ABSTRACT

As with any new technology, the advent of 5G wireless networks brings about new potential security threats and requirements. This paper examines aspects of security in 5G wireless networks, with some comparison to traditional legacy cellular networks such as 4G. The paper begins with a brief introduction to 5G wireless networks as well as the new requirements of 5G wireless security. The potential attacks and solutions are summarised, with consideration of new service requirements and use cases in 5G. The paper would also examine some challenges in 5G security implementation and future research directions in the area.

I. INTRODUCTION

5th generation wireless systems, or 5G, are the next generation mobile wireless telecommunications after the current 4G systems. 5G brings many new service capabilities and seeks to fulfil the following characteristics: increased capacity over 4G, higher density of mobile broadband users, and supporting device-to-device (D2D) communications and massive machine-type communications. 5G planning also aims for lower latency and lower energy consumption, for better implementation of Internet of Things (IoT). However, the standardization process for 5G wireless systems is still in relative infancy.

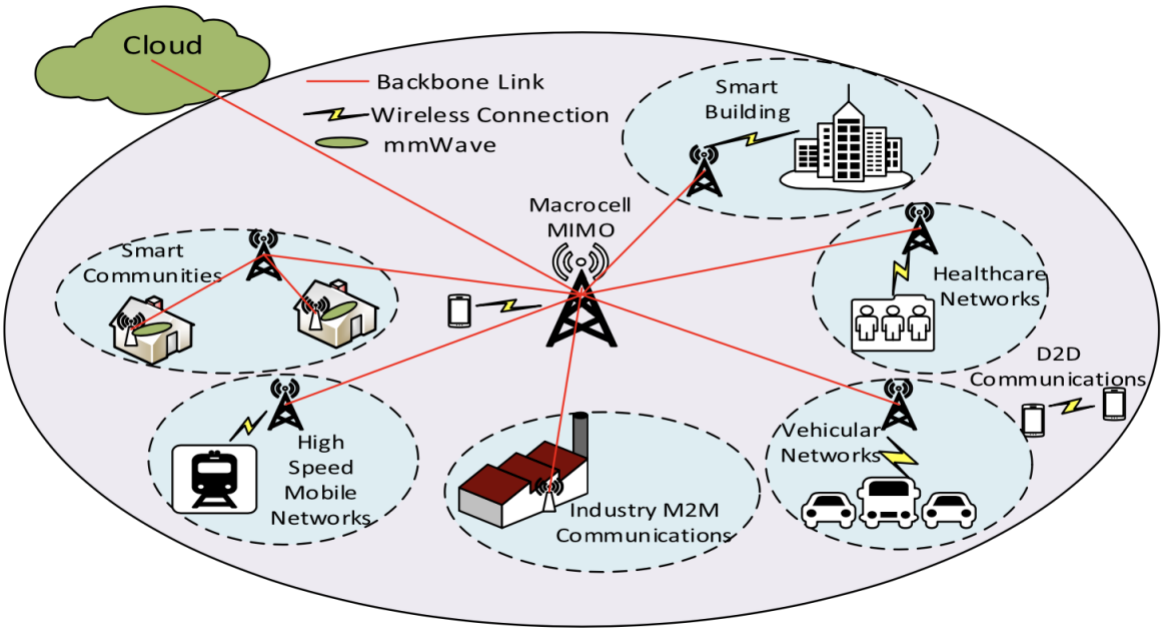

FIGURE 1. A generic architecture for 5G wireless systems.

Figure 1 illustrates a generic architecture of 5G wireless systems. 5G wireless systems can provide not only traditional voice and data communications, but also other new use cases, new industry applications, and a multitude of devices and applications to connect society at large. 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. However, the new architecture, technologies, and use cases in 5G wireless systems may bring new challenges to security and privacy protection.

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. Currently, there are various security issues in cellular networks at media

access control (MAC) layer and physical layer (PHY) in terms of possible attacks, vulnerabilities and privacy concerns [1]. Security protections for 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 the 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 [2]. Besides encryption of user traffic, mutual authentication is achieved between a UE and a base station. In addition, the security of the access management and mobility management of LTE are ensured by a key hierarchy and handover key management mechanism [3]. However, for 5G, new security requirements are needed to support a variety of new use cases and the new networking paradigms. The security mechanisms have to comply with the overall 5G advanced features such as low latency and high energy efficiency (EE). Some security requirements of 5G wireless networks are shown in Table 1:

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

TABLE 1. Security requirements for 5G wireless networks

Moreover, unlike the legacy cellular networks, 5G wireless networks are going to be service-oriented which places a special emphasis on security and privacy requirements from the perspective of services.

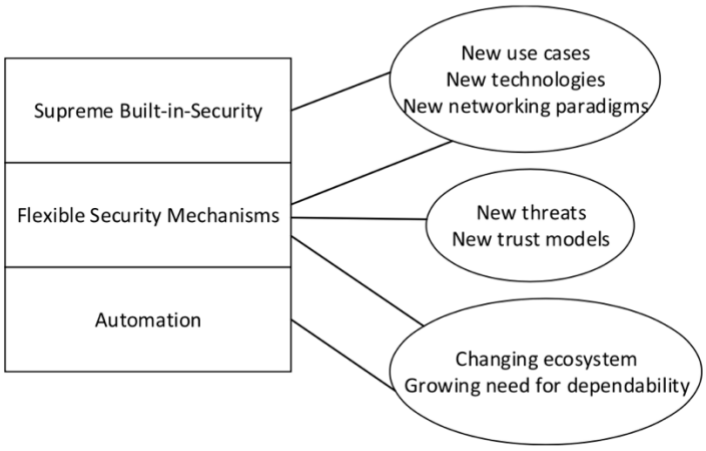

FIGURE 2. Major drives for 5G wireless security

Fig. 2 illustrates the major drives for 5G wireless security. The new use cases can have a variety of specific requirements such as ultra-low latency in the user communications. To address these issues, security should be considered as an integral part of the overall architecture and be integrated into the system design at the very beginning. Also, to support various use cases and new trust models optimally, flexible security mechanisms are needed.

The trust models of the legacy cellular networks and 5G wireless networks are presented in Fig. 3.

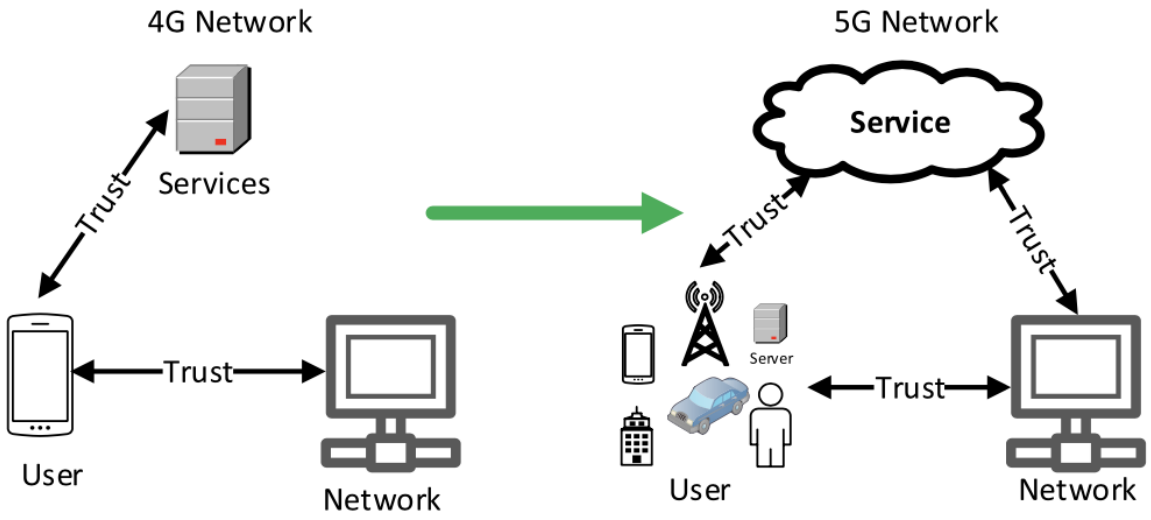

FIGURE 3: Trust model of 4G and 5G wireless networks

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. For industrial use cases, the security demands can vary significantly between different applications. For example, 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. Also, the authentication management in 5G is more complex due to various types of and quantity of devices connected. In Fig. 3, user authentication can be done by the network provider, or by the service provider, or by both.

Security attacks can be classified into two types: passive attacks and active attacks. 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 involve two kinds, 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. These can violate data integrity or availability of services. Typical active attacks include man-in-the-middle attack (MITM), denial of service (DoS) attack, and distributed denial of service (DDoS) attack.

The solutions or services used to tackle security attacks can be mainly classified under two categories: cryptographic approaches with new networking protocols and physical layer security (PLS) approaches.

The cryptographic techniques are the most commonly used security mechanisms, typically deployed at the upper layers of the 5G wireless networks with new networking protocols. Modern cryptography consists of symmetric-key cryptography and public key (or asymmetric) 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 involves a public-private key pair, with the public key for encryption and the private / secret key for decryption. The performance of a cryptographic algorithm depends on the key length and its computational complexity. In traditional cellular networks, the management and distribution of the symmetric keys are well protected. However, due to more complex protocols and heterogeneous

network architectures in 5G, the management and distribution of symmetric keys may encounter new challenges.

Unlike cryptography, physical layer security (PLS) approaches are currently not as prevalent, although there has been extensive PLS research conducted recently in 5G wireless systems. PLS is identified as a promising security strategy to provide secure wireless transmissions by exploiting the unique wireless physical layer medium features. Compared to cryptography, PLS has 2 advantages: low computational complexity and high scalability. These make PLS an ideal candidate technique for cryptographic key distribution in 5G wireless networks. For more information on PLS techniques, one can refer to [4].

Apart from PLS and cryptography, there has been some research done on security architecture [5], vulnerability assessment mechanisms [6], and intrusion detection mechanisms based on data analysis [7].

II. ATTACKS AND SECURITY SERVICES IN 5G WIRELESS NETWORKS

Under the attacks section, four types of attacks are discussed: eavesdropping and traffic analysis, jamming, DoS and DDoS, and MITM, in 5G wireless networks. Subsequently, security services in 5G networks are introduced that cover these 4 aspects of security: authentication, confidentiality, availability, and integrity.

A. ATTACKS IN 5G WIRELESS NETWORKS

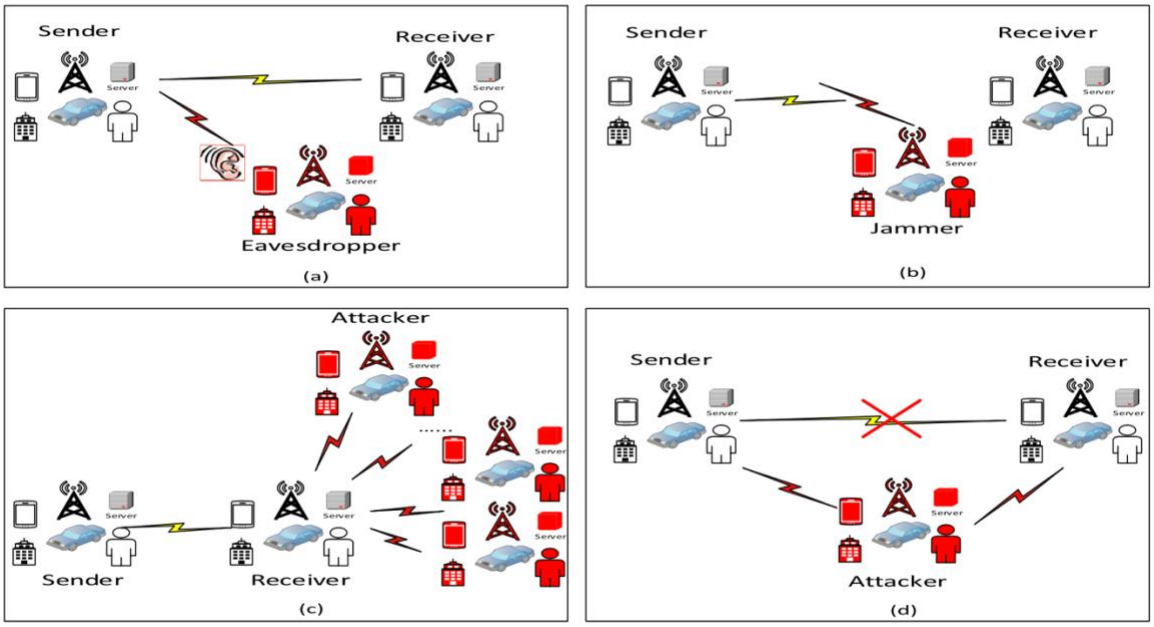

FIGURE 4. Attacks in 5G wireless networks: (a) Eavesdropping; (b) Jamming; (c) DDoS; (d) MITM

Fig. 4 illustrates all four attacks, which will be examined based on attack type (passive or active) as well as solutions to react to / prevent this attack. Here, the focus is on security attacks at the physical and MAC layer, where the key differences on security between wireless and wire-line networks occur.

1) Eavesdropping and Traffic Analysis

As the name suggests, 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. 4a. 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 cannot intercept the received signal directly due to the encryption. Traffic analysis is another passive attack that an attacker can use to intercept information such as location and identity of the communication parties by analysing the traffic of the received signal, without understanding the content of the signal itself. As such, even if the signal is encrypted, traffic analysis can still be used to reveal the patterns of the communication parties. Traffic analysis does not impact legitimate communications either.

The effectiveness of the 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. Given the increasingly powerful computers that adversaries can utilise, existing mechanisms to tackle eavesdropping face a big challenge as many of them assume a small number of simultaneous eavesdroppers with low computing and data analysis capability. Furthermore, the new characteristics of 5G networks may lead to many more complicated scenarios involving potential eavesdroppers, for example, eavesdroppers with multiple antennas are considered. Also, 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 garnered increasing attention.

2) Jamming

Unlike eavesdropping and traffic analysis, jamming can completely disrupt the communications between legitimate users. Fig. 4b 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 such 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 secure communication methods 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 [8], a pseudorandom time hopping anti-jamming scheme is proposed for users to improve the performance compared to FHSS.

3) DoS and DDoS

An attacker can use DoS attacks to exhaust network resources. DoS affects network availability, and jamming can be used to launch a DoS attack. DDoS occurs when more than one distributed adversary exists, for example in a botnet attack where multiple devices have been compromised. Fig. 4c shows a DDoS model. DoS and DDoS are both active attacks that can be applied at different layers. As it is envisioned that 5G will support billions of machine-to-machine/IoT devices with limited computational and patching capabilities, in much greater quantity than legacy cellular networks, DoS and DDoS will likely become a serious threat for operators [9]. Many of these IoT devices

serve as potential targets for botnet malware, especially those unpatched devices or those without security defence systems due to limited computational capabilities and storage space.

4) Man-in-the-middle (MITM)

In a MITM attack, the attacker secretly takes control of the communication channel between two legitimate parties. The MITM attacker can intercept, view, and modify the communication messages between the two legitimate parties. Fig. 4d 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. In legacy cellular networks, rogue base station based MITM is an attack whereby the attacker forces a legitimate user to create a connection with a fake base transceiver station. Mutual authentication between the mobile device and the base station is normally used to prevent rogue base station based MITM.

B. SECURITY SERVICES IN 5G WIRELESS NETWORKS

With the new architecture, technologies, and use cases in 5G networks, there are also 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 types of authentications: entity authentication and message authentication. Entity authentication is used to ensure the communicating entity is the one that it claims to be. In legacy cellular networks, mutual authentication between user equipment (UE) and mobility management entity (MME) is implemented before the two parties communicate with each other. The mutual authentication between UE and MME is the most important security feature in the traditional cellular security framework. In addition, in 4G LTE cellular networks, the authentication and key agreement (AKA) 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, authentication by service provider, and authentication by both network and service provider. 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 [10], 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. For message authentication, in [11], 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 limits data access to authorised users only, while 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 sender / receiver location. With various applications in 5G, there exists massive data related to user privacy, e.g., vehicle routing data, health monitoring data.

Data encryption has been widely used to maintain data confidentiality by preventing unauthorized users without the key from decrypting the data. Symmetric key encryption can be used, but 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, such as quantum computing. Rather than relying solely upon generic higher-layer cryptographic mechanisms, PLS can support confidentiality service [12], against jamming and eavesdropping attacks. Besides the data encryption services in 5G, privacy protection service also matters to some users. Privacy in 5G deserves much more attention than in the legacy cellular networks due to the massive number of data connections. Anonymity

service is a basic security requirement in many use cases, especially those involving sensitive data, such as personal health information and vehicle routing data (which can expose user location). In [13], cryptographic mechanisms and schemes are proposed to provide secure and privacy-aware real-time video reporting service in vehicular networks. Privacy will be discussed in more detail in a later section.

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 is a key performance metric in 5G. Jamming or interference can disrupt the communication links between legitimate users by interfering with radio signals. With many unsecured IoT devices that could be compromised as part of a botnet, 5G wireless networks face a big challenge in preventing such DDoS attacks to ensure service availability. For availability at the physical layer, DSSS and FHSS are two classical PLS solutions. 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. Adem et al. [8] 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.

4) Integrity

Although message authentication corroborates the message source, 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 critical applications such as metering for the quality of the drinking water and scheduling of the transportation. In these cases, data integrity would be a key security requirement.

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. Integrity services can be provided by using mutual authentication, which can generate an integrity key to certify its integrity.

SECTION III: Challenges and Future Directions for 5G Wireless Security

Some of the security solutions in 4G will be adapted into 5G. However, with extensive use cases and various integrated technologies in 5G, security services in 5G face many challenges in addressing 5G advanced features. Some challenges and corresponding future research directions are discussed below:

A. New Trust Models

5G brings about new applications in various industries, such as smart grid, smart home, vehicular networks and mobile health networks. In the legacy cellular networks, only the

user terminals, home, and serving networks are considered in the trust model for entity authentication. However, in 5G, the varying use cases involving new actors would require new trust models. These actors can also have multiple trust levels, further complicating the model.

There has been research work on trust models for different use cases. Eiza *et al.* [13] proposed a system model to facilitate secure data transmission over 5G wireless networks for vehicular communications. 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 authentication. For applications like IoT, 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 the internet. For these, the trust requirements of different devices should be different. In a mobile health network, Zhang *et al.* [14] provided a trust model between client, network management and physician based on the privacy requirements.

B. New Security Attack Models

Based on 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. Eavesdroppers can also be armed with multiple input, multiple output (MIMO) antenna technology [15]. In actual 5G scenarios, there may exist different types of attacks, possibly involving multiple

cooperating jammers or eavesdroppers, which are not considered in PLS and could further complicate PHY security.

Other various new attack models in 5G wireless networks based on the new technologies and delivery methods could make security implementation more challenging as compared to legacy cellular networks. However, there has been limited work on new security attack models and corresponding solutions.

C. Privacy Protection

With data involved in various new applications in 5G, huge volumes of sensitive data are being transmitted through 5G networks. 5G networks raise potential concerns on privacy leakage due to the open nature of the network platforms. For example, in [14], 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. For vehicular communications, the privacy protection can be considered as protection of the identity of a vehicle and the video contents.

The privacy protection is mostly implemented by encryption mechanisms currently. But with the massive data throughput, 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 powerful data analysis methods such as machine learning. However, data analysis can also be used as a mechanism to help implement privacy protection intelligently. For example, before data transmission, data analysis can

be applied to find out the highly sensitive dimensions, such that only those need to be encrypted, to reduce the encryption cost for privacy protection. For identity privacy, new identity management models should be considered instead of using only device-based identity management. Adding all this together makes it more challenging to provide satisfactory privacy protection in 5G wireless networks.

SECTION VI: Conclusion

5G wireless networks are expected to provide advanced performance whilst enabling many new applications. However, with any new technology comes new security threats and requirements. Also, with more devices also expected to be connected and more potentially sensitive data passing through, security in 5G should not be neglected.

3418 words (excluding abstract)

References:

[1] S. Vij and A. Jain, ‘‘5G: Evolution of a secure mobile technology,’’ in Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom), Mar. 2015, pp. 2192–2196.

[2] ‘‘5G security,’’ Ericsson, Stockholm, Sweden, White Paper, Jun. 2015.

[3] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, ‘‘A survey on security aspects for LTE and LTE-A networks,’’ IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 283–302, 1st Quart., 2014.

[4] 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,’’ IEEE Wireless Commun., vol. 18, no. 2, pp. 66–74, Apr. 2011.

[5] Z. Yan, P. Zhang, and A. V. Vasilakos, ‘‘A security and trust framework for virtualized networks and software-defined networking,’’ Secur. Commun. Netw., vol. 9, no. 16, pp. 3059–3069, 2015.

[6] S. Luo, J. Wu, J. Li, L. Guo, and Q. Shi, ‘‘Toward vulnerability assessment for 5G mobile communication networks,’’ in Proc. IEEE Int. Conf. Smart City/SocialCom/SustainCom (SmartCity), Dec. 2015, pp. 72–76.

[7] N. Ulltveit-Moe, V. A. Oleshchuk, and G. M. Køien, ‘‘Location-aware mobile intrusion detection with enhanced privacy in a 5G context,’’ Wireless Pers. Commun., vol. 57, no. 3, pp. 317–338, 2011.

[8] N. Adem, B. Hamdaoui, and A. Yavuz, ‘‘Pseudorandom time-hopping anti- jamming technique for mobile cognitive users,’’ in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2015, pp. 1–6.

[9] 5G Security Recommendations Package #1, NGMN Alliance, Glasgow, U.K., May 2016.

[10] X. Duan and X. Wang, ‘‘Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer,’’ in Proc. IEEE Int. Conf. Commun. (ICC), May 2016, pp. 1–6.

[11] E. Dubrova, M. Näslund, and G. Selander, ‘‘CRC-based message authentication for 5G mobile technology,’’ in Proc. IEEE Trust- com/BigDataSE/ISPA, Aug. 2015, pp. 1186–1191

[12] W. Trappe, ‘‘The challenges facing physical layer security,’’ IEEE Commun. Mag., vol. 53, no. 6, pp. 16–20, Jun. 2015.

[13] M. H. Eiza, W. Ni, and Q. Shi, ‘‘Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks,’’ IEEE Trans. Veh. Technol., vol. 65, no. 10, pp. 7868–7881, Oct. 2016.

[14] 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 Trans. Inf. Forensics Security, vol. 12, no. 3, pp. 662–675, Mar. 2017.

[15] 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,’’ IEEE Access, vol. 4, pp. 3016–3025, 2016.