive MIMO, HetNet, and D2D communications. (3) The next generation core will be based on cloud using network slicing, SDN and NFV to handle different use cases. The flexible service-oriented VEPC will be applied. With network slicing, SDN and NFV, different network functions can be applied to the service-oriented VEPC for different use cases. The next generation core is expected to be access-independent. Separation of control and user plane is important to achieve an access-agnostic, flexible and scalable architecture. (4) Edge cloud is applied to 5G wireless network to improve the performance of the network, such as latency.

B. 5G Wireless Security Architecture

Based on the illustrated 5G wireless network architecture, we propose a 5G wireless security architecture as shown in Fig. 16. With the new characteristics of the next generation core, a separation of data plane and control plane of VEPC is proposed, where the data plane can be programmable for its flexibility. The major network functions in the control plane of the next generation core are identified in TR 23.799, which are utilized in our proposed security architecture as follows:

- Access and mobility management function (AMF): The function is applied to manage access control and mobility, which is implemented in MME for legacy cellular network. This can be vary with different use cases. Mobility management function is not necessary for fixed access applications.
- Session management function (SMF): Based on network policy, this function can set up and manage sessions. For a single AMF, multiple SMF can be assigned to manage different sessions of a single user.
- Unified data management (UDM): UDM manages subscriber data and profiles (such as authentication data of users) for both fixed and mobile access in the next generation core.
- Policy control function (PCF): This function provides roaming and mobility management, quality of service, and network slicing. AMF and SMF are controlled by PCF. Differentiated security can be provided with PCF.

AMF and SMF are integrated in the legacy cellular networks as MME. The separation of AMF and SMF can support a more flexible and scalable architecture. In the network function based control plane, different network functions can be applied to different use cases.

Similar to the legacy cellular networks, four security domains are defined in Fig. 16 as A, B, C, D. The details of these security domains are introduced as follows.

Network access security (A). The set of security features that provide the user interface to access the next generation core securely and protect against various attacks on the radio access link. The new physical layer technologies applied to the radio access network including massive MIMO, HetNet, D2D communications and mmWave bring new challenges and opportunities in network access security. This level has security mechanisms such as confidentiality and integrity protection between the user interface and radio access network. Current researches on network access security focus on providing user identity and location confidentiality, user data and signaling data confidentiality, and entity authentication.

Network domain security (B): The set of security features that protect against attacks in the wire line networks and enable different entities and functions to exchange signaling data and user data in a secure manner. As we can see in Fig. 16, this level security exists between access network and next generation core, control plane and user plane. Since new technologies such as cloud technique, network slicing and NFV are applied to 5G core and radio access network, new vulnerabilities in this level need to be addressed. However, with the separation of control plane and user plane, the amount of signaling data will

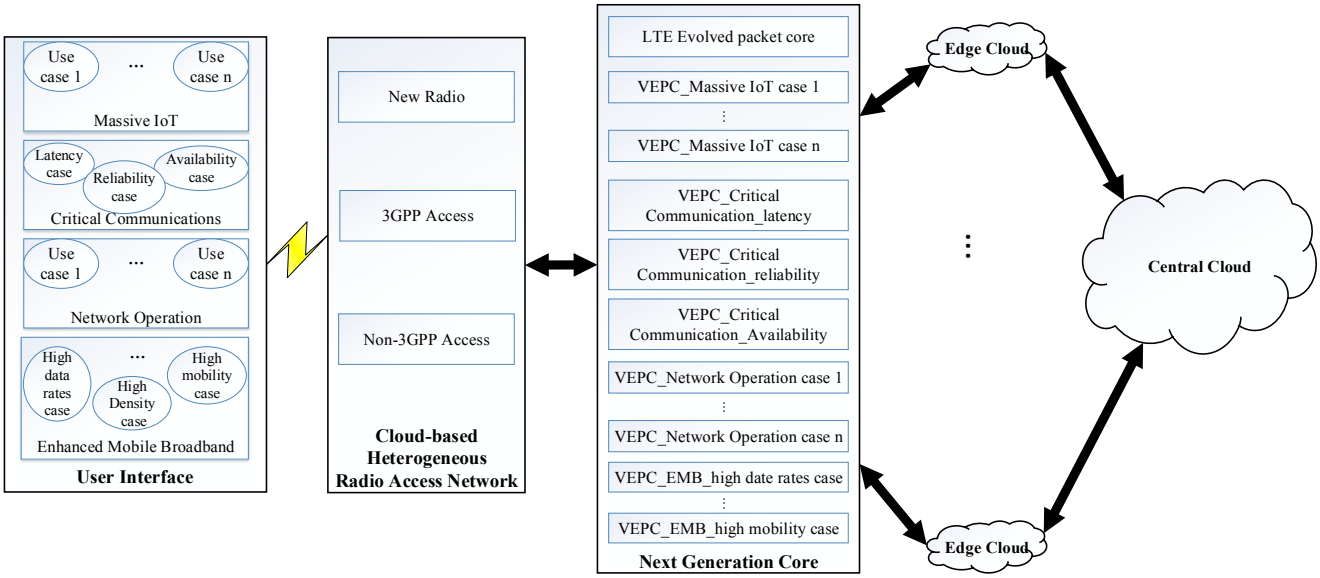


Fig. 15: A general 5G wireless network architecture

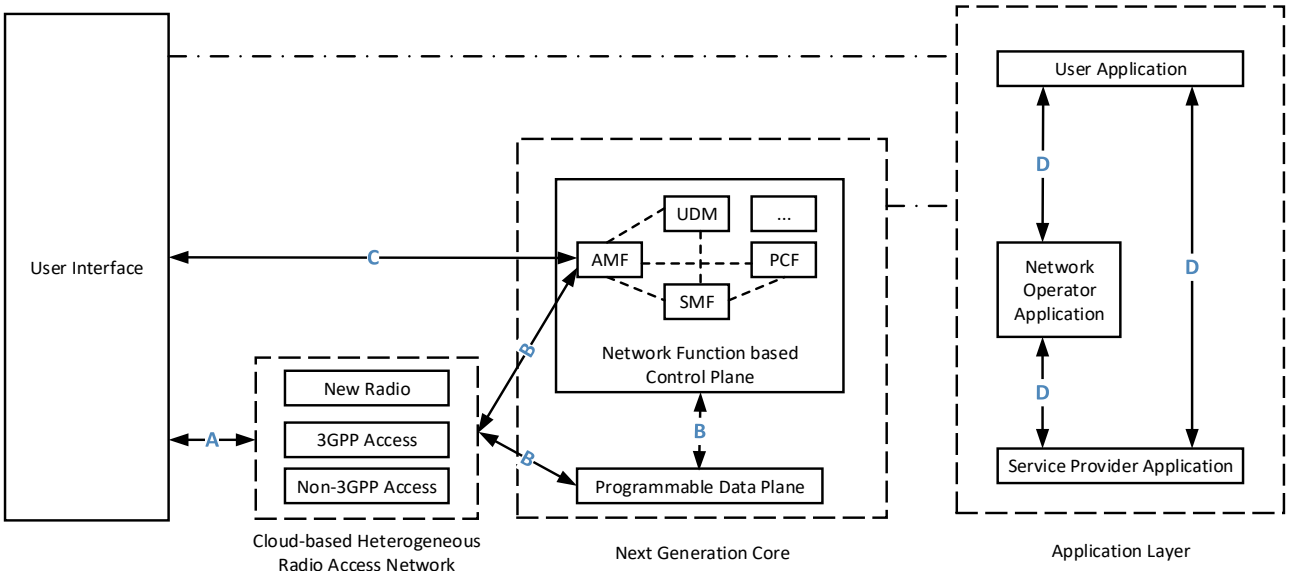


Fig. 16: The proposed 5G wireless network security architecture

be significantly reduced. The network function based control plane also reduces the required signaling overhead for data synchronization. Entity authentication, data confidentiality and data integrity are the main security services in this level. With the independent characteristics of access technologies of AMF, the network domain security performance can be simplified and improved.

User domain security (C): The set of security features that provide mutual authentication between the user interface and the next generation core before the control plane access to the user interface. Authentication is the main focus in this level. Based on the use case, the authentication may be needed for more than two parties. For example, the authentication can be required between user and network operator as well as between user and service provider. Moreover, different service providers may need to authenticate each other to share the same user identity management. Compared to the device-based identity management in legacy cellular networks, new identity management methods are needed to improve the security performance.

Application domain security (D): The set of security features that ensure the security message exchange between applications on the interfaces, between user interface and service provider, as well as between user and network operator.

C. 5G Wireless Security Services

In this subsection, we first analyze the identity management and flexible authentication based on the proposed 5G wireless

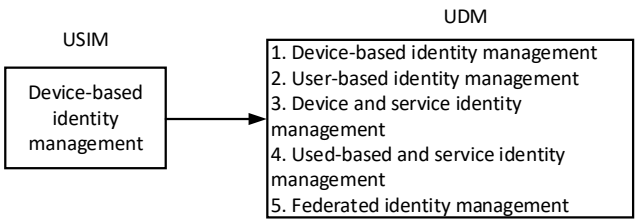


Fig. 17: Identity management in 5G wireless networks

Fig. 18: Authentication mechanism selection

security architecture. An analysis on the handover procedure and signaling load based on the proposed security architecture are presented.

1) Identity management: In the legacy cellular networks, the identity management relies on the universal subscriber identity module (USIM) cards. However, in 5G wireless networks, there are many equipment such as smart home devices, sensors and vehicles that are supported without USIM card. As shown in Fig. 16, UDM will handle the identity management based on cloud. Moreover, anonymity service is required in many use cases in 5G wireless networks. Therefore, the identity management will be different in 5G wireless networks compared with that in the legacy cellular networks. New identity management is required.

With the massive connected devices and applications, efficiently managing massive identities is significantly important to ensure the service performance. In the legacy cellular networks, the identity management is device-based. For a certain new use case such as smart home, one user can have multiple devices needed to access the network and services. User-based identity management will be more efficient to let the user determine what devices are allowed to access the network and services. One user may have multiple device identities. Except only considering the device identity, service identity can be added with device identity as device and service identity management. The device identity is unique and service identity can be assigned by service providers in certain session. With service identity, revocation process will be simplified.

Moreover, for the trusted service providers, federated identity management can be applied to simplify the identity management and also improve the user experience. The identity management in 5G wireless networks is not unified for all use cases. Based on the characteristics of the use case, different identity management can be applied as shown in the Fig. 17.

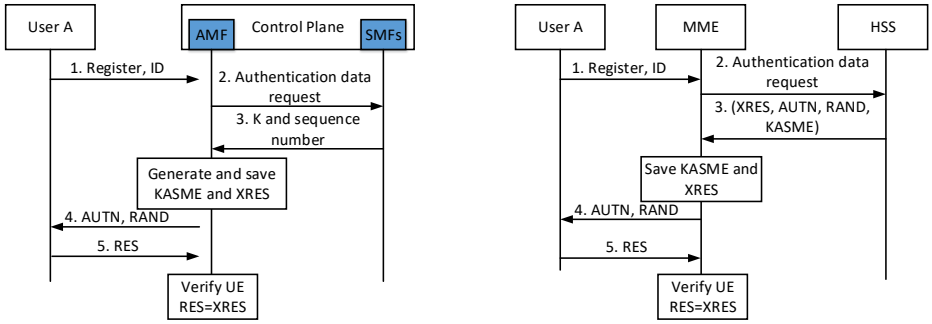
2) Flexible authentication: As discussed in the previous section, in the legacy cellular networks, mutual authentication is applied between a user and the network. However, the authentication between a user and the services provider is not implemented by the network. In 5G wireless network systems, some use cases may require both the service provider and network provider to carry out authentication with the users. In the legacy cellular networks, for 3GPP access, the AKA is applied between a user equipment and a mobile management entity. For non-3GPP access, AKA is applied between a user equipment and an authentication authorization and accounting (AAA) server. Full authentication is required once a user changes its access technology. Based on our proposed security architecture, AMF can handle the authentication independent of the access technologies. In other words, a full authentication is not required when a user changes its access technology. Moreover, based on PCF, AMF can perform different authentication schemes for different service requirements.

Flexible authentication is required in 5G wireless networks to ensure the security while satisfying the quality of services requirements. The input and output of the authentication mechanism selection are shown in Fig. 18. The input information can be included in PCF, which can control AMF to perform the authentication procedure.

D. Handover Procedure and Signaling Load Analysis

In this subsection, analysis on handover procedure and signaling load are presented based on the proposed security architecture for a HetNet with different access technologies including 5G new radio, 3GPP access and Non-3GPP access. The system model is shown in Fig. 19, where a user A currently associates with 3GPP access point MBS. Assume that SBSs have different access technologies compared with MBS. When user A is moving, it may need to connect with a new radio access point (NRAP), in which case handover is needed in the legacy cellular networks. In our proposed security architecture, AMF is independent from different access technologies. User A can connect with the same AMF through different access technologies. The first time user A associates with an access point, a general authentication procedure is needed. Assume that the same authentication scheme is applied to the proposed 5G wireless network security architecture and the legacy security architecture. The authentication of first time access to the network for user A based on different security architectures is shown in Fig. 20. Since AMF and UDM are both in the control plane, the cost for information exchange between AMF and UDM is less than that between different entities such as MME and HSS. Based on the legacy security architecture, the authentication vector is generated at HSS and is then transmitted to MME. However, in our proposed security architecture, authentication vector can be generated at AMF to reduce the overhead of communications and to reduce the risk to expose the KASME and XRES. With the flexibility of network functions, AMF and UDM can be widely distributed to handle the authentication of a massive number of user devices. Nevertheless, due to the coupled control plane and user plane, MME and HSS have limited scalability.

Once user A changes its access point using another access technology in legacy cellular networks, the same authentication as shown in Fig. 20b is needed for each handover, which not only increases latency and communication overhead



a. Based on the proposed 5G security architecture

b. Based on legacy security architecture

Fig. 20: Authentication based on different security architecture

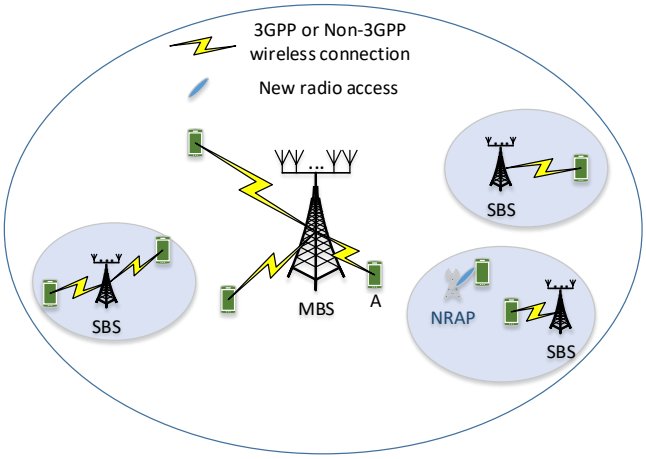


Fig. 19: A two-tier HetNet model

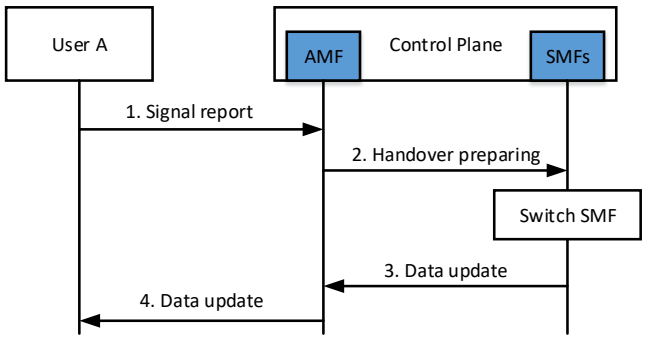


Fig. 21: A handover procedure for access technologies change

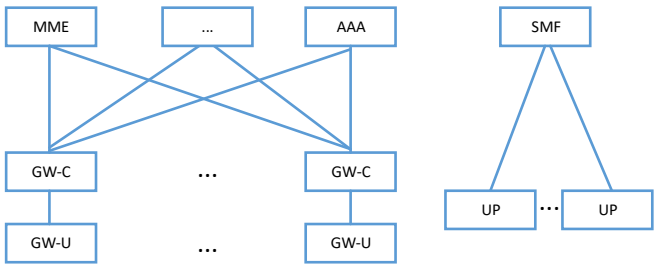


Fig. 22: Signaling architecture comparison of legacy cellular network and 5G cellular network

but also leads to possible connection outage. However, based on the proposed security architecture, no authentication will be needed by switching to different SMF for a new session and a new IP address allocation. The handover based on the proposed 5G wireless security architecture is presented in Fig. 21. The data update from SMF includes the new session key and new IP address from the new access point. The communication latency between AMF and SMF can be neglected compared to the communication latency from MME to HSS. Moreover, the signaling overhead based on the 5G wireless security architecture is much lower because of the separation of control plane and user plane as shown in Fig. 22. To satisfy certain latency requirement, the number of gateway nodes needs to be increased by a factor of 20 to 30 times of the current number [72]. The separation of control and user plane of gateway can also facilitate distributed gateway deployment. Therefore, for the new core network based on control and user plane separation, the signaling load can be significantly reduced.

VI. Challenges and Future Directions for 5G Wireless Security

The challenges and future directions for 5G security research and development are presented in this section. According to the previous sections, part of the security solutions used in 4G will be evolved into 5G. However, with extensive use cases and various integrated technologies applied to 5G, security services in 5G face many challenges in order to address 5G advanced features. Several perspectives of the challenges and corresponding future directions are discussed as follows.

A. New Trust Models

With the advanced services offered by 5G wireless networks, not only new types of functions are provided to people and society, but also new services are applied to vertical industries, such as smart grid, smart home, vehicular networks and m-health networks, etc. In the legacy cellular networks, user terminals, home, and serving networks are considered in

the trust model. The trust models vary among different use cases which can involve new actors in 5G wireless networks [12]. The authentication may need to be implemented between various actors with multiple trust levels.

There have been research work on trust models for different use cases. In [44], the authors proposed a system model to facilitate secure data transmission over 5G wireless networks for vehicular communications. DMV, TA, LEA, and vehicles are included in the proposed system model. The trust model between them is more complex than the trust model in the legacy cellular networks. With the massive number of devices over 5G wireless networks, new trust models are needed to improve the performance of security services such as IoT user cases authentication. However, it lacks a trust model between devices and fusion center in [40]. For some applications, there are various types of devices connected to the same network, some of which may be used only to gather data and some of which may be used only to access internet. The trust requirements of different devices should be different. For different security demands, the corresponding trust model may have different security requirements. As an example, a high security level demand may require both password and biometric authentication simultaneously [15]. In a m-health network, in [45] the authors provided the trust model between client, network management and physician based on the privacy requirements.

In summary, various new trust models for new applications in 5G are needed. These new trust models will affect the security services.

B. New Security Attack Models

Based on the recent research activities on PLS, the most used attack model consists of a single eavesdropper armed with a single antenna. However, the number of eavesdroppers can be high in 5G wireless networks. Moreover, eavesdroppers can be armed with massive MIMO technology [38]. In practical scenarios, there may exist different types of attacks. By only considering one kind attack, the cooperation of jammer or eavesdroppers are not considered in PLS, which can make the security in PHY more complex. Although increasing the transmission power of the sender can fight against jamming attack, it may also increase the risk of eavesdropping attacks.

Moreover, with the new service delivery model applied to SDN and NFV, there are more vulnerable points exposed [9]. Decoupling software from hardware makes the security of software no longer depending on the specific security attributes of the hardware platform [12]. Therefore, the demands on strong isolation for virtualization are ever increasing. Network slicing is introduced in [11] to provide the isolated security. In [36], an effective vulnerability assessment mechanism is proposed for SDN based mobile networks using attack graph algorithm. A comprehensive security attack vector map of SDN is presented.

The various new attack models in 5G wireless networks based on the new technologies and delivery models make the security implementation harder than in the legacy cellular networks. However, there has been limited work on the new security attack models and corresponding solutions.

C. Privacy Protection

With data involved in various new applications in 5G, huge volume of sensitive data are being transmitted through the 5G wireless networks. 5G wireless networks raise serious concerns on privacy leakage due to the open network platforms [15]. The protection of the privacy is an important requirement for implementing different applications. The privacy protection in different use cases can vary based on the security requirements, such as location privacy, identity privacy. For example, in [45], to secure the privacy of patients, the proposed protocol provides security of data access and mutual authentication between patients and physician. The location privacy also draws great attention. In [48], a differential private association algorithm is proposed to secure the location information due to the vulnerable location leakage in HetNets. For vehicular communications, in [44], the privacy protection is considered as protection of the identity of a vehicle and the video contents. In order to offer differentiated quality of privacy protection, the type of service offered to a user needs to be sensed. However, the service type sensing may also have a chance to leak user privacy [15].

The privacy protection is mostly implemented by encryption mechanisms currently. With the massive data, encryption and decryption may violate other service requirements of 5G, such as latency and efficiency. To efficiently protect privacy is a big challenge, especially when facing the powerful data analysis methods such as machine learning. However, data analysis can also be used as a mechanism to help implement the privacy protection intelligently. For example, before the data transmission, data analysis can be applied to find out several highly sensitive dimensions to reduce the encryption cost with privacy protection. For the identity privacy, new identity management should be considered instead of using only device-based identity management. Location privacy can be enhanced if multiple association mechanisms are applied to different use cases. Adding all this together makes it more challenging to provide satisfactory privacy protection in 5G wireless networks.

D. Flexibility and Efficiency

To address different security requirements for different applications and dynamic configurations of the 5G architecture based on virtualization, the security mechanisms must be flexible [12] [15]. The security setup must be customized and optimized to support each specific application instead of an approach fitting all [20]. Therefore, for each security service, different security levels need to be considered for different scenarios. If differentiated security is offered, a flexible security architecture is needed [15]. In our proposed security architecture, network functions in the control plane are various depending on the use cases. AMF and SMF provide flexible security mechanisms based on the requirements of PCF. Therefore, the flexibility is not only required in security architecture but also in security mechanisms.

Besides the flexibility of security architecture and mechanisms, efficiency of security is another key requirement in 5G wireless networks to ensure both the latency requirement and

EE. One of the potential security requirements is to minimize the security-related signaling overhead to ensure the efficiency [20] [73]. The latency can be reduced by reducing the overhead of security load [74]. Since EE and latency performances of 5G wireless networks are expected to be improved compared to the legacy wireless networks, the security efficiency should be ensured to secure the performances of 5G wireless networks. Based on the proposed security architecture, the separation of control plane and user plane and network functions inside the control plane reduce the signaling overhead. For the IoT applications, the nodes normally have limited computation capability and battery power, efficient security mechanisms are required. Moreover, distributed authentication nodes need to support the fast network access for massive number of devices. For the vehicular communications sensitive to latency, lightweight and efficient security solutions are desirable [12][15][45]. Moving the control plane closer to the edge of the core network can also reduce the communication latency. Therefore, to improve the efficiency of 5G wireless networks, both security architecture and security mechanisms need to be improved.

E. Unified Security Management

Although there are different services, access technologies and devices over 5G wireless networks, a security framework with a common and essential set of security features such as access authentication and confidentiality protection is needed [74]. The basic features of these security services may be similar to those in the legacy cellular networks. However, there are many new perspectives of these security features in 5G wireless networks, such as the security management across heterogeneous access and security management for a large number of devices. As we present in the previous section of the new identity management, flexible authentication and the handover between different access technologies based on the proposed security architecture, security management across heterogeneous access need to be defined to offer flexibility for all access technologies. Also, for a large number of devices, such as IoT applications, security management of burst access behavior need to be studied in order to support the efficient access authentication.

VII. Conclusions

5G wireless networks are expected to provide advanced performance to enable many new applications. In this paper, we have presented a comprehensive study on recent development of 5G wireless security. The current security solutions mainly based on the security services provided such as authentication, availability, data confidentiality, key management and privacy have been introduced. Many new security aspects in 5G are expected due to the applications of technologies such as HetNet, D2D, massive MIMO, SDN and IoT. The security involving these technologies have been summarized. Based on these studies, we have proposed a 5G wireless security architecture. The analysis of identity management and flexible authentication based on the proposed security architecture have been presented. A handover procedure and performance have been studied to show the advantage of the proposed security architecture. Finally, we have presented the challenges and future directions of 5G wireless security. We expect that this work could address the security concerns from both industry and academia to provide research directions for implementing security on 5G wireless networks in the near future.

References

[1] N. Panwar, S. Sharma and A. K. Singh, "A Suvery on 5G: The Next Generation of Mobile Communication", *Physical Communication*, vol. 18, no. 2, pp. 64-84, 2016.
[2] "5G Vision", *5G PPP*, February, 2015.
[3] "NGMN 5G WHITE PAPER", *NGMN Alliance*, February, 2015.
[4] J. G. Andrews et al., "What Will 5G Be?", *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065-1082, 2014.
[5] "Understanding 5G: Perspectives on future technological advancements in mobile", *GSMA Intelligence*, December, 2014.
[6] M. Agiwal, A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey", *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617-1655, 2016.
[7] J. Qiao, X. S. Shen, J. W. Mark, Q. Shen, Y. He, and L. Lei, "Enabling Device-to-Device Communications in Millimeter-Wave 5G Cellular Networks", *IEEE Communications Magazine*, vol. 53, no. 1, pp. 209-215, 2015.
[8] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, "Energy Efficiency and Spectrum Efficiency of Multihop Device-to-Device Communications Underlaying Cellular Networks", *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 367-380, 2016.
[9] M. Dabbagn, B. Hu, M. Guizani, and A. Rayes, "Software-Defined Networking Security: Pros and Cons", *IEEE Communications*, vol. 53, no. 6, pp. 73-79, 2015.
[10] J. Zhang, W. Xie, and F. Yang, "An Architecture for 5G Mobile Network based on SDN and NFV", *6th International Conference on Wireless, Mobile and Multi-Media (ICWMMN2015)*, 2015, pp. 87-92.
[11] "5G security recommendations package #2: network slicing", *NGMN Alliance*, April, 2016.
[12] "5G SECURITY", *ERICSSON WHITE PAPER*, June, 2015.
[13] "The Road to 5G: Drivers, Applications, Requirements and Technical Development", *GSA*, November, 2015.
[14] "Leading the world to 5G", *QUALCOMM*, February, 2016.
[15] "5G Security: Forward Thinking Huawei White Paper", *HUAWEI WHITE PAPER*, 2015.
[16] S. Vij, and A. Jain, "5G: Evolution of a secure mobile technology", *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2015, pp. 2192-2196.
[17] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks", *IEEE Journals & Magazine*, vol. 16, no. 1, pp. 283-302, 2014.
[18] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian "SeDS: Secure Data Sharing Strategy for D2D Communications in LTE-Advanced Networks", *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2659-2672, 2016.
[19] M. J. Wang, Z. Yan, and V. Niemi, "UAKA-D2D: Universal Authentication and Key Agreement Protocol in D2D Communications", *Mobile Networks and Applications*, vol. 22, no. 3, pp. 510-525, 2017.
[20] "Security challenges and opportunities for 5G mobile networks", *NOKIA*, 2017.
[21] "5G security recommendations Package #1", *NGMN Alliance*, May, 2016.
[22] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security", *IEEE Security & Privacy*, vol. 14, no. 4, pp. 34-44, 2016.
[23] V. G. Vassilakis, I. D. Moscholios, and B. A. Alzahrani, "On the security of software-defined next-generation cellular networks", *IEICE Information and Communication Technology Forum (ICTF)*, 2016, pp. 61-65.
[24] H. Wang, T. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical Layer Security in Heterogeneous Cellular Networks", *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204-1219, 2016.
[25] Y. Deng, L. Wang, K. K. Wong, A. Nallanathan, M. Elkashlan, and S. Lambotharan, "Safeguarding Massive MIMO Aided HetNets Using Physical Layer Security", *International Conference on Wireless Communications & Signal Processing (WCSP)*, 2015, pp. 1-5.

[26] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security", *Mobile Networks and Applications*, vol. 21, no. 5, pp. 729-743, 2016.

[27] F. Y. Tian, P. Zhang, and Z. Yan, "A Survey on C-RAN Security", *IEEE Access*, 2017. vol. 5, no. , pp. 13372-13386, 2017.

[28] Q. Fang, Z. WeiJie, W. Guojun, and F. Hui, "Unified Security Architecture Research for 5G Wireless System", *2014 11th Web Information System and Application Conference*, 2014, pp. 91-94

[29] P. Schneider, and G. Horn, "Towards 5G Security", *Trustcom/BigDataSE/ISPA*, 2015, pp. 1165-1170.

[30] W. Stallings, "Cryptography and Network Security Principles and Practice Sixth Edition", *PEARSON*, 2014.

[31] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial", *Wireless Communications*, vol. 18, no. 2, pp. 66-74, 2011.

[32] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security", *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515-2534, 2008.

[33] U. Maurer, "Secret key agreement by public discussion from common information", *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733-742, 1993.

[34] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G Wireless Communication Network Using Physical Layer Security", *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20-27, 2015.

[35] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking", *Security and Communication Networks*, vol. 9, no. 16, 2015.

[36] S. Luo, J. Wu, J. Li, L. Guo, and Q. Shi, "Toward Vulnerability Assessment for 5G Mobile Communication Networks", *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, 2015, pp. 72-76.

[37] N. Ulltveit-Moe, V. A. Oleshchuk, and G. M. Kien, "Location-aware mobile intrusion detection with enhanced privacy in a 5G context", *Wireless Personal Communications*, vol. 57, no. 3, pp. 317-338, 2011.

[38] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original Symbol Phase Rotated Secure Transmission Against Powerful Massive MIMO Eavesdropper", *2015 IEEE Access*, vol. 4, pp. 3016-3025, 2016.

[39] N. Adem, B. Hamdaoui, and A. Yavuz, "Pseudorandom Time-Hopping Anti-Jamming Technique for Mobile Cognitive Users", *2015 IEEE Globecom Workshops (GC Wkshps)*, 2015, pp. 1-6.

[40] M. Labib, S. Ha, and W. Saad, and J. H. Reed, "A Colonel Blotto Game for Anti-jamming in the Internet of Things", *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1-6.

[41] W. Baker et al., "Data breach investigations report", *Methodology*, vol. 36, pp. 1-63, 2011.

[42] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle Attacks", *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027-2051, 2016.

[43] X. Duan, and X. Wang. Renzo, "Fast Authentication in 5G HetNet through SDN Enabled Weighted Secure-Context-Information Transfer", *2016 IEEE International Conference on Communications (ICC)*, 2016, pp. 1-6.

[44] M. H. Eiza, W. Ni, and Q. Shi, "Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G Enabled Vehicular Networks", *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 7868-7881, 2016.

[45] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and Robust Security-Aware D2D-assist Data Transmission Protocol for Mobile-Health Systems", *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 662-675, 2017.

[46] E. Dubrova, M. Naslund, and G. Selander, "CRC-Based Message Authentication for 5G Mobile Technology", *IEEE Trustcom/BigDataSE/ISPA*, 2015, pp. 1186-1191.

[47] W. Trappe, "The challenges facing physical layer security", *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16-20, 2015.

[48] S. Farhang, Y. Hayel, and Q. Zhu, "PHY-Layer Location Privacy Privacy-Preserving Access Point Selection Mechanism in Next-Generation Wireless Networks", *2015 IEEE Conference on Communications and Network Security (CNS)*, 2015, pp. 263-271.

[49] E. A. Elrahman, H. L. Khedher, and H. Afifi, "D2D Group Communications Security", *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, pp. 1-6, 2015.

[50] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications", *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 998-1010, 2012.

[51] "An analysis of the security needs of the 5G market", *SIMalliance*, 2016.

[52] Y. Wang, Z. Miao, and L. Jiao, "Safeguarding the Ultra-dense Networks with the Aid of Physical Layer Security", *IEEE Access*, vol. 4, pp. 9082-9092, 2016.

[53] A. Zappone, P. H. Lin, and E. Jorswieck, "Artificial-noise-assisted energy-efficient secure transmission in 5G with imperfect CSIT and antenna correlation", *IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2016, pp. 1-5.

[54] I. Abualhaol, and S. Muegge, "Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns", *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 5763-5771.

[55] K. Fan, Y. Gong, Z. Du, H. Li, and Y. Yang, "RFID Secure Application Revocation for IoT in 5G", *IEEE Trustcom/BigDataSE/ISPA*, 2015, pp. 175-181.

[56] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications", *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589-3603, 2010.

[57] Y. Li, B. Kaur, and B. Andersen, "Denial of service prevention for 5G", *Wireless Personal Communications*, vol. 57, no. 3, pp. 365-376, 2011.

[58] S. A. M. Ghanem, and M. Ara, "Secure Communications with D2D cooperation", *Communications, Signal Processing, and their Applications (ICCSPA)*, 2015 International Conference on, 2015, pp. 1204-1219.

[59] Y. Luo, L. Cui, Y. Yang, and B. Gao, "Power control and channel access for physical-layer security of D2D underlay communication", *International Conference on Wireless Communications & Signal Processing (WCSP)*, 2015, pp. 1-5.

[60] N. I. Bernardo, and F. De Leon, "On the trade-off between physical layer security and energy efficiency of massive MIMO with small cells", *International Conference on Advanced Technologies for Communications (ATC)*, 2016, pp. 135-140.

[61] N. P. Nguyen, T. Q. Duong, H. Q. Ngo, Z. H. Velkov, and L. Shu, "Secure 5G Wireless Communications: A Joint Relay Selection and Wireless Power Transfer Approach", *IEEE Access*, vol. 4, pp. 3349-3359, 2016.

[62] C. Zhang, J. Ge, J. Li, F. Gong, and H. Ding, "Complexity-Aware Relay Selection for 5G Large-Scale Secure Two-Way Relay Systems", *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5461-5465, 2017.

[63] Q. Xu, P. Ren, H. Song, and Q. Du, "Security Enhancement for IoT Communications Exposed to Eavesdroppers With Uncertain Locations", *IEEE Access*, vol. 4, pp. 2840-2853, 2016.

[64] Y. Ju, H. M. Wang, T. X. Zheng, and Q. Yin, "Secure transmission with artificial noise in millimeter wave systems", *IEEE Wireless Communications and Networking Conference*, 2016, pp. 1-6.

[65] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical Layer Security for 5G Non-orthogonal Multiple Access in Large-scale Networks", *2016 IEEE International Conference on Communications (ICC)*, 2016, pp. 1-6.

[66] M. Xu, X. Tao, F. Yang, and H. Wu, "Enhancing secured coverage with CoMP transmission in heterogeneous cellular networks", *IEEE Communications Letters*, vol. 20, no. 11, pp. 2272-2275, 2016.

[67] R. Sedidi, and A. Kumar, "Key Exchange Protocols for Secure Device-to-Device (D2D) Communication in 5G", *2016 Wireless Days (WD)*, 2016, pp. 1-6.

[68] K. Gai, M. Qiu, L. Tao, and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G", *Security and Communication Networks*, vol. 9, no. 16, pp. 3049-3058, 2016.

[69] M. J. Wang, Z. Yan "A Survey on Security in D2D Communications",*Mobile Networks and Applications*, vol. 22, no. 2, pp. 195-208, 2017.

[70] C. Kolias et al., "OpenFlow-Enabled Mobile and Wireless Networks", *Open Networking Foundation*, 2013

[71] $http://www.3gpp.org/news-events/3gpp-news/1786-5g_reqs_sa1$

[72] "5G network architecture - a high-level perspective", *HUAWEI WHITE PAPER*, July, 2016.

[73] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727-1765, 2016.

[74] "5G scenarios and security design", *HUAWEI*, 2016.

Dongfeng Fang received her B.S. degree in Control Theory and Control Engineering from Harbin Institute of Technology, China, in 2009 and her M.S degree in Control Theory and Control Engineering from Shanghai University, China, in 2013. She is a Ph.D. student in Department of Electrical & Computer Engineering, University of Nebraska-Lincoln, USA. Her current research interests include energy efficient and green networks, big data, cloud computing and network security.

Yi Qian is a professor in the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln (UNL). Prior to joining UNL, he worked in the telecommunications industry, academia, and the government. Some of his previous professional positions include serving as a senior member of scientific staff and a technical advisor at Nortel Networks, a senior systems engineer and a technical advisor at several start-up companies, an assistant professor at University of Puerto Rico at Mayaguez, and a senior researcher at National Institute of Standards and Technology. His research interests include information assurance and network security, network design, network modeling, simulation and performance analysis for next generation wireless networks, wireless ad-hoc and sensor networks, vehicular networks, smart grid communication networks, broadband satellite networks, optical networks, high-speed networks and the Internet. Prof. Yi Qian is a member of ACM and a senior member of IEEE. He was the Chair of IEEE Communications Society Technical Committee for Communications and Information Security from January 1, 2014 to December 31, 2015. He is a Distinguished Lecturer for IEEE Vehicular Technology Society. He is serving on the editorial boards for several international journals and magazines, including serving as the Associate Editor-in-Chief for IEEE Wireless Communications Magazine. He is the Technical Program Chair for IEEE International Conference on Communications (ICC) 2018.

Rose Qingyang Hu received B.S. degree from University of Science and Technology of China, M.S. degree from New York University, and Ph.D. degree from the University of Kansas. Currently she is a full professor with the Department of Electrical and Computer Engineering at Utah State University. She also has more than 10 years of R&D experience with Nortel, Blackberry and Intel as a technical manager, a senior research scientist, and a senior wireless system architect. Her current research interests include next-generation wireless communications, wireless network design and optimization, green radios, IoT, cyber-physical systems, wireless system modeling and performance analysis. She has published extensively and holds numerous patents in her research areas. Prof. Hu is an IEEE Communications Society Distinguished Lecturer class 2015-2018 and received the best paper awards from IEEE Globecom 2012, IEEE ICC 2015, IEEE ICC 2016 and IEEE VTC 2016 spring. Prof. Hu is currently serving on the Editor Boards of IEEE Transactions on Wireless Communications and IEEE Transactions on Vehicular Technology. She is a senior member of IEEE and a member of Phi Kappa Phi and Epsilon Pi Epsilon Honor Societies.