Is 5G Handover Secure and Private? A Survey

Dongsheng Zhao, Zheng Yan, *Senior Member, IEEE,* Mingjun Wang, Peng Zhang, and Bin Song, *Senior Member, IEEE*

***Abstract*—The next generation mobile cellular communication and networking system (5G) is highly flexible and heterogeneous. It integrates different types of networks, such as 4G legacy networks, Internet of Things (IoT), Vehicular Ad-hoc Network (VANET) and Wireless Local Access Network (WLAN) to form a heterogeneous network. This easily results in continual vertical handovers between different networks. On the other hand, substantial deployment of small/micro Base Stations (BSs) brings frequent horizontal handovers within a network. The continual handovers among BSs and various networks expose Mobile Equipment (ME) to risk of security and privacy threats. So far, many security and privacy mechanisms have been proposed to ensure secure handover either vertically or horizontally in 5G networks. Nevertheless, there still lacks a thorough survey to summarize recent advances and explore open issues although handover security and privacy are crucial to 5G. In this paper, we summarize security and privacy requirements in handovers to resist potential attacks. Following these requirements as evaluation criteria, we review secure and privacy-preserving handover schemes by categorizing them into two scenarios, i.e. vertical handover and horizontal handover. As for vertical handover, we review related work from three classes, i.e., handovers within Third Generation Partnership Project (3GPP) networks, between 3GPP and non-3GPP networks, and between non-3GPP networks. Concerning horizontal handovers, we review related work from two classes, i.e., intra-Mobile Service Controller (MSC) and inter-MSC handover. Meanwhile, we analyze and compare the technical means and performance of these works in order to uncover open issues and inspire future research directions.**

***Index Terms*—Handover, HetNets, 5G Networks, Security, Privacy Preservation.**

I. Introduction

With the continuous increase of data and devices in wireless networks, existing wireless networks have been facing difficulty to withstand increasing traffic load. Consequently, the next generation of mobile cellular communication and networking system (5G) has emerged to meet these intense demands via innovative technologies, e.g., Network Function Virtualization (NFV), Software-Defined Network (SDN) [1], Device-to-Device (D2D) communications [2], and edge computing [3]. International Telecommunication Union (ITU) defined three application scenarios for 5G, named Enhanced Mobile Broadband (eMBB), Massive Machine-Type Communications (mMTC) and Ultra-reliable and Low Latency Communications (URLLC) [4]. Enhanced Mobile Broadband brings 100 times higher data rates than that of 4G that can reach 10 gigabits per second. Massive Type Communications require a Base Station (BS) to manage an enormous number of devices that are designed for Internet of Things (IoT) in general. And Ultra-reliable and Low Latency Communications guarantee high bandwidth and low delay in some critical-reliability scenarios like Vehicle-to-Everything (V2X) [5] and critical machine communications.

5G is highly flexible and heterogeneous with numerous communication networks involved, for instance, New Radio (NR), Long Term Evolution (LTE), IoT, Vehicular Ad-hoc Network (VANET), Wireless Local Area Networks (WLAN), and several types of Wi-Fi [1]. These networks have different Radio Access Technologies (RAT), e.g., Evolved Universal Terrestrial Radio Access (E-UTRA), World Interoperability for Microwave Access (WiMAX), and the WLAN 802.11 family of standards [6]. On the other hand, due to the low penetrability of high-frequency signals adopted in 5G, networks consist of a large number of small Access Points (AP) to provide high data access rates and available network bandwidth. The continuous network densification and increasing heterogeneity pose challenges in terms of Mobile Equipment (ME) mobility support.

Mobile handover technology, as a cornerstone for mobile network service continuity, supports ME to seamlessly move among different Base Stations (BSs) or APs equipped with multifarious access technologies. In 5G networks, diversity of service networks increases the complexity of handover among different RATs, which lengthens the handover time and thus influences user experiences of 5G network. On the other hand, high-density access networks result in high handover frequency of ME among small BSs/APs compared with 3G/4G networks. According to the research of Talukdar et al. [7], the deployment of small APs brings frequent horizontal handovers in the cellular network.

Meanwhile, frequent handovers between small cells and Heterogeneous Networks (HetNets) cause multifarious poten-

D.S. Zhao is with the State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an, 710071, China (e-mail: mjhzds@163.com).

Z. Yan is with the State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an, 710071, China and the Department of Communications and Networking, Aalto University, Espoo, 02150, Finland (e-mail: zyan@xidian.edu.cn).

M.J. Wang is with the State Key Laboratory on Integrated Services Networks, School of Telecommunications Engineering, Xidian University, Xi'an, 710071, China (e-mail: mjwang@xidian.edu.cn).

P. Zhang is with Zalando, Helsinki, Finland (e-mail: pengzhangzhang@gmail.com).

B. Song is with the State Key Laboratory on Integrated Services Networks, School of Telecommunications Engineering, Xidian University, Xi'an, 710071, China (e-mail: bsong@mail.xidian.edu.cn).

tial threats on access control [8], communication security [9] and privacy [10]. Specifically, when a handover occurs, a lot of control signaling need to be exchanged frequently to guarantee the continuity of service, which brings huge security and privacy risks to both networks and mobile users. It becomes critical to guarantee the security and privacy of the users during their device handovers in 5G networks.

In the past decade, a number of surveys about handover schemes [11]–[17] have been conducted. Table I lists and compares a number of existing surveys related to handover. We compare them from the review scenario, focus point and publication year. [11], [13] and [17] focus on handover efficiency. [12] [15] and [16] focus on handover decision algorithms. [14] focuses on handover tools and architectures. It can be seen that there is no handover survey in recent years.

And we also find that there still lacks a thorough survey that classifies existing works, summarizes recent advances, and explores open issues on security and privacy of handover in 5G networks. To fill this gap, we search for handover schemes from 2008 up to now. Some schemes are not designed for 5G network, but it inspires later articles. In our reference, there are many 4G handover designs because the authors abstract the handover-related entities into logical entities, which can be used in both 4G and 5G scenarios. This paper seriously reviews secure and privacy-preserving handover schemes in 5G networks by 1) categorizing 5G handover into two main types, i.e., vertical handover and horizontal handover; 2) exploring security and privacy threats to 5G handover; 3) analyzing security and privacy requirements to resist potential threats; 4) comparing and analyzing existing works under a set of standardized evaluation criteria.

Following our taxonomy, we review the current literature from two aspects: vertical and horizontal handovers in 5G networks. As for vertical handover, we review the literature by classifying them into three classes, i.e., handovers within Third Generation Partnership Project (3GPP) networks, handovers between 3GPP and non-3GPP networks, and handovers between non-3GPP networks. Concerning horizontal handovers, we review two typical types of handovers, intra-Mobile Service Controller (MSC) and inter-MSC handover. Here, MSC refers to a component that handles access and handover requests. Meanwhile, comparison and analysis of the reviewed schemes are performed based on our explored requirements to assist us in finding out open issues and proposing future research directions.

Specifically, the main contributions of this paper are:

- Our paper is the first work to thoroughly review the current advance of security and privacy in the handover of 5G networks with detailed taxonomy.
- We study more than 100 pieces of literature on the security and privacy of handover in 5G heterogeneous networks and categorize them into two high-level categories, i.e. vertical handover and horizontal handover based on handover mode. For each category, we further divide it into several sub-classes based on handover scenarios to perform refined analysis.
- We analyze the security and privacy threats and propose corresponding requirements of handover in 5G networks to resist the threats.
- We are the first to set the security and privacy requirements for the 5G handover as evaluation criteria. By employing these criteria, we review existing security and privacy countermeasures to analyze their pros and cons.
- We figure out the open issues and propose some research directions based on the above serious literature review and analysis.

TABLE I
COMPARISON OF EXISTING SURVEYS

Existing work	Scenario	Focus points	Published Year
[11]	Vehicular network	Mechanisms that can speed up handover process	2010
[12]	Vehicular network	Handover execution and decision algorithms	2016
[13]	High-speed mobile environment	Efficiency of handover schemes	2014
[14]	Heterogeneous wireless networks	Tools and architectures that support handover	2016
[15]	Heterogeneous wireless networks	Handover decision algorithms based on network context	2015
[16]	Heterogeneous wireless networks	Algorithms used in handover process	2011
[17]	IEEE 802.11 networks	Schemes to reduce handover delay	2007
Our Work	HetNets in 5G	Handover security and privacy preservation	-

The rest of the paper is organized as follows. We first give a brief introduction of handover in 5G networks and classify the handover schemes in Section II. Then, we analyze security and privacy threats and potential attacks in order to specify security and privacy requirements on the handover in 5G networks in Section III, which also summarizes typical techniques for constructing security protection measures. In Section IV and Section V, we respectively review the literature about the security and privacy countermeasures in 5G handover with a detailed taxonomy. In Section VI, open issues and future research directions are discovered and proposed. Finally, we conclude our paper in the last section. Abbreviations used in this paper are listed in Appendix A.

II. HANDOVER IN 5G

In this section, we introduce some basic concepts of handover and classify the handover scenarios in 5G networks.

A. 5G Network Architecture

As shown in Fig. 1, 5G network mainly consists of two parts, named Core Network (CN) and Radio Access Network (RAN). CN mainly contains Access and Mobility Management Function (AMF), User Plane Function (UPF), Session Management Function (SMF), and Authentication Server Function

(AUSF). In RAN, there are g-Node Base Stations (gNB) which communicate with MEs. If a ME wants to connect to the 5G CN, AMF would firstly represent AUSF to perform mutual authentication with the ME.

In addition to NR of 5G and LTE of 4G, the 5G system also supports other non-3GPP access networks via Non-3GPP Interworking Function (N3IWF) and Trusted Non-3GPP Gateway Function (TNGF). WLAN is a typical non-3GPP network and it is widely used in our daily life. To improve network resource utilization, 5G system supports D2D communications. Two devices in close proximity can communicate directly without the involvement of base stations to forward messages. Vehicular network is another important part of the 5G system. Vehicles can connect to Road Side Unit (RSU) to get road information and they also can connect to 5G CN via a 5G wireless access network. The vehicular network is treated as a key technology to realize autonomous driving.

B. Handover in 5G

Handover is extremely important in any mobile network with a distributed access architecture [18]. It is designed to ensure the continuity of network services, for instance, connection maintenance between ME and BS, security and privacy protection, and Quality of Service (QoS) when ME moves from one cell or one radio network to another. In 5G networks, massive BS deployment and continual network heterogeneity are introduced as a cornerstone to confront mobile data traffic explosion. These new technologies arouse serious challenges to handover in 5G networks. For example, handover among multifarious networks calls for highly compatible handover system. On one hand, the deployment of vast small cells makes handover occur frequently. Talukdar et al. [7] simulated that cell shrinking and low penetrability of millimeter-wave make the handover happens every 11.6 seconds. On the other hand, smoothly supporting mobility among networks with different RATs is also a big challenge. Both of the above problems require better handover performance in 5G networks than before.

We illustrate the multifarious handover scenarios in 5G in Fig. 1. Generally, there are six kinds of network entities involved in the handover procedure, i.e., ME, source BS, target BS, source MSC, target MSC, and Authentication Server (AS). All these six entities can be divided into three parts based on their functionalities and deployment locations, namely ME, RAN, and CN. ME represents the equipment that wants to obtain a seamless service from 5G networks. Since the heterogeneity of 5G networks, the MEs could be smartphones, laptops, smart wearable devices, sensors, vehicles, etc. The resources, such as computational resources of these devices are limited, which leads to a high delay in handover. RAN provides a radio access service for ME with various types of BSs, e.g., gNB of 5G, e-Node Base Station (eNB) of LTE, AP of WiMAX, and RSU of VANET. CN in handover mainly involves MSC, (e.g., Mobility Management Entity (MME) in LTE, AMF in 5G) and also AS (e.g., Home Subscriber Server (HSS) in LTE and AUSF in 5G). MSC is responsible for user mobility management and handover authentication. AS stores user information and is responsible for access authentication and service authorization. AS could support authentication for both 3GPP access and non-3GPP access [19].

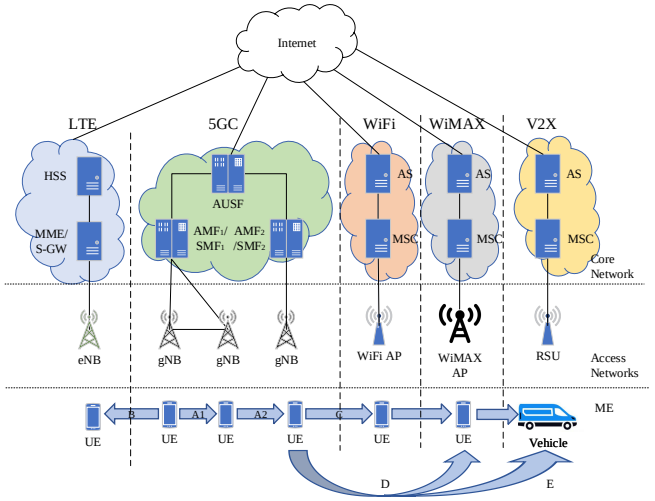


Fig. 1. Handover scenarios in 5G networks

Specifically, in a 5G scenario, when an ME moves from a source gNB to a target gNB or when a source gNB cannot provide better data services or voice services than another gNB, the ME launches handover by sending a handover request to the target gNB in order to guarantee the continuity of communications. Only after subscription service checking and security authentication by the target gNB, AMF and UDM, the ME will be able to connect to the target BS to get a continuous service.

C. Classification of Handover

There are many taxonomies to classify handover [20], for instance, based on the carrier frequency, handover can be classified into inter/intra-frequency handover; based on operator, handover can be classified into inter or intra operator handover. Herein, we classify handover based on radio access technology because RAT is a key feature to differentiate wireless networks, especially the generation of 3GPP networks.

On the basis of RATs involved in a handover procedure, we classify handover of 5G into two main categories: horizontal handover and vertical handover [21]. Horizontal handover occurs when an ME moves among wireless networks with the same RAT. It is also called intra-RAT handover. In this paper, we only consider horizontal handover between NR within 5G networks, i.e., the handover A1 and A2 in Fig. 1. Vertical handover occurs when an ME moves among wireless networks with different RATs. Vertical handover is also known as Inter-RAT handover [22]. We can see from Fig. 1 that the handover B (handover between NR and LTE), handover C (handover between NR and Wi-Fi), the handover D (handover between NR and WiMAX), and the handover E (handover between NR and V2X) belong to vertical handovers.

The horizontal handover can be further divided into sub-categories in light of the level of network control entities involved. For instance, if a handover occurs between two

BSs under control of the same MSC, it is an intra-MSC handover (handover A1 in Fig. 1), otherwise, it is an inter-MSC handover (handover A2 in Fig. 1). In the 5G network, intra-AMF handover is also called Xn-based inter-NG-RAN handover, in which ME handovers from a source BS to a target BS under the same AMF. Herein, Xn is the interface between 5G BSs. Inter-AMF handover is called N2 based inter-NG-RAN handover, where N2 is the interface between 5G BS and AMF located in 5G core network.

On the other hand, the vertical handover can be divided into sub-categories based on the type of RATs. Because RATs introduced by 3GPP account for a large part of mobile networks, we classify RATs into two main groups, i.e., RATs of 3GPP and non-3GPP. As shown in Fig. 2, we further classify vertical handover into three sub-categories based on the RAT involved, i.e., handover within 3GPP networks, handover between 3GPP and non-3GPP networks, and handover between non-3GPP networks. Since the evolution of 3GPP networks, there currently exist three generations of 3GPP networks, i.e., 3G, LTE, and 5G networks. However, with the widespread deployment of the 5G, the 3G network is quitting. So, in this survey, we only take LTE and 5G networks into consideration. Thus, the handover within 3GPP networks can be specified as handover between NR and LTE, which is shown as the handover B in Fig. 1. As for the handover between 3GPP and non-3GPP networks, 3GPP defines two scenarios, i.e., handover from a 3GPP network to an untrusted non-3GPP network and handover from an untrusted non-3GPP network to a 3GPP network. The handover C, D, E which are shown in Fig. 1 belong to the handover between 3GPP and non-3GPP networks. In this paper, we do not discuss the handover between non-3GPP networks since it is not the mainstream handover technique.

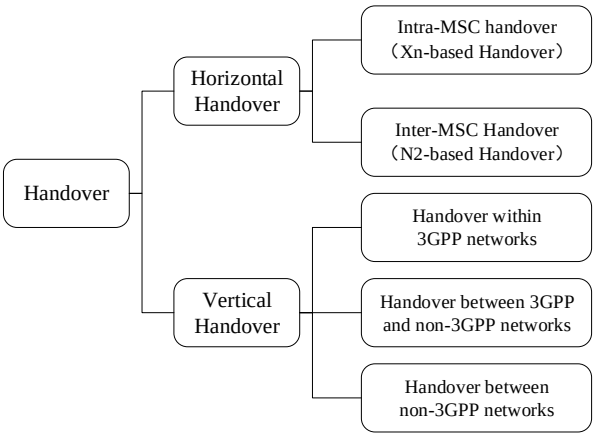


Fig. 2. Handover classification

III. Security and Privacy of Handover in 5G Networks

In this section, we first introduce the 5G security architecture. Then, we analyze the security and privacy threats and attacks encountered in the handover in 5G networks. For counter measuring potential attacks and threats, we specify the security and privacy requirements of the 5G handover, as depicted in Fig. 3. Finally, we list a set of common security techniques used to construct security and privacy protection measures.

A. 5G Security Architecture

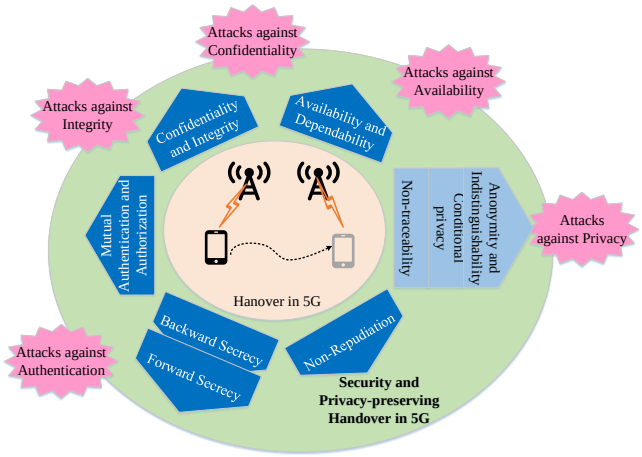


Fig. 3. Security and privacy requirements of handover to countermeasure potential attacks

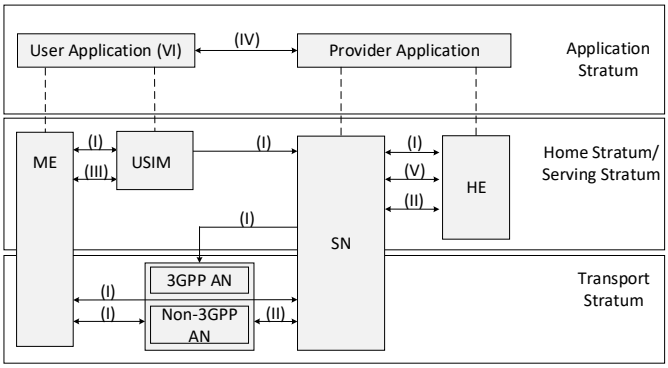


Fig. 4. 5G Security Architecture

3GPP standard [23] has introduced six security domains in 5G network as depicted in Fig. 4.

- Network access security (I): It refers to a set of security features that enable a ME to authenticate and access services securely via an Access Network (AN), and to protect AN against attacks. In addition, it includes security context delivery from a Serving Network (SN) to the AN.
- Network domain security (II): It refers to a set of security features that enable network entities to securely exchange data.
- User domain security (III): It refers to a set of security features that ensure secure user access to mobile equipment.
- Application domain security (IV): It includes a set of security features that enable applications in a user domain and in a provider domain to communicate securely.

- Service-Based Architecture (SBA) domain security (V): It contains a set of security features about SBA that enables network functions of the SBA to securely communicate with each other.
- Visibility and configurability of security (VI): It refers to a set of features that inform the user whether a security feature is guaranteed.

B. Security Threats in Handover

1) Threats in 3GPP Architecture: Although 5G has a great improvement in the security aspect, i.e. authentication method 5G-AKA, EPS-AKA', the key derivation function in mobility still suffers from potential attacks. Cao et al. [24] conducted a detailed survey about the security aspects of the 5G network and pointed out some weaknesses of X1 and N1 based handover. One threat is that the handover in the 5G network cannot ensure backward secrecy, which means that an adversary can compute subsequent handover session keys if it gets a session key between ME and gNB. Moreover, 5G handover is also vulnerable to replay attacks, which can destroy the establishment of a secure link between ME and a targeted message.

Recently, Khan et al. [25] proposed a downgrade attack against 5G ME, which can catch ME's International Mobile Subscriber Identity (IMSI) which is a global identity of ME. Hussain et al. [26] came up with an attack named ToRPEDO that can enable an adversary to verify a victim's coarse-grained location information, inject fabricated paging messages, and initiate DoS attacks. Moreover, they extended their study and found a flaw of several network providers that enables an adversary to launch an attack named PIERCER. This attack can attach a user's phone number to the IMSI of the user's ME, subsequently making it possible to trace the target user. Park et al. [27] found that LTE architecture is more vulnerable to IP address spoofing, Denial of Service (DoS) attack and spam emails compared with a traditional closed environment (e.g., Public Switched Telephone Network). Wu and Gong [28] found an adversary can forge the Message Authentication Code to threat integrity protection on LTE handover messages.

Owing to the IP-based structure, the 3GPP standard provides communications between different access networks. As shown in Fig. 5, 3GPP proposed two network functions named TNGF and N3IWF to manage trusted non-3GPP APs and untrusted non-3GPP APs [23] in a 5G system. However, the convergence of multi-access networks makes the networks vulnerable because security contexts and levels of diversified access networks are uneven. Different security and privacy requirements of access networks jointly determine the security context between ME and CN during handover. Adversaries can attack a robust network through its interworking network with a low-security level. For example, an adversary can get the security context information transmitted between devices and the CN during authentication through a compromised Wi-Fi access point, then it is able to use this disclosed information to attack the next-hop connection.

2) Threats out of 3GPP Scope: Except for 3GPP access networks, there are many non-3GPP networks that make up a crucial part of the whole mobile communication system [29]. The most common non-3GPP networks are Wi-Fi [30] and WiMAX [31].

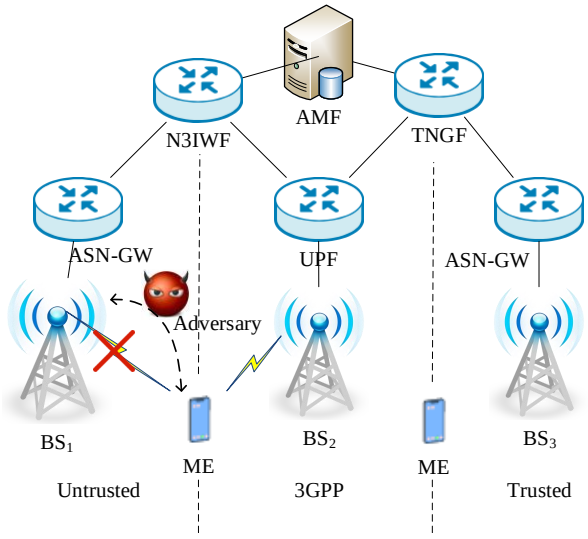


Fig. 5. Integrated network structure of non-3GPP and 3GPP networks

The latest version of Wi-Fi is Wi-Fi 6. It is a kind of WLAN technology based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 ax [32]. Its transmission speed is as fast as 9.6Gbps, which can meet the most critical needs of personal and business use in the 5G era. However, the latest security protocol used in Wi-Fi is Wireless Application Protocol 2 (WAP2), which has been found vulnerable to key reinstallation attacks [33].

WiMAX is a kind of wireless communication technology based on IEEE 802.16 standards [34]. The security of communication in WiMAX is protected by the Privacy Key Management Protocol (PKM), which ensures authentication to run correctly. Nevertheless, WiMAX is vulnerable to impersonate attacks [27]. Jatav et al. [35] found a collaborative attack model that combines scrambling and water-torture attacks together to implement destructive threats at the physical layer and it is more hidden than a single attack. Scrambling can disturb the connection between BS and a victim by catching and interfering unencrypted control messages. Water-torture attack is a kind of Distributed Denial of Service (DDoS) attack that uses Domain Name System (DNS) as an attack vector. Once the DNS server is taken down, the victim's domains will appear to be inaccessible.

As discussed above, security mechanisms, key management, encrypt algorithms, and privacy protection of Wi-Fi and WiMAX vary from each other, which brings a lot of difficulties to design a secure handover scheme for the handover between non-3GPP networks.

C. Attacks in Handover Process

Many potential attacks may threaten the security and privacy of 5G handover. Herein, we classify these attacks into five categories according to the taxonomy specified in [10].

1) Attacks against Authentication: The goal of attacks against authentication is to disrupt the mutual authentication between MEs and CN during the handover process. Impersonation attack is a typical attack in which an adversary impersonates the identity of another entity to get messages belongs to the impersonated entity [36]. It is also referred to as spoofing attack. In fact, this attack may be the basis of other attacks. Man-in-the-Middle (MitM) attack is another kind of attack on authentication [37], [38]. In the MitM attack, an adversary impersonates the identities of two communication entities and communicates with each one using the identity of another [37]. Consequently, it can establish connections with these two communication entities respectively and eavesdrop on valuable information through message forward.

2) Attacks against Integrity: An attack against message integrity is another threat to the handover in 5G networks. It could threaten the integrity of signaling and user data during handover. Representative attacks against integrity include but are not limited to message blocking, message modification attack, message insertion attack, and tampering attack.

3) Attacks against Confidentiality: An attack against message confidentiality is very common in various communication processes, so is handover in 5G. Passive and active adversaries try their best to get useful information about signaling and user messages. Confidentiality keeps the message from being obtained by illegal users.

4) Attacks against Availability: Availability means that network services are available to legal users. Attacks against availability in handover take up most of the resources so that legitimate user requests cannot be processed. DoS attack is the most common attack on availability. It could target all network entities in the handover procedure, especially at edge entities with low computation and communication capability, such as mobile devices, APs, or micro BSs. The DoS attack can be implemented in many Open System Interconnection (OSI) layers. For example, on the network layer, it is named Smurf attack and on the transport layer, it is called flooding attack.

5) Attacks against Privacy: The main attacks against privacy in handover target user identity, location, and other sensitive personal information. For example, when a user moves from a BS in his/her home network to a BS in a foreign network, the real identity of this user is under risk of disclosure attacks, since the real identity is transmitted during handover for access authentication. Typical attacks against privacy in handover include privacy violation and disclosure attack.

D. Security and Privacy Requirements for Handover in 5G

In [39], the authors analyzed and summarized the security requirements for the 5G system, which are listed below:

- Identity and location privacy of user/device: the real identity of the user/device covered should be hidden and the use of pseudonyms is suggested.
- Mutual authentication and key agreement between mobile devices and the network: the ME and the network should check their legitimacy before ME accessing the network. After that, they should negotiate a session key to protect communications between them.
- Confidentiality and integrity of data in the control plane: the confidentiality and integrity of control signaling should be ensured.
- Confidentiality of data in the user plane: the user data should be protected against unauthorized access.
- Security visibility and configurability: the relevant security features are visible to users and can be configurated based on user requirements.
- Platform security: secure execution environments in core network should be provided.

However, they did not mention strong security and privacy requirements for handover in 5G network. To protect the handover from the security and privacy threats mentioned in Section III-B, we specify the security and privacy requirements for designing a secure and privacy-preserving handover scheme in 5G networks. We draw Table II to show potential attacks on handover and corresponding requirements raised to resist them.

1) Security Requirements:

a) Mutual Authentication and Authorization: Authentication is the cornerstone of handover security. An ME should be successfully authenticated by both its source network and its target network whenever a handover occurs. On the other hand, the ME must confirm the validity of the target network before accessing it. After the success of mutual authentication, subscribed services should be negotiated and authorized for the ME. The requirements on mutual authentication and authorization mainly prevent the handover in 5G networks from attacks against authentication, e.g., impersonation attacks, spoofing attacks, and MitM attacks.

b) Confidentiality and Integrity: As 3GPP required, confidentiality and integrity of transmitted data should be guaranteed for control plane messages or user plane messages. This is a basic security requirement for the 5G networks, naturally also for handover. Correspondingly, ME and the network should agree on a session key after the handover in order to achieve confidentiality and integrity in each communication session against both passive attacks, such as eavesdropping, and active attacks, such as message blocking attacks, message modification attacks, and tampering attacks.

c) Forward Secrecy: Forward Secrecy (FWS) is a feature that for an entity with knowledge of session key K_m between the entity with a second entity, it is infeasible to predict any future K_{m+n} (n$>$0) used between a third entity and the second entity. Forward secrecy protects future communications from the threat of current keys leakage. In the context of handover, forward secrecy refers to the property that, for a gNB with knowledge of a K_{gNB}, shared with a UE, it is computationally infeasible to predict any future K_{gNB} that will be used between the same UE and another gNB.

d) Backward Secrecy: Contrary to FWS, Backward Secrecy (BWS) is a feature that for an entity with knowledge of session key K_n, it is infeasible to predict any previous K_{n-m} (n$>$m$>$0) from which K_n is derived. Backward secrecy protects previous communications from the threat of current keys leakage. In the context of handover, backward secrecy refers to the property that, for a gNB with knowledge of a K_{gNB}, shared with a UE, it is computationally infeasible to

predict any previous K_{gNB} that has been used between the same UE and a previous gNB.

e) Availability: Availability means that the network is available for legal users in any situation even under common attacks. The services should be robust anytime and anywhere even under DoS or DDoS attacks. Since 5G is an open environment, an adversary can attack ME or BS from different networks by raising various kinds of attacks. So, a handover protocol must defend against various kinds of attacks as aforementioned in Section III-C.

Note that formal verification is a set of methods that are critical for the development of a correct protocol and have been applied to the system design of hardware and software [40]. Formal verification is a necessary method to guarantee protocol availability and robustness.

2) Privacy Requirements:

a) Anonymity and Indistinguishability: In many handover scenarios in 5G networks, user identity privacy preservation is a significant requirement. Mobile users prefer to enjoy seamless mobile network services without using their real identities and exposing locations or other personally sensitive information. The real identity of an ME must be hidden from visiting networks or other MEs, and no attacker can link specific conversations to the real identity so that the user's privacy can be well protected from various attacks against privacy.

b) Non-traceability: To distribute pseudonyms to the mobile user is a good way to achieve anonymity, but the adversary is able to trace users by linking a number of fixed pseudonyms between different sessions. Therefore, it is necessary to ensure non-traceability in handover.

c) Conditional Privacy: Although it is quite significant to preserve user privacy, some sensitive information is requested to be provided in order to offer some services in certain situations. For example, when a user falls into a dangerous situation and needs help, his/her location should be conditionally available to ambulancemen. Thus, conditional privacy should be offered in the 5G handover.

TABLE II
ATTACKS AND CORRESPONDING REQUIREMENTS

Attacks	Corresponding Security Requirements
Attacks against Authentication	Mutual authentication and Authorization
Attacks against Integrity	Integrity
Attacks against Confidentiality	Confidentiality, Forward Secrecy and Backward Secrecy
Attacks against Availability	Availability
Attacks against Privacy	Anonymity, Indistinguishability, Non-traceability, and Conditional Privacy

E. Security Enabler Techniques

A number of security techniques construct the cornerstone of most security protection schemes. In this subsection, we briefly introduce them and classify them based on their functions in Fig. 6.

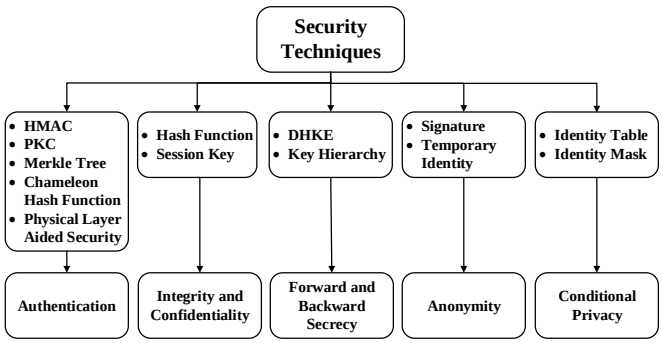


Fig. 6. Classification of security techniques

1) Public Key Cryptography: Public key cryptography is also called asymmetric cryptography. It is an essential building block to construct a secure protocol. Also, it's an important signature method to realize authentication between network entities. Many schemes deploy public key cryptography to complete initialization and re-authentication and build secure connections in handover. Diffie-Hellman Key Exchange (DHKE) is a key component for public key cryptosystem, which can let entities agree on the same session key. By employing it, communication parties can negotiate session keys by exchanging some public information over an insecure channel.

2) Symmetric Key Cryptography: Symmetric Key Cryptography uses the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. In the handover of mobile communication, symmetric key cryptosystem works along with hierarchical key management, for instance, key hierarchy in LTE or 5G networks. In general, there is a long-term key stored secretly, which can derive lots of session keys by using the key derivation function. The key derivation function is a well-designed function that can generate session keys by combining a nonce with the long-term key. Under this key hierarchy, even if the long-term key is exposed, the session key can still keep confidential. The key hierarchy in the 3GPP handover is shown in Fig. 7.

3) Merkle Tree: Merkle Tree is a tree data structure, consisting of a root node, a set of intermediate nodes, and a set of leaf nodes. Each leaf node can be verified through its authentication path from the leaf node to the root node. Since all authentication procedure only consists of hash function operations, Merkle tree is a lightweight authentication method.

4) Physical Layer Aided Security: Physical layer information [41] can be used to assist security protection, such as authentication and key generation. Owing to the natural randomness of physical layer information, they can be used to recognize the identity of communication entities. There are three mechanisms adopted commonly according to different randomness properties, which are Channel State Information (CSI)-based authentication, Radio Frequency (RF) recognition approaches, and wiretap code-based authentication [42], [43].

5) Hash Function: The hash function has been widely used in communication and security protocols. By comparing

two hash values, the message receiver can judge whether the message is modified to protect the integrity of communication data Hash-based Message Authentication Code (HMAC) is also often applied in authentication. Communication parties share a session key in advance. They use this session key to compute HMAC and compare the HMAC values to see whether they are equal. If so, communication parties achieve authentication.

6) Identity Privacy and Management: To avoid being identified as real identity in an open network, MEs use temporary identity to authenticate and communicate. And change temporary identity periodically can avoid being linked to a specific temporary identity. The authentication server stores a user's real identity and its corresponding temporary identity so that it can get the user's real identity according to his/her temporary identity.

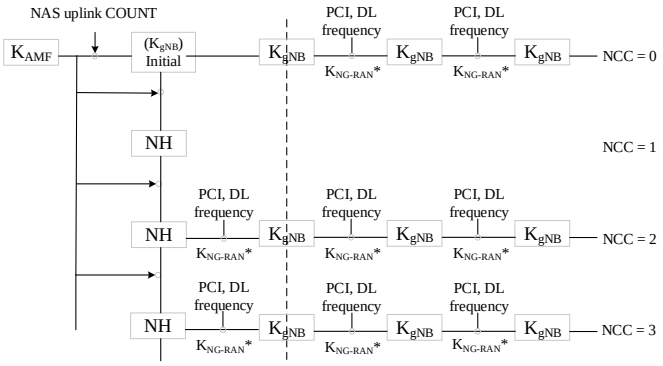


Fig. 7. 3GPP handover key hierarchy

IV. Security Countermeasures for Handover in 5G Networks

In this section, we review the security schemes proposed for handover in 5G networks based on the classification shown in Fig. 2. In our review, we comment the pros and cons of each scheme based on the proposed security requirements and specify their computation and communication overheads. Before going into details, we list the notations used in the evaluation of computation and communication overheads in Table III. Here, we abstract the operations of each protocol, such as modular multiplication, hash, modular exponentiation, etc. and we denote the time cost of each operation as symbols in Table III. For every handover protocol, we add up all time cost of operations to present the computation cost of the protocol. Similarly, we use δ, ϵ, η, γ, θ and μ to indicate communication cost between different entities and for every protocol we add up all communication costs in handover phase together as the communication cost of the handover protocol. All communication and computation cost in this paper are limited in handover phase without considering initial authentication when user access the network at first time.

A. Security Schemes for Vertical Handover

1) Handover within 3GPP Networks: With the emergence of 5G, existing interworking techniques are insufficient to address handover security issues. In 5G networks, Next Generation Radio Access Network (NG-RAN) provides both NR and E-UTRA for MEs to access CN, inter-RAT measurement is limited to E-UTRA according to the specification presented in [44]. A new BS gNB replaces LTE BS eNB in the 5G System (5GS). The gNB is responsible for decisions of horizontal handover, i.e., Xn and N2 handovers, in 5G networks according to the specifications described in [23].

TABLE III
Notation Description

Symbol	Description
T_m	The cost of modular multiplication
T_h	The cost of hash operation
T_e	The cost of modular exponentiation
T_p	The cost of pairing function
T_s	The cost of symmetric encryption/decryption operation
T_{as}	The cost of asymmetric encryption/decryption operation
T_{ABS}	The cost of attribute-based sign operation
T_{KDF}	The cost of key derivation function
δ	The delay of communication between ME and BS
ϵ	The delay of communication between BSs
η	The delay of communication between MMEs
γ	The delay of communication between BS and MME
θ	The delay of communication between ME and MME
μ	The delay unit of communications between MEs

The 5G standard [45] defines interworking as Inter-RAT mobility, which refers to mobility between 5G and LTE networks. The inter-RAT handover is backward, so resources are prepared in a target 3GPP access system before ME is commanded by a source 3GPP access system to change to the target 3GPP access system. To ensure handover with other 3GPP networks (i.e., LTE), 5GS introduces converged interoperability architecture. A subcomponent in NG-RAN called Serving Gateway (SGW) provides mobility management for handovers. The interworking of 5GS with other 3GPP networks is performed at higher layers and therefore is less complex than the interworking of 5GS with non-3GPP networks.

For the handover from Evolved Packet Core (EPC)/E-UTRAN to 5GS/NG-RAN as shown in Fig. 8, the EPC maps its 4G-Globally Unique Temporary Identity (GUTI) to 5G-GUTI and 5GS keeps its Packet Data Network (PDN) session according to its PDN session ID. Then, the source MME sends ME's security context to the target AMF, and the target AMF derives a key K_{AMF} from the received security context. Further, AMF shall derive K_{gNB} from K_{AMF}. Simultaneously, the ME can obtain K_{AMF} and K_{gNB} in the same way. Afterwards, the Packet Data Network Gateway (PGW) performs a release of resources in EPC for PDN connections. The whole procedures are executed in CN, so the security and privacy of these handovers can be guaranteed under the security framework of a 5G core network. For communication cost, as shown in Fig. 8, there are two communications between MME and AMF, three communications between ME and BS, five communications between BS and AMF or MME,

so the whole communication cost for handover phase is 2η + 3δ + 5γ. As for computation overhead, since this process only consists of four hash operations, so the computation cost is $4T_h$.

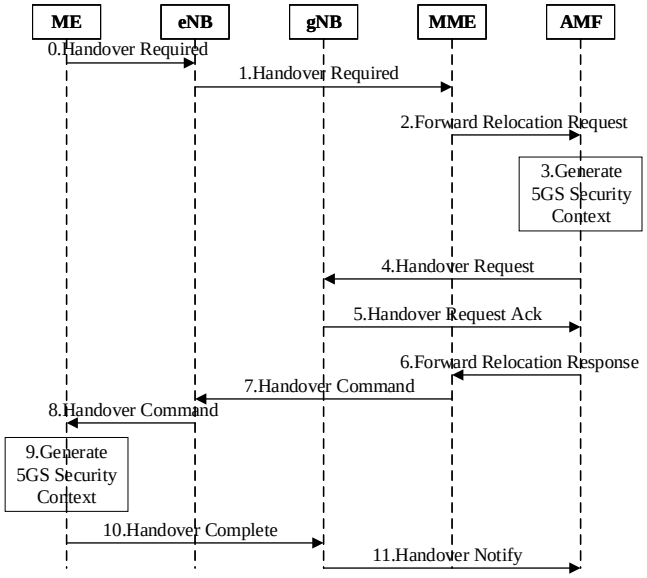


Fig. 8. Handover from EPC to 5GS

2) Handover between 3GPP and Non-3GPP Networks: Earlier in 3G, 3GPP proposed an interworking structure between the Universal Mobile Telecommunications System (UTMS) and non-3GPP networks to provide sound services to support user mobility [46], [47]. Later in 4G, E-UTRAN even supports more access technologies. Generally, 5GS is more heterogeneous with various access technologies than LTE. Consequently, many researchers focus on designing fast and secure handover schemes between 3GPP and non-3GPP networks. The basic procedure of handover from a non-3GPP network to 5GS is shown in Fig. 9. N3IWF is a link set between the two networks. Same as the calculation method of handover from EPC to 5GS, the computation and communication costs of handover from a non-3GPP network to 5GS are $7T_h$ and 2η + 3δ + 5γ, respectively.

Song et al. [48] and Cao et al. [49], [50] both proposed handover authentication schemes between 3GPP and non-3GPP networks based on the 3GPP network structure. Song's scheme introduces an additional network element named Data Forward Function (DFF) to achieve authentication even when the ME disconnects with a target BS. This scheme reduces handover delay, but it only meets such basic security requirements as mutual authentication confidentiality and integrity protection. This scheme consumes 3δ in communication between ME and BS. Other security and privacy requirements were not considered.

In contrast, Cao's scheme not only reduces the delay of authentication but also improves the security of authentication. It guarantees mutual authentication based on Identity-Based Cryptography (IBC) [51]. When MEs request for handover, legally registered MEs and BSs can negotiate a consistent token based on their public and private keys. As a random value used in Key Derivation Function (KDF), it is updated in every session, this scheme can realize FWS. Since a pairwise transient key is agreed between ME and BS, confidentiality and integrity of messages can be protected. In the end, the authors gave a test result under a model checker. The result shows that these schemes can resist such protocol attacks as MitM attacks, impersonation attacks, etc. However, identities of users are transmitted in plain text when the ME launches a handover request in [49], [50] so that the identity privacy of users is not protected, , therefore, non-traceability and conditional privacy were not achieved. As for computation and communication overheads, these two schemes both cost $4T_h + 5T_m$ at ME side and consume 3δ for communicates between ME and BS.

3GPP and WiMAX Forum respectively specified interworking architectures between 3GPP networks, WLAN, and WiMAX [31], [52]. In [53], he authors proposed a scheme that modifies the standard Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) protocol to derive handover related parameters. It also reduces the authentication delay by rejecting redundant communications with a home network. The key is reused in this scheme when ME revisits the network. In addition to fast authentication, this scheme also provides some security features, like mutual authentication, confidentiality, integrity, FWS, and BWS, but it does not offer good privacy protection. Unfortunately, the robustness test on this scheme was not given. The communication delay of this scheme is up to 3δ+3θ+γ+η. The authors did not discuss computation cost.

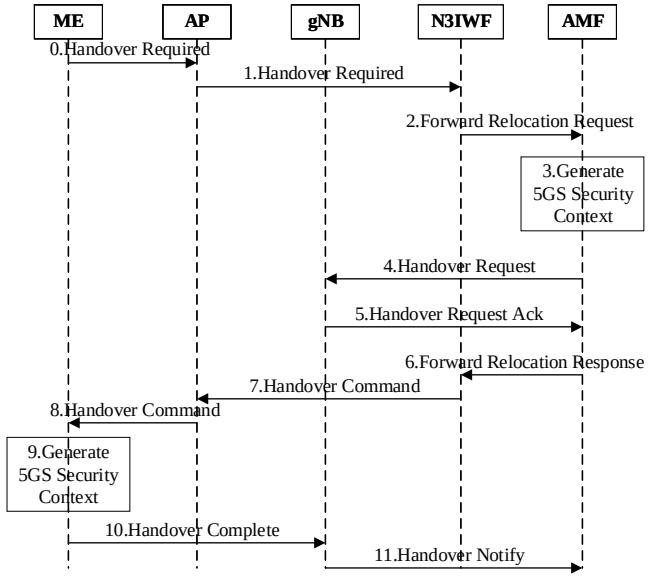


Fig. 9. Handover from a non-3GPP network to 5GS

With the emergence of SDN, a new handover authentication mechanism based on SDN was proposed [54]. By using SDN, the control logic unit was removed from the underlying infrastructure and was replaced by a controller in the control plane of SDN so that software can be installed in the controller to provide global and efficient management over a whole HetNets. In [55], the authors proposed an SDN-based

authentication structure as depicted in Fig. 10. It implements an Authentication Handover Module (AHM) and a Privacy Protection Module (PPM) in the SDN controller. The controller can trace and predict ME's location and inform relevant cells of potential handover. Additionally, this authentication mechanism is a non-cryptography method in which an ME proves its identity with unique Secure Context Information (SCI) consisting of identity, location, round-trip time, and physical layer attributes. But the authors did not provide a detailed algorithm about how to compare two secure context information. Later, Duan et al. [56] proposed a protocol to instantiate the security authentication structure proposed in [55]. In Duan's scheme, a user's privacy can be protected by dispersing user sensitive data over different SDN-controlled network paths. This scheme reduces computation overhead at the user side to zero, and it only takes 2δ to complete handover. Nevertheless, this scheme does not support mutual authentication, the SCI transferred between BS and MEs is vulnerable to eavesdropping attacks. Moreover, the authentication in this scheme is one-way, i.e., every AP is able to get the identity of MEs but MEs cannot verify the validity of the network.

After, Ozhelvaci et al. [57] proposed a more secure scheme by deploying Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) module in SDN networks to realize mutual authentication, confidentiality, integrity, anonymity, and non-traceability. After comparing the SCI from both ME and the SDN controller, the target AP can authenticate the identity of ME. Then ME can start to negotiate a session key. This scheme achieves mutual authentication and protection of user privacy, but it fails to ensure FWS and does not consider conditional privacy. Its communication cost is 11δ. Computation cost in this scheme was not mentioned.

Alam and Ma proposed a handover scheme based on SDN and Merkle tree [58]. By transferring data through the SDN controller, handover delay is reduced. Also, applying the Merkle tree decreases communication overload. This work not only achieves high efficiency but also improves security and privacy preservation. Mutual authentication, confidentiality and integrity protection, FWS, anonymity, and non-traceability were also supported in this scheme. Moreover, dual connectivity and coordinated multipoint access are supported, too, thus this scheme sharply improves the efficiency of authentication. Nonetheless, conditional privacy is not offered. Notably, analysis against attacks was presented in an informal way in [58]. This scheme only takes $5T_h$ and δ+ϵ to complete handover authentication.

Cao et al. [59] proposed a handover scheme by integrating the capabilities of network entity proposed in [60] into Duan's scheme [55]. The scheme fulfills all the security and privacy metrics as described above with low computation and communication overheads. In this scheme, an AHM in the SDN controller is deployed in the SDN controller to assist the whole handover procedure including predicting the location and traverse route of MEs and transmitting relative information to candidate cells. The target BS authenticates an ME by checking a credential generated by AHM. In this credential, a temporary identity and the capability of ME are sealed and signed by AHM. It works like a ticket or getting a permission to access to the target network. On the ME side, it verifies the target BS through the Message Authentication Code (MAC) generated by the secret key of the target BS. But there is a flaw in this scheme that the credential of ME is constant without being updated. Once one BS is compromised, the security and privacy of the ME will be in high risk. Regarding computation and communication overheads, it separately takes $4T_h + 2T_s$ and 3δ.

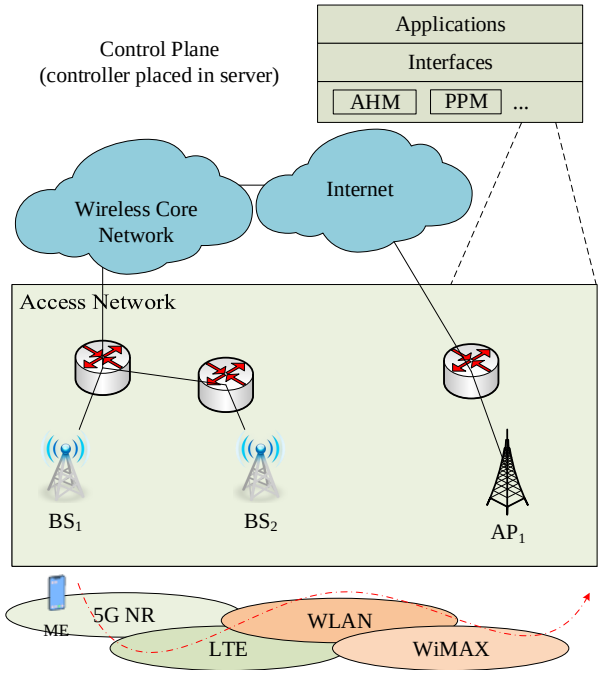


Fig. 10. SDN-enabled 5G wireless HetNets structure

Recently, blockchain technology has gained tremendous attention. Blockchain is a decentralized structure with several key characteristics, such as decentralization, persistence, anonymity, and auditability [61]. Many researchers are leveraging blockchain technology to solve 5G security handover issues. Yazdinejad et al. [62] proposed a scheme that combines blockchain with SDN to improve security, privacy, and efficiency of handover. In this scheme, a new network entity called blockchain center is deployed outside an access network. It is responsible for generating and storing security parameters. Underneath the blockchain center, there is an SDN controller network. Once one SDN controller is down, the blockchain center can manage the access network via other controllers. As for handover, owing to the common blockchain center, there is no need for re-authentication when an ME leaves one cell and enters another under the same controller. In other situations, the BS can authenticate MEs by using authentication information got from the blockchain center. The blockchain center regularly checks whether the BS is valid. One advantage of deploying blockchain is that all information is on the blockchain so that nobody can repudiate it. However, this scheme introduces high communication overhead between the SDN controller and the blockchain center. Moreover, the authors only considered data privacy rather than identity and location privacy. On the other hand, there is no stable attack

simulation result provided in this paper. As for efficiency, a block where handover-related keys are stored is produced per second, which is far from the requirement of handover delay.

To remove an Authentication, Authorization, and Accounting (AAA) server and a global private key generator from the handover structure, Zhang et al. [63] introduced blockchain into handover as a global storage media. To implement handover authentication without a private key generator, the authors adopted the chameleon hash into the handover. The chameleon hash is a special hash function with a trap door to compute a collision [64]. Therefore, given a pre-registered hash value, a legal ME can generate the same hash value because only the legal user knows the trapdoor of the chameleon hash. With this scheme, an ME generates a chameleon hash value when it is firstly registered into the AAA server and the AAA server records the hash value in the blockchain. The ME can check the validity of the hash value through the blockchain to ensure consistency of the hash value. When a handover happens, the ME produces a pair of parameters that can lead to the same hash value as on the blockchain, then sends them to the target BS to prove the legitimacy of its identity. In turn, the target BS also uses the same way to prove its legitimacy. Moreover, the authors leveraged the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol and used two random values to guarantee the FWS. Since the authentication information is not sent to the AAA server, no one can track the MEs, However, conditional privacy was not considered in this scheme. As for efficiency, it needs $4T_h + 10T_m$ at ME side and communication overhead is 3δ.

Blockchain also can be combined with IoT. Shen et al. [65] proposed cross-domain handover protocols for industrial IoT based on blockchain. In each domain, there is a Key Generator Center (KGC), an Authentication Agent Server (AAS), and a Blockchain Agent Server (BAS), responsible for key generation, authentication and blockchain operation respectively. This scheme is based on blockchain and IBC. ME sends a handover request with an identity-based signature, and the corresponding public key of ME is shared on blockchain. If the foreign domain can get the public key of ME and decrypt the signature, ME can verify its legality via a signed message. In the meanwhile, foreign can authenticate ME based on the signature. However, in this scheme, ME outsources heavy computational operation to the agent server and the private key of ME is also kept in the agent server which is not secure. Therefore, the computational cost on the ME side is $3T_e$ and the communication overhead is $6(\delta + \gamma) + 10\theta$.

Guo et al. [66] proposed a master-slave blockchain-based cross-domain handover mechanism in IoT. The main chain and slave chain are both consortium blockchains on account of efficiency. Each slave chain represents an IoT domain and the connected devices have built a trust relationship with the network. The main chain is responsible for ensuring cross-domain trusted handover of IoT devices. When handover happens, a certificate of a device is transmitted from the source domain to the target domain via the main chain so that the target domain and the device can perform mutual authentication. As for efficiency, this scheme needs T_{as} on computation and 2δ on communication. Nonetheless, the authors only considered mutual authentication and session key establishment.

Similar to the multi-blockchain system structure in [66], Dong et al. proposed a cross-domain authentication for IoT based on the Cosmos network. Cosmos network is a heterogeneous network that supports interactions between different blockchains. By the Cosmos network, handover-related information can be transferred from the source domain to the target domain successfully. However, the authors only proposed a handover framework in this paper rather than a detailed protocol.

D2D communication is a kind of communication that mobile users communicate directly to each other without the help of a BS or CN. It is considered as a new paradigm to revolutionize the traditional communication ways of cellular networks [2]. Some researchers have studied D2D communication security and privacy preservation [67]–[69]. However, research on handover security and privacy preservation in D2D communication is still a blank. Consequently, Kumar et al. [70] proposed a handover scheme for D2D communications in 5G-WLAN networks. The BS authenticates users with the help of an AS based on bilinear pairing. However, its computation cost is quite high because of pairing operations and exponential operations. Although all the security and privacy requirements except conditional privacy are fulfilled, handover delay is not a neglectable attribute. Its computation overhead is heavy, which takes $7T_h + 5T_m + 2T_p$ and the communication overhead is 3δ.

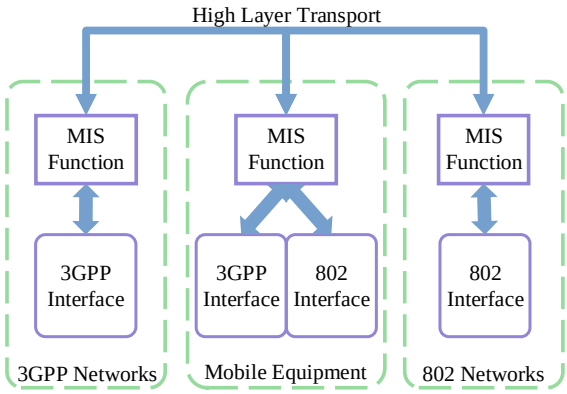


Fig. 11. The MIS structure between networks

The aforementioned schemes are all about one ME handover between networks. Some researches focus on group-based handover authentication schemes [71]–[73]. Cao et al. [71], [72] proposed two schemes of group handover authentication in LTE networks by using an aggregate signature to reduce communication costs. Instead of performing authentication one by one, group members choose a leader to aggregate all signatures generated by them and communicate with MME or Access Service Network Gateway (ASN-GW) to complete handover authentication. If handover is performed successfully, all group members can separately establish a secure tunnel with MME or ASN-GW. Although the scheme in [71] can reduce signaling overhead, the aggregate signature algorithm suffers from a key escrow problem, which is caused by an untrusted Private Key Generator (PKG) that holds all private keys to sign and decrypt

user messages illegally. Moreover, its computation overhead is heavy, which needs $2T_h + (8 + n)T_m + T_{as}$, although communication cost is 3δ. FWS, BWS, and privacy were not considered in this work. Furthermore, the authors did not give a detailed security proof, neither simulate attacks to study its robustness.

Lai [73] made some modifications based on Cao's scheme and proposed a group handover scheme for Machine-to-Machine (M2M) communications between 3GPP and WiMAX. It introduced a certificateless aggregate signature-based scheme to overcome the drawback of key escrow in ID-based aggregate signature schemes and realized FWS. But the authors only considered identity privacy. The cost of ME is that computation takes $T_h+(7+n)T_m+T_s$ and communication takes 4θ.

Lately, Cao et al. [72] came up with a group handover authentication scheme in LTE-A&WLAN HetNets. With this scheme, the handover is divided into two cases, the handover to a new WLAN and the handover to a previously visited WLAN, thus the handover procedure can be speeded up. It deploys an Aggregate Message Authentication Code (AMAC) to aggregate all messages of group members into a single message for authentication. All the aforementioned security and privacy requirements except conditional privacy are met in this scheme. In addition, if some group authentication messages from a group member are compromised or modified by an attacker, which fails authentication, the AAA server can quickly find out the rogue group member. Compared to previous work [71] , this paper gave detailed security proof and considered identity privacy as well as location privacy. In particular, communication and computation overheads are $4T_h$ and 3δ+4ϵ, respectively.

3) Handover between Non-3GPP Networks: As the most common non-3GPP networks are WLANs, especially Wi-Fi and WiMAX, we review schemes to support handover between Wi-Fi and WiMAX. IEEE proposed a Media Independent Services (MIS) framework [22] shown in Fig. 11, which enables the optimization of services including the handover between heterogeneous IEEE 802 networks. There are four main services in MIS services: Media Independent Event Service (MIES), Media Independent Command Service (MICS), Media Independent Information Service (MIIS), and management service. The MIES defines status change events in a dynamic link. The MICS provides commands to control a link status. The MIIS consists of a series of information-related elements, structure, and transfer mechanisms to provide information transformation services. Finally, the management service is responsible for registration and service discovery. By using these four services and deploying a standard service interface at a high layer, the MIS framework enables applications in the high layer to ignore different media-specific layers.

In academic, there are also plentiful researches [74]–[76] on handover between non-3GPP networks. Formally, when an ME executes handover from one network to a HetNet, the ME should mutual re-authenticate with the target network access server. Sun et al. proposed a scheme [75] to securely transfer a current session key from a serving network to a target network. By reusing the session key, the proposed scheme enables ME to access the target network without executing an entire authentication process. When handover happens, the only negotiation between two ASs is needed. Meanwhile, the handover scheme adopts public key cryptography and symmetric cryptography to guarantee the confidentiality of handover information. But, to transfer the session key from Wi-Fi to WiMAX may expose the session key to a risk of leakage. If one network is compromised by an adversary, the other network will be corrupted consequently. The corrupted network can use a false base station attack against legitimate users [77]. In short, this scheme realizes mutual authentication, confidentiality, and integrity protection, as well as FWS. It does not consider the privacy requirements of handover. Neither, the authors gave formal proof of security. The communication overhead of the scheme is 4δ+γ+η+θ.

Yan et al. [76] proposed an improved scheme by using both access authentication and Mobile IPv6 (MIPv6) authentication to guarantee network security, but there is no detailed description of the handover scheme. Privacy was not considered, either. In this scheme, communication takes 2θ+ϵ. Eastwood et al. [74] proposed a scheme to acquire information about a target network including service availability, and owner identity of the network by applying MIS. However, these two schemes only achieve mutual authentication and key establishment. All these three schemes [74]–[76] did not discuss computational overhead.

Different from the aforementioned schemes that reuse the session keys, Hou et al. [78] proposed a fast authentication scheme with a pre-authentication structure in Wi-Fi/WiMAX hybrid networks. This scheme does not modify the authentication in Wi-Fi and WiMAX standards, but just divide authentication into a pre-authentication phase and a re-authentication phase. During authentication, there is no communication between the AP and AS. Nevertheless, this scheme does not improve the robustness of handover security. EAP-TLS protocol was adopted in this scheme so that mutual authentication, confidentiality and integrity protection are fulfilled. As for privacy protection, the authors did not consider it. Regarding communication overhead, it takes δ+2γ+θ.

Some researchers proposed an interworking function to realize communications between Wi-Fi and WiMAX. Huang et al. [79] used a Wi-Fi Interworking Function (WIF) in a WiMAX network to communicate with the AAA server to guarantee security. This scheme retains the security requirement in Wi-Fi and WiMAX specifications. In this scheme, mutual authentication, confidentiality, integrity, and user anonymity are guaranteed, but other security and privacy requirements are not considered. The communication overhead of this scheme is 2δ+2θ, while computation cost is not discussed. Similarly, Yang et al. [80] designed a scheme based on WIF and PKC. The authors achieved user anonymity by distributing a pseudonym to ME and direct handover by using a private key to generate a consistent token. In this scheme, security and privacy requirements are fulfilled except conditional privacy. However, this paper lacks solid security proof. As for computation and communication overheads, they are $3T_h + 6T_m$ and 3δ, respectively.

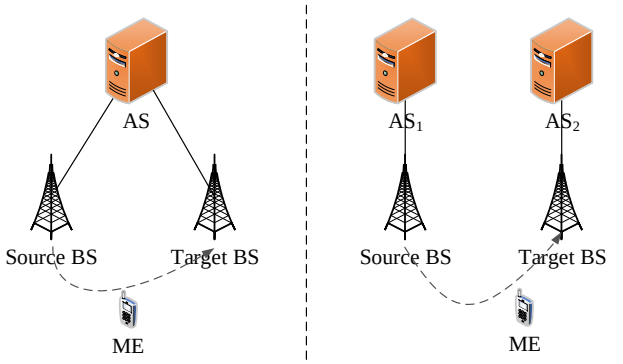
In the meanwhile, Fu et al. [81] proposed a handover

authentication scheme based on a ticket generated by a previously visited network, which can be used to perform key agreements without connecting to the AAA server. In particular, two APs in different networks can easily derive a session key with this ticket, so that confidentiality and integrity are promised. Moreover, with a random number in both ME and AP during the execution of the key agreement protocol, the scheme achieves FWS and BWS. A formal analysis of this protocol was given by using a formal verification tool. However, privacy issues were not considered in this protocol. The communication overhead of this scheme is $5T_m+4T_{KDF}$, while its communication overhead is 4δ.

We summarize and compare the security performance of vertical handover schemes analyzed above in Table IV. We use $\surd$, $\times$ and - to indicate whether these requirements are met or not considered in these schemes.

B. Security Schemes for Horizontal Handover

Horizontal handover or roaming is another common handover scenario. We divide horizontal handover into two types: intra-MSC and inter-MSC handover, according to handover range. These two types of handover are depicted in Fig. 12.



(a) Intra-MSC handover (b) Inter-MSC handover

Fig. 12. Intra-MSC and inter-MSC handover structure

1) Intra-MSC Handover: Intra-MSC handover is a kind of internal handover between cells controlled by a single BS or between two different BSs controlled by one MSC, in which three entities are involved, a source BS, a target BS, and a ME.

Some schemes [83]–[86] use AS to authenticate the ME when it performs handover between BSs. This kind of scheme is called AS-based scheme with such an assumption that AS has powerful security features. Kumar et al. [83] proposed a handover authentication scheme for WLAN. This scheme uses Identity-Based Signature (IBS) to achieve mutual authentication between ME and AS. However, this scheme does not provide conditional privacy and proof of security. The computation overhead is $2T_h + T_m + 3T_e + 2T_s$ and the communication overhead is 2δ+γ.

Sharma et al. [85] proposed a handover scheme with the assistance of the AS for 5G Xhaul networks [87]. MEs perform authentication via a pre-shared secret key between MEs and AS. Every time when the handover procedure completes, the session key will be updated. It fulfills all security and privacy requirements except conditional privacy with $4T_h + T_m + 2T_e$ computation cost and 6δ+2γ+ϵ communication overhead. Recently, Chen et al. proposed a handover authentication scheme based on a Number Theory Research Unit (NTRU) algorithm [88]. Since the NTRU algorithm is based on lattice theory that is secure against quantum adversaries, this scheme is sufficiently secure even though a quantum computer is created. In this scheme, an ME uses a family of uncorrelated pseudonyms. Every pseudonym is only used once during authentication. This scheme provides good security performance with low computation cost for cryptographic operations. However, Wang et al. [89] pointed out that every valid participant in the authentication can recover the private key of AS and has the possibility of impersonating the AS.

The second type of handover authentication scheme is called Security Context Transfer (SCT)-based scheme. In this type of schemes, authentication context is transferred without involving the AS, which effectively enhances the efficiency of authentication. Choi et al. [90] proposed a scheme based on chameleon hashing. In this scheme, an AS generates two chameleon hash values and related key pairs for ME and AP. As only ME and AP know the trap door of chameleon hash, nobody else can compute the same hash value. The ME and the AP authenticate each other using the hash value as a credential without involving direct communication between APs. The computation cost and communication overhead are $4T_e + T_{as}$ and 3δ, respectively. Gupta et al. [91] proposed a handover scheme based on the chameleon hash and Public Key Cryptography (PKC) that not only realizes mutual authentication, confidentiality, integrity, FWS, anonymity, and non-traceability but also solves the key escrow problem. However, this scheme's computation cost is $3T_h + 3T_m + T_{as}$, which is higher than Choi's scheme [90]. But it has a lower communication cost as 2δ. Fu et al. and Abouhogail et al. [92]–[94] proposed handover protocols based on a signature which can be used as a ticket for fast authentication, but Fu's schemes [92], [93] demand that MEs and APs share a same group identity, which is not practical in most scenarios and neither schemes provide conditional privacy. Abouhogail's scheme [94] fails to establish a session key between MEs and APs. Moreover, it cannot offer FWS.

The third type of handover authentication is physical layer-based handover. As physical layer attributes are environmentally dependent random features that can be used as a natural credential, it can achieve lightweight authentication without applying cryptographic methods. Moreira et al. [95] proposed a cross-layer handover scheme by using received Radio Signal Strength (RSS) to authenticate and applying a fingerprint source to generate an unpredictable secret key. Since the pre-shared key is generated from unpredictable RSS, this scheme can guarantee FWS. Applying the trust zone not only simplifies frequent handover but also obfuscates ME's location.

Similarly, Fan et al. [96] proposed a region-based handover scheme for small cell networks. Quite similar to the aforementioned trust zone, the main idea of this scheme is to build a region containing one eNB and several Home Evolved Node

TABLE IV
COMPARISON OF VERTICAL HANDOVER SCHEMES

Scheme	MA	CI	FWS	BWS	AD	AI	NT	CP	Computation overhead	Communication overhead
[47]	√	√	×	√	×	√	×	×	$7T_h$	2η + 3δ + 5γ
[49]	√	√	×	√	√	×	×	×	$4T_h + 5T_m$	3δ
[50]	√	√	×	√	√	×	×	×	$4T_h + 5T_m$	3δ
[53]	√	√	√	√	√	√	√	×	-	3δ+3θ+γ+η
[56]	√	-	-	-	-	-	-	-	-	-
[55]	√	×	×	×	×	×	×	×	0	2δ
[58]	√	√	√	√	√	√	√	×	$5T_h$	11δ
[82]	√	×	×	×	√	×	×	×	$T_h + 3T_s$	3δ
[59]	√	×	×	×	√	×	×	√	$4T_h + 2T_s$	3δ
[62]	√	√	√	√	×	×	×	×	-	-
[63]	√	√	√	√	√	√	√	√	$4T_h + 10T_m$	3δ
[70]	√	√	√	√	√	√	√	×	$7T_h + 5T_m + 2T_p$	3δ
[71]	√	√	√	√	×	√	√	×	$2T_h + (8+n)T_m + T_{as}$	3δ
[72]	√	√	√	√	√	√	√	×	$4T_h$	3δ+4γ
[73]	√	√	×	×	×	√	√	×	$T_h + (7+n)T_m + T_s$	4θ
[74]	√	√	×	×	×	-	-	-	-	-
[75]	√	√	×	×	×	-	-	-	-	4δ+γ+η+θ
[76]	√	√	×	×	×	-	-	-	-	2θ+ϵ
[77]	√	√	√	√	×	√	√	×	-	δ+2γ+θ
[78]	√	√	√	√	×	×	×	×	-	2δ+2θ
[79]	√	√	√	√	×	√	√	×	$3T_h + 6T_m$	3δ
[80]	√	√	×	×	√	×	×	×	$5T_m + 4T_{KDF}$	4δ

MA: mutual authentication; CI: confidentiality and integrity; FWS: forward secrecy; BWS: backward secrecy; AD: availability and dependability; AI: anonymity and indistinguishability; NT: non-traceability; CP: conditional privacy;
T_m: computation cost of multiply operation; T_h: computation cost of hash point function; T_p: computation cost of bilinear pairing function; T_e: computation cost of modular exponentiation; T_{KDF}: computation cost of key derivation function; T_s: computation cost of symmetry encryption/decryption operation; T_{as}: computation cost of asymmetric encryption/decryption operation
δ: transmission time between ME and BS; ϵ: transmission time between BSs; η: transmission between MMEs; θ: transmission between ME and MME; γ: transmission between MME and BS; μ: transmission between MEs
- : this scheme does not consider in paper; ×: this scheme does not satisfy the requirement ; √: this scheme satisfies the requirement

Base Stations (HeNBs). When an ME firstly enters a new region, it completes a full initial handover authentication and is issued a warrant for future handover. If the ME possesses a regional warrant and is ready to handover to another HeNB under the same eNB, it can use the warrant to perform a fast handover with assistance of MME and the AAA server. In fast handover, upon receiving the warrant, the AAA server checks the expiration time and validity of the warrant at first. If it holds, the AAA server will compute a new session key and a temporary identity for the ME in case of anonymity and key compromise. However, in this scheme, the ME must communicate with the AAA server via eNB every time, which causes heavy communication overhead.

The last method of handover authentication is direct handover based on PKC. By deploying PKC, mutual authentication can be achieved straightaway. When a handover authentication happens, an ME first sends a handover request to a target AP. Both legal ME and BS/AP can get private keys from AS. Using the private keys, ME and BS/AP can derive a consistent token and achieve mutual authentication and generate a session key based on the token. In the end, the target AP may inform the AAA server of the successful handover authentication.

Many cryptographic technologies can be adopted to achieve handover. He et al. proposed a privacy-preserving handover scheme based on a bilinear pairing function [97]. They continuously deployed IBC to implement mutual authentication. Its computation cost is $3T_h + T_m + T_p$ and its communication overhead is 2δ. Later, Islam et al. [98] proposed a handover authentication scheme without using bilinear pairing, which enormously improves the efficiency of handover. It satisfies all the requirements mentioned above by using IBC. After authentication, target AP informs AS of successful handover and sends handover parameters to AS. And if necessary, AS can get the real identity of ME according to the pseudo-identity. As for efficiency, its computation overhead is $2T_h + 4T_m$ and its communication cost is 2δ.

Jo et al. [99] proposed a handover scheme based on IBC, similar to the abovementioned schemes. It uses a signcryption algorithm to minimize the number of pseudo identities in subscriber identification cards. The authors claimed that their scheme is formally proved secure in a Canetti-Krawczyk (CK) model [100]. But computation and communication costs are both high, which are respectively $7T_h + 3T_m + 2T_e + T_{KDF}$

and 3θ. However, recently, Odelu et al. [101] proved that Jo's scheme fails to achieve security under the CK-adversary model, and is also vulnerable to user impersonation attack.

Xu et al. [84] proposed a scheme with all security requirements satisfied except conditional privacy. Nevertheless, the computation cost of this scheme is high, which reaches $2T_h + 3T_m + 2T_s + T_p$. Yang et al. [102] proposed another scheme that greatly reduces computation cost, but remains the same security level as [84]. The computation overhead of this scheme is $4T_h + 4T_m$ and communication overhead is 2δ. Unfortunately, formal proof of security is missed in [102]. Similarly, Mo et al. [103] proposed an efficient handover based on IBC without using any pairing functions. In addition, the authors proved the security of mutual authentication, confidentiality, integrity, FWS, user anonymity, and non-traceability. The computation and communication costs are $2T_h + 5T_m$ and 2δ, respectively.

Li et al. [104] proposed a privacy-aware handover authentication scheme by using IBS. When an ME first enters the network, it performs full authentication and builds a secure connection with a serving AP. Also, AS distributes security parameters to every legal AP. And when an ME moves into the coverage of a new AP, it generates a signature and sends it to the target AP together with its pseudonym distributed from AS. After receiving this message, the target AP first checks the timestamp of the signature for resistance against a replay attack. Once the signature is accepted, the target AP sends a response message to the ME consisting of the identity of the target AP and a MAC. The ME can verify the identity of the target AP by comparing MAC with its computing result. If two values are equal, the authentication is successful. Otherwise, it fails. The computation cost of this scheme is $4T_h + 5T_m$ and communication overhead is 2δ. However, this scheme suffers from an impersonation attack since the ME cannot identify the legality of the target AP. When an attacker eavesdrops on the request message from an ME, it is easy for the attacker to calculate a certain value of MAC and session key by using its own identity. After receiving the response message from the attacker, the authentication procedure goes on, and then the ME builds a connection with the impersonated "AP" without aware that this "AP" is an attacker. Both Chaudhry et al. [105] and Xie et al. [106] found this weakness and changed a parameter used in verifying a legitimate user to remedy this flaw with the same computation and communication overheads. He et al. proposed [107], this scheme have deployed group signature to realize high security and privacy. Forward secrecy and backward secrecy are supported, because of a dynamic user revocation mechanism of the adopted group signature. However, the authors did not give detailed security proof, and its computation cost is too heavy due to the usage of a group signature. It does not meet the requirement of efficiency although its communication overhead is 2δ.

Attribute-Based Signature (ABS) is a kind of public-key signature that users sign messages with any attributes issued from an attribute authority. Using ABS, a signer can keep anonymous and is indistinguishable among all the users whose attributes satisfy the predicate specified in the signature [108]. This feature makes it appropriate to be applied in anonymous authentication. Zeng et al. [109] proposed an ABS-based anonymous handover scheme. However, its computation overhead is too heavy to be applied in practice. As noted, the authors did not give security proof on their scheme. Unfortunately, all public-key-based handover methods need a trusted third party as a private key generator and are vulnerable to the key escrow problem.

2) Inter-MSC Handover: Inter-MSC handover happens when an ME moves between two different base stations belonging to different MSCs.

Cao et al. [110] proposed a uniform handover authentication scheme based on the proxy signature for all potential handover scenarios. Taking advantage of the proxy signature, ME and the target BS can ensure mutual authentication by checking the message from the other side whether the AS signs or not. After authentication, ME and the BS negotiate a session key using DHKE. This scheme performs well in terms of security, it fulfills mutual authentication, confidentiality, integrity and FWS. Strong security proof of security was also given. However, this scheme cannot protect the privacy of user identity very well, since it uses the GUTI rather than a pseudonym for authentication, which can be traced when the GUTI is used for a long time. Moreover, this scheme requires MEs to perform five times of RSA verification, which increases the computation cost that is up to $3T_h + 4T_m + 4T_e$. The communication overhead is 3δ+4γ+2η. Gupta et al. [111] proposed another handover scheme based on a proxy signature to overcome the drawbacks of privacy preservation in Cao's work [110]. They also considered revocation property of users in all mobility scenarios. Unfortunately, the communication and computation overheads of their scheme increase accordingly, which are $11T_h + 11T_m$ and 3δ+6γ+2η, respectively. Qiu et al. [112] proposed a similar scheme to decrease the high computation and communication cost of Cao's scheme, which are $6T_h + 4T_m$ and 3δ, respectively.

Ahmad et al. [113] proposed a handover scheme that makes use of an ME's historical mobility pattern. When an ME is ready for handover, it first looks into its mobility history to select a target cell. If its current trajectory is not in a historical record or the load of the target cell is full, the ME will look for a new target cell according to its distance from other BSs. But the authors only considered the efficiency of handover regardless of security and privacy issues. This work only helps MEs decide which BS to connect with rather than a detailed handover scheme. Sharma et al. [114] introduced blockchain into distributed mobility management to implement secure and energy-efficient handover in fog networks. As shown in Fig. 13, three types of blockchain are used in this framework, namely Proof of Work (PoW)-wise, region-wise, and user-wise. The PoW-wise blockchain is at a fog server level in a fog network. It is responsible for inter-mobility-anchors ledgers to handle conflict issues between Mobility Anchors and Access Routers (MAARs). The region-wise blockchain controls MAARs and the user-wise blockchain contains users. When handover happens, MAARs send a handover request and broadcast it. If there is no conflict in the PoW-wise blockchain, the target MAAR conducts a handover. Then, the ME sends an attachment request to the target MAAR. After

checking the information on the user-wise blockchain, it sends an acknowledgment message to the ME and sends an updating message to the serving MAAR. All two MAARs update user-wise and region-wise ledgers. However, this framework only provides a mutual authentication method, session key establishment with privacy and anonymity remains unsolved.

Recently, Ma et al. [115] proposed a universal handover scheme. It enables an ME first to perform mutual authentication with a target AP. Then the target AP sends a notification message to a target MME. On receiving the message, the target MME sends a handover completed message to the serving MME. It uses a certificateless public key mechanism to overcome the key escrow problem. In this scheme, mutual authentication, confidentiality, integrity, FWS, nonrepudiation, user anonymity, and non-traceability can be guaranteed like normal public key-based schemes, but conditional privacy was not considered by the authors. The computation cost is $7T_h + 6T_m$ and the communication overhead is 3δ+γ.

Yang et al. [116] proposed a secure anonymous roaming scheme in which a visiting network can authenticate a user's home network with a token, which is generated by the home network, without knowing the real identity of the user. Its computation cost is $6T_h + T_{as}$ and communication overhead is 3δ+5η. Additionally, another two two-party authentication schemes were proposed based on IBS and group signature [117]. The scheme based on IBS can achieve basic security requirements such as mutual authentication and key establishment, but it cannot provide privacy protection to a user's identity because the identity of the user is transmitted in plaintext during handover. On the contrary, the scheme based on the group signature provides perfect privacy protection. The user can perform handover with pseudonyms and the serving network authenticates the user without knowing his/her real identity. Moreover, the home network can get the real identity of the user if necessary since it locally keeps the track key of the user. Taking user revocation into consideration, the authors modified the group signature signing procedure to fasten user revocation.

Xue et al. [118] proposed a handover authentication scheme for IoT in Space Information Networks (SIN). SIN enables every IoT object to be connected to the Internet no matter where it is. Traditional handover schemes are not suitable to be applied to SIN because of its high signaling overhead and high processing delay. Xue's scheme enables the handover authentication between an ME and two satellites without the involvement of any ground stations, which significantly decreases processing delay. To protect user identity privacy, the ground station distributes a set of irrelevant pseudonyms to the ME. When handover happens, the ME and the satellite could achieve mutual authentication by adopting PKC and generate a shared session key to protect the confidentiality and integrity of communications. FWS is also guaranteed since the session key is generated based on both the secret session key and a random value. Dependability was tested under an attack simulation. This scheme can achieve user anonymity and non-traceability by using a pseudonym mechanism. Its computation cost is $4T_h + 7T_m$.

All aforementioned schemes focus on a single ME handover.

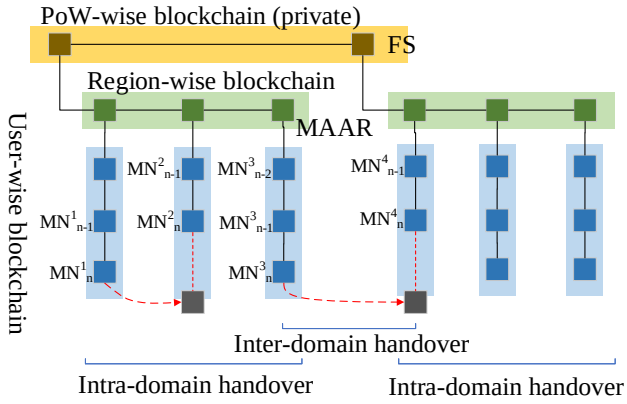


Fig. 13. Structure of blockchain-based DMM

Some researchers also notice that there is a handover scenario where many MEs move together so that it is possible to form a handover group to reduce handover communication costs. Fu et al. [119] proposed a group handover authentication scheme for handover in a WiMAX network. When the first ME of the group arrives in a target BS, the BS gets authentication information of all group members from a serving BS, so that when the rest of the group members come to the target BS, they can bypass the Extensible Authentication Protocol (EAP) and directly perform handover authentication, which distinctly improves handover efficiency. This scheme uses pseudonyms and a key hierarchy mechanism to guarantee mutual authentication, confidentiality, integrity, FWS, anonymity, and non-traceability. But BWS, dependability, and conditional privacy were not considered by the authors.

Cao et al. [120] proposed another uniform group handover authentication scheme. In this scheme, when the first group member performs handover, the handover required contexts of other members are transmitted during the handover phase of the first ME. Only mutual authentication, confidentiality, integrity, and FWS were considered in this work. BWS is not supported. Furthermore, Cao et al. [121] proposed a group handover authentication scheme that deploys multi-signature and AMAC to promote the efficiency of handover. Different from authenticating group members one by one in [120], all group members send handover requests via a group leader, the leader batches all requests and sends them to a target AP. Then, the target AP can authenticate all the group members at once. Later, the target AP computes session keys for every MEs. After receiving the response message from the target AP, every ME checks the validity of the target AP and computes a corresponding session key to build up a secure communication channel with the target AP. Compared to previous schemes, this scheme achieves better efficiency and can also protect the real identity of the ME from leakage. In addition, tracing the real identity of the ME is possible by some authorized party if necessary.

We summarize and compare the security performance of vertical handover schemes in Table V. We specify used security methods and indicate whether the proposed requirements are met or not considered in the schemes. Since BS, CN and other servers are entities with powerful computation and

TABLE V
COMPARISON OF HORIZONTAL HANDOVER SCHEMES

Scheme	MA	CI	FWS	BWS	AD	AI	NT	CP	Computation overhead	Communication overhead
[23]	√	√	×	√	×	√	×	×	$4T_h$	2η + 3δ + 5γ
[83]	√	√	×	×	×	×	×	×	$2T_h + T_m + 3T_e + 2T_s$	2δ+γ
[84]	√	√	√	√	√	√	√	×	$2T_h + 3T_m + 2T_s + T_p$	4δ+ϵ
[85]	√	√	√	√	√	√	√	×	$4T_h + T_m + 2T_e$	6δ+2γ+ϵ
[97]	×	√	√	√	√	√	√	×	$4T_h + 2T_m + T_p$	2δ
[90]	√	√	×	√	×	×	×	×	$4T_e + T_{as}$	3δ
[122]	√	√	√	√	√	√	√	×	$4T_h + 4T_m + T_p$	2δ
[123]	√	√	√	√	√	√	√	×	$4T_h + 4T_m + T_p$	2δ
[98]	√	√	√	√	√	√	√	×	$2T_h + 4T_m$	2δ
[104]	×	√	×	×	×	√	√	×	$4T_h + 5T_m$	2δ
[105]	√	√	√	√	√	√	√	×	$4T_h + 5T_m$	2δ
[106]	√	√	√	√	√	√	√	×	$4T_h + 5T_m$	2δ
[91]	√	√	√	√	√	×	×	×	$3T_h + 3T_m + T_{as}$	2δ
[124]	√	√	√	√	×	√	√	×	$3T_h + T_m + T_p$	2δ
[102]	√	√	√	√	×	√	√	√	$4T_h + 4T_m$	2δ
[103]	√	√	√	√	√	√	√	×	$2T_h + 5T_m$	2δ
[99]	√	√	√	√	√	√	√	√	$7T_h + 3T_m + 2T_e + T_{KDF}$	3δ
[109]	√	√	√	√	×	√	√	×	$2T_e + T_{ABS} + T_{as}$	3δ
[110]	√	√	√	√	√	√	√	×	$3T_h + 4T_m + 4T_e$	3δ+4γ+2η
[111]	√	√	√	√	√	×	×	×	$11T_h + 11T_m$	3δ+6γ+2η
[112]	√	√	√	√	√	√	√	×	$6T_h + 4T_m$	3δ
[115]	√	√	√	√	√	×	×	×	$7T_h + 6T_m$	3δ+ϵ
[116]	√	√	√	√	×	√	√	×	$6T_h + T_{as}$	3θ+5η
[118]	√	√	√	√	√	√	√	×	$4T_h + 7T_m$	-
[119]	√	√	×	√	×	√	√	×	$3T_h + 2T_m$	2nμ+ 2δ
[120]	√	√	×	√	×	√	√	×	$4T_h + 2T_m$	2nμ+ 3δ
[121]	√	√	×	√	√	√	√	×	$5T_e$	$(2n+1)\mu$ + 3δ
[121]	√	√	√	√	√	-	-	-	$T_h + T_3T_e + T_p$	$(2n)\mu$ + 2δ

MA: mutual authentication; CI: confidentiality and integrity; FWS: forward secrecy; BWS: backward secrecy; AD: availability and dependability; AI: anonymity and indistinguishability; NT: non-traceability; CP: conditional privacy;
T_m: computation cost of multiply operation; T_h: computation cost of hash point function; T_p: computation cost of bilinear pairing function; T_e: computation cost of modular exponentiation; T_{KDF}: computation cost of key derivation function; T_s: computation cost of symmetry encryption/decryption operation; T_{as}: computation cost of asymmetric encryption/decryption operation
δ: transmission time between ME and BS; ϵ: transmission time between BSs; η: transmission between MMEs; θ: transmission between ME and MME; γ: transmission between MME and BS; μ: transmission between MEs
- : this scheme does not consider in paper; ×: this scheme does not satisfy the requirement ; √: this scheme satisfies the requirement

communication capability, we only consider the computational overhead on ME which is equipped with restricted resources. As for communication overhead, it is evaluated in terms of all communication delay during handover process.

V. PRIVACY COUNTERMEASURES FOR 5G HANDOVER

Except for designing solutions to solve security issues in handover in 5G networks, some researchers focus on user privacy preservation issues in handover. Because various user information is selected and processed in 5G networks, users are keen to keep their private information secret when they enjoy the convenience of networking services. In the process of handover, there are two classes of user information involved mostly, which are user identity and location. According to this idea, we review the privacy solutions designed for handover in 5G networks in this section.

A. Identity Privacy Preservation

1) Pseudonym-based Methods: Nowadays, most handover schemes that provide identity privacy preservation apply pseudonyms instead of user real identities. Generally, in this kind of scheme, AS initially prepares a set of pseudonyms for an ME. If the authentication between an ME and a BS/AP is based on a digital signature algorithm, a corresponding private key should be generated and attached to each pseudonym. Thus, when handover occurs, the BS/AP only knows the pseudonym of the ME, which can preserve user identity privacy. However, if an ME uses one pseudonym unchanged or the unlinkability of the pseudonyms is weak, an adversary is able to trace the user according to the pseudonyms and link pseudonyms to the real identity of the user.

Many schemes [58], [59], [85], [86], [88], [90], [94], [96], [101]–[103], [105], [106], [116], [118], [120], [125] adopted pseudonym-based mechanism to achieve identity pri-

vacy preservation. In order to prevent adversaries from identity tracing, the ME changes its pseudonym every time when it performs handover. Unfortunately, user pseudonyms in [90], [94] are not changed periodically so that adversaries can trace MEs straightforward.

Another security intractable problem of the pseudonym-based method is that the generated pseudonyms should be stored in the AS, which will be a target of attackers, such as DoS/DDoS attacks, etc.

2) Signature-based Methods: AAnother classic method to preserve user identity privacy is applying cryptography, especially some digital signatures, e.g., group signature and proxy signature could achieve authentication with some special anonymous features [109], [112].

In [109], the authors designed a lightweight ABS-based handover scheme. On one hand, MEs authenticate APs based on a challenge-response pair, message, and normal signature, i.e., Elliptic Curve Digital Signature Algorithm. Only APs that have private keys can generate valid signatures on fresh challenges from MEs. On the other hand, APs authenticate MEs based on ABS. Only MEs that have the right attribute list can generate valid signatures. Since attribute information rather than identity-related parameters are transmitted through messages, it is impossible to extract ME's identity or link any messages to the same user.

Qiu et al. [112] adopted a proxy signature in handover authentication. Due to the verifiability and unforgeability of the proxy signature, this scheme can well implement mutual authentication. The legality of ME is guaranteed by proxy signature because only legal ME can represent the AS to generate a valid proxy signature. The drawback of the signature-based methods is heavy computation cost, which causes serious handover delay.

3) Hybrid Methods: Combining signature and pseudonym together can achieve identity privacy preservation with special characteristics and sound performance. A good example is the scheme proposed by He et al. [124]. In this scheme, the authors took advantage of IBS to achieve mutual authentication and used pseudonyms to prevent MitM attacks. MEs and BSs share a common parameter of their private key, they can achieve mutual authentication by computing a consistent authentication token. This authentication procedure only involves the temporary identities of MEs. So, the identities of MEs are well protected. But conditional privacy is not supported.

To fulfill the demands of conditional privacy, He et al. [107] proposed a group signature-based privacy-preserving handover scheme. Using the group signature, the AAA server can obtain the identities of users by following a group open function. Nevertheless, the normal group signature mechanism does not support dynamic user revocation. In order to repair this drawback of group signature, the authors applied Forward Secure Revocation (FSR) group signature [126] to provide conditional privacy and revocable anonymity.

To sum up, we draw Table VI to compare the privacy performance of most of schemes. We use $\surd$ and $\times$ to denote whether the scheme satisfy the requirement or not. Also, we specify their used mechanisms to achieve privacy preservation. Nearly all schemes can achieve user anonymity and most of them provide conditional privacy.

TABLE VI
ANALYSIS OF PRIVACY PRESERVATION PERFORMANCE

Scheme	Privacy	Mechanisms	AI	NT	CP
[127]	Location Privacy	Proxy Ring Signature	$\surd$	$\surd$	$\surd$
[128]		Group Signature	$\surd$	$\surd$	$\surd$
[129]		BLS Signature	$\surd$	$\surd$	$\times$
[58]	Identity Privacy	Pseudonym	$\surd$	$\surd$	$\times$
[59]		Pseudonym	$\surd$	$\surd$	$\surd$
[85]		Pseudonym	$\surd$	$\surd$	$\surd$
[88]		Pseudonym	$\surd$	$\times$	$\surd$
[90]		Pseudonym	$\surd$	$\surd$	$\surd$
[94]		Pseudonym	$\surd$	$\surd$	$\surd$
[96]		Pseudonym	$\surd$	$\surd$	$\surd$
[86]		Pseudonym	$\surd$	$\times$	$\times$
[101]		Pseudonym	$\surd$	$\times$	$\times$
[102]		Pseudonym	$\surd$	$\times$	$\times$
[103]		Pseudonym	$\surd$	$\surd$	$\surd$
[104]		Pseudonym	$\surd$	$\surd$	$\times$
[105]		Pseudonym	$\surd$	$\surd$	$\surd$
[106]		Pseudonym	$\surd$	$\surd$	$\surd$
[107]		Pseudonym	$\surd$	$\surd$	$\surd$
[116]		Pseudonym	$\surd$	$\surd$	$\surd$
[112]		Proxy Signature	$\surd$	$\surd$	$\surd$
[109]		ABS	$\surd$	$\surd$	$\surd$
[111]		Proxy Signature	$\surd$	$\times$	$\surd$
[119]		Group Signature	$\surd$	$\times$	$\surd$
[120]		Group Signature	$\surd$	$\surd$	$\surd$
[118]		IBS	$\surd$	$\surd$	$\times$
[121]		Aggregate Signature	$\surd$	$\surd$	$\surd$
[121]		Group Signature	$\surd$	$\times$	$\surd$
[118]		Signature	$\surd$	$\surd$	$\surd$
[130]		Group Signature	$\surd$	$\surd$	$\surd$

AI: anonymity and indistinguishability; NT: non-traceability; CP: conditional privacy;

B. Location Privacy Preservation

Location privacy preservation is another significant privacy issue in the 5G handover. The increasing concerns on location privacy protection from network users make the conflict between user and service provider more sharpened. Network operators or service providers expect to trace the moving trail of a user to predict the behavioral model, thus, to deliver advertisements or services precisely. However, users are eager to escape from massive annoying ads supported by user tracking. As far as right now, many pieces of research focus on location privacy preservation in 5G networks and creative applications [131]–[133], but a few works on location privacy preservation during handover [127]–[129]. So, we sum them up in Table VI.

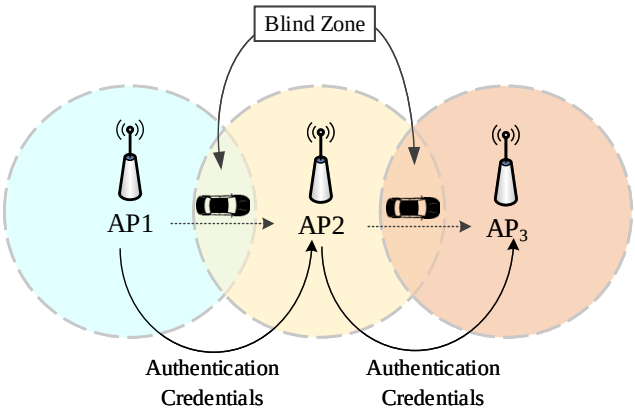


Fig. 14. The blind zone

In [127], Zhang et al. proposed an authentication scheme in vehicular networks. By using a blind signature which is constructed based on the Boneh–Lynn–Shacham (BLS) short signature [134], this scheme can provide good location privacy preservation and avoid being traced during handover. The blind signature can prevent the target AP from knowing the identities of MEs. When a vehicle first registers into a AAA server, it gains a credential for future handover authentication. A blind zone is defined in this paper as shown in Fig. 14. When a vehicle enters the range of the target AP, the serving AP is responsible for sending relevant authentication information to the target AP. Since the vehicle uses a pseudonym to request the target AP for authentication and the authentication credentials are blind to the target AP, it is hard for the target AP to identify the real identity of the vehicle. MEs and APs can achieve mutual authentication by using valid credentials that are confidential. When MEs and APs compute a session key, they both use new random values to ensure FWS. However, this scheme has a flaw that if there is only one vehicle performing handover authentication at a moment, the vehicle is still possible to be traced. And there is no formal proof of security and privacy or a test under multiple attacks, so availability and dependability were not considered. Conditional privacy was not supported, either. The computation overhead at the ME side is $T_h + 2T_m$ and the communication overhead is 3δ.

Jing et al. proposed a scheme [128] that combines proxy and ring signatures named proxy ring signature to protect the location privacy of MEs. In this scheme, an ME chooses two handover candidate target APs and represents the source AP to generate a ring signature for the target AP's neighboring APs. Based on the anonymity of candidate APs and ring signature, the source AP does not know which exactly is the target AP. Meanwhile, the target AP cannot get where the ME comes from. The ME and the target AP can authenticate each other based on the proxy signature. After mutual authentication, the ME and the target AP can negotiate a session key to protect message confidentiality and integrity. Compared to using an identity-based ring signature, this scheme achieves FWS. However, conditional privacy was not considered. The computation overhead at ME side is $6T_h + 11T_m$ and the communication overhead is 3δ.

Yu et al. presented a scheme [129] based on pseudonyms and group signature. They found that a single vehicle has many opportunities to encounter other vehicles, and the strength of privacy preservation mainly depends on the number of vehicles running within one cell at the same time. So, in the scheme, the vehicles communicate with RSUs based on a group. Every vehicle uses in-group identities to communicate within the group. Once a vehicle leaves the group, it uses its pseudonym to broadcast leaving messages. In most conditions, a vehicle exchanges information with RSUs by using group identity which can guarantee the privacy of the vehicle. Vehicles can prevent from being tracked by frequently changing their in-group pseudonyms. As for security requirements, authors only considered mutual authentication, confidentiality, and integrity. The computation overhead is high due to adopting the group signature. And the communication overhead is 5δ.

In some related work, e.g., [59], MEs are traceable because the AP/BS needs to track ME location to provide authentication parameters and other services.

VI. Open Research Issues and Future Directions

A. Open Issues

According to the above literature review with analysis and comparison, we found that the research on security and privacy preservation on handover in 5G is still far from impeccable. There currently exist several open security and privacy issues on 5G handover that should be solved before large-scale 5G network commercial deployment.

First, most of the research on handover security and privacy preservation focuses on handover within the same type of networks or between at most two kinds of networks. These schemes were designed for specific scenarios and use cases, which are not proper to be directly applied into 5G with high heterogeneity. The versatility of these schemes is limited because of their "ad hoc" features. Recently, some work [49], [50], [63] tries to construct a universal and scalable security framework to address handover security and privacy preservation among 5G HetNets, but suffers from conspicuous drawbacks, e.g., low efficiency, and security and privacy deficiency. Therefore, building a universal, scalable and highly efficient handover framework in 5G networks with security and privacy preservation is imperative.

Second, almost all related works addressed security and privacy issues in handover based in a centralized way, which means the handover procedure and security and privacy management are controlled by a centralized network server, e.g., AHM [55], [59] and AS [83]–[85] in various networks. This system structure makes the centralized server under a high risk of various attacks, especially DoS/DDoS attacks. So far, there exist some researches [62], [63], [114] on using decentralization methods, e.g., blockchain technology, to construct a decentralized security handover protocol. For example, in [62], [63] blockchain was introduced as a distributed ledger to store essential parameters used for handover. The blockchain takes the place of a central server for mobility and security management, which protects the system from attacks. In [114] blockchain was adopted for distributed mobility management.

However, some inherent shortcomings of blockchain, e.g., latency of block generation and data disclosure of transactions, makes using blockchain full of challenges. Therefore, in 5G networks, using a decentralization technology, such as blockchain, to protect handover security and privacy against severe attacks is a promising but challenging work.

Third, there is always a tradeoff among efficiency, security and privacy preservation. As we can see from the Table IV, V , a scheme is designed with a high level of security and privacy preservation normally at the expense of high computation cost and long handover delay, especially at ME, which is against the performance requirements of 5G networks, i.e., low latency [135]. So, it is significant to analyze the relation between security/privacy and handover performance to build a formal quantitative model for handover security and privacy preservation.

Fourth, how to ensure FWS and BWS in group handover is still an open issue. From Table IV and V, we can see that FWS and BWS are security properties weakly supported in handover research so far. Group handover, which can improve the performance of handover in 5G network, is attracting special attention in handover research [71]–[73], [120], [121], [130]. But it is urgent to work out an effective and efficient FWS and BWS protection solution for group handover before its wide adoption.

Fifth, conditional privacy is a specific privacy requirement that has not been seriously considered. Generally, privacy preservation and privacy leakage are in conflict. However, in some use cases in 5G, vehicle rescue, for instance, is inescapable for users to disclose some private information, e.g., location information, for safety assurance. However, it is still an open issue to provide self-adaptive or configurable privacy protection, i.e., conditional privacy, in 5G handover, especially for some special 5G communication scenarios.

B. Future Research Directions

According to the above listed open issues, we further propose several interesting research directions that we think worth special efforts.

1) Universal Handover Architecture for 5G Network with Security and Privacy-preservation: A universal handover architecture with security and privacy preservation is essentially necessary for designing and building a secure and seamless mobile roaming system for 5G networks. The universal handover architecture should address all handover scenarios occurring in the heterogeneous networking environments in 5G. Moreover, according to different security and privacy levels required by specific handover scenarios, the security and privacy requirements can be specified and fulfilled under the universal architecture in an adaptive and configurable way. Such a study is still missed and should be performed in the future.

2) Security and Privacy-preservation Handover and Blockchain: Blockchain was proposed as a decentralization method to solve many of the problems caused by centralization [136]. Some features of blockchain technology, e.g., preventing data tampering and anonymous can power security and privacy preservation for handover in the 5G network. Although some researchers [62], [63], [114] have adopted blockchain to rebuild or improve handover structure, there are still many issues that should be addressed. For instance, handover security context information can be recorded on the blockchain to reduce the communication overhead between the AAA servers of different networks. However, a significant parameter of blockchain is the time cost of block generation, which indirectly influences the latency of handover. On the other hand, privacy protection for mobile users should be ensured when we apply blockchain into 5G handover. Decentralized management on handover security and privacy is a very interesting research topic with high potential in this field.

3) Security and Privacy-preservation Handover and SDN/AI: In 5G networks, SDN and Artificial Intelligence (AI) are two promising technologies that can be adopted to improve network performance. As we can see from our review, some researchers [55]–[59] have leveraged SDN to control the handover from a high level to reduce handover delay. Besides, AI can also be used in the handover procedure in order to protect the security and privacy of 5G networks and reduce latency at the same time. For instance, using AI such as neural networks for security and privacy in the previous generation network, e.g., LTE may not be applicable because of the limitation of the computation power of network nodes. In 5G networks, more powerful servers deployed in the cloud and edge facilities boost the application of AI extensively. A precise prediction of ME's trajectory or handover intention could greatly increase the overall efficiency of the handover and its security. However, the application of AI on security in 5G networks is still in its infancy, e.g., how to enhance privacy when applying AI for handover is worth special investigation. At the same time, additional security and privacy issues in handover in 5G networks could be addressed with the assistance of SDN, AI, and other emerging technologies, e.g., intrusion detection and risk analysis.

4) Cross-layer Design to Improve Handover Security and Performance: Cross-layer design for security and privacy is useful in 5G networking. SDN could control an overall network from a high level in 5G networks, which makes it possible to design security and privacy by fusing cross-layer SCI. In our review, most handover authentication schemes focus only on the security of the network layer. Information about the physical layer and the data link layer can be taken into consideration in order to offer handover with high performance. For example, related work [55], [56] leveraged physical layer information as secure SCI to authenticate handover MEs, which can reduce computation cost and handover delay comparing with cryptography-based authentication methods. We estimate that SCI-based handover with privacy preservation is an interesting research topic worth further investigation.

5) Security and Privacy-preservation of Group-based Handover for Massive Users: Because of the involvement of IoT and VANET in 5G, it is usually the case that massive users request to handover and authenticate concurrently. If BS or CN handles these handover and authentication requests separately,

the computation and communication cost will increase with the number of users, which will greatly affect handover latency. Thus, it is necessary to handle massive handover requests using a secure and high-efficient method. Group-based handover has been paid attention recently. However, it is still far from enough to meet the security and privacy requirements proposed in Section III. Additional research should be performed on this aspect.

6) Security and Privacy-preserving Handover in eMBB, URLLC and mMTC: eMBB strengthens what we have today with improved network performance and seamless user services. This scenario requires higher traffic capacity, higher data rate than 4G. URLLC focuses on reliability, latency, and availability. This scenario requires higher reliability, lower latency than 4G, which can be used in V2X, remote medical surgery, etc. mMTC is a scenario that there are a large number of devices connecting to the access network. In our review, most handover authentication schemes are designed for the eMBB scenario. There are few schemes [71], [72], [120], [121] designed for URLLC and mMTC that are worthy of future research in the 5G network.

VII. Conclusion

In this paper, we first specified a detailed list of security and privacy requirements for the purpose of resisting potential threats and attacks in handovers of 5G HetNets. We then surveyed the state-of-the-art schemes by employing the proposed requirements as performance evaluation criteria to evaluate and compare them. We also analyzed the efficiency of existing works in terms of computational cost at mobile devices and handover protocol communication overheads. The analysis and comparison results indicate that existing works are far from comprehensively satisfying all security and privacy requirements. Moreover, it is defective for the trade-off between handover performance and the strength of security and privacy preservation. Extensive literature review allows us to indicate a number of open research issues in this field. At last, we pointed out a number of attractive future research directions to motivate special efforts to achieve secure and privacy-preserving handover in 5G HetNets.

Appendix

Acronym	Definition
5G	Next Generation Mobile Cellular Communication and Networking System
3GPP	Third Generation Partnership Project
5GS	5G System
AAA	Authentication, Authorization, and Accounting
ABC	Always Best Connected
ABS	Attribute-Based Signature
AHM	Authentication Handover Module
AI	Artificial Intelligence
AMAC	Aggregate Message Authentication Code
AMF	Access and Mobility Management Function
AN	Access Network
AP	Access Point
ASN-GW	Access Service Network Gateway
AUSF	Authentication Server Function
BLS	Boneh–Lynn–Shacham
BS	Base Station
BWS	Backward Secrecy
CN	Core Network
CSI	Channel State Information
D2D	Device-to-Device
DDoS	Distributed Denial of Service
DFF	Data Forward Function
DHKE	Diffie-Hellman Key Exchange
DNS	Domain Name System
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
eMBB	Enhanced Mobile Broadband
eNB	e-Node Base Station
EPC	Evolved Packet Core
EPS-AKA	Extensible Authentication Protocol-Authentication and Key Agreement
E-UTRA	Evolved Universal Terrestrial Radio Access
FSR	Forward Secure Revocation
FWS	Forward Secrecy
gNB	g-Node Base Station
GPS	Global Positioning System
GUTI	Globally Unique Temporary Identity
HeNB	Home Evolved Node Base Station
HetNet	Heterogeneous Network
HMAC	Hash-based Message Authentication Code
HSS	Home Subscriber Server
IBC	Identity-Based Cryptography
IBS	Identity-Based Signature
IEEE	Institute of Electrical and Electronics Engineers
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
ITU	International Telecommunication Union
KDF	Key Derivation Function
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAAR	Mobility Anchors and Access Router
MAC	Message Authentication Code
MBS	Macro Base Station
ME	Mobile Equipment
MICS	Media Independent Command Service
MIES	Media Independent Event Service
MIIS	Media Independent Information Service
MIPv6	Mobile IPv6
MIS	Media Independent Services
MitM	Man-in-the-Middle
MME	Mobility Management Entity
mMTC	Massive Machine-Type Communication
MSC	Mobile Service Centre
N3IWF	Non-3GPP Interworking Function
NFV	Network Function Virtualization
NG-RAN	Next Generation Radio Access Network

Acronym	Definition
NR	New Radio
NTRU	Number Theory Research Unit
OSI	Open System Interconnection
PDN	Packet Data Network
PGW	Packet Data Network Gateway
PKC	Public Key Cryptography
PKG	Private Key Generator
PKM	Privacy Key Management
PoW	Proof of Work
PPM	Privacy Protection Module
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RF	Radio Frequency
RSS	Radio Signal Strength
RSU	Road Side Unit
SCI	Secure Context Information
SCT	Security Context Transfer
SDN	Software-Defined Network
SGW	Serving Gateway
SIN	Space Information Network
SMF	Session Management Function
SN	Serving Network
TNGF	Trusted Non-3GPP Gateway Function
UAV	Unmanned Aerial Vehicle
UPF	User Plane Function
URLLC	Ultra-reliable and Low Latency Communication
UTMS	Universal Mobile Telecommunications System
V2X	Vehicle-to-Everything
VANET	Vehicular Ad-hoc Network
WAP	Wireless Application Protocol
WIF	Wi-Fi Interworking Function
WiMAX	World Interoperability for Microwave Access
WLAN	Wireless Local Access Network

ACKNOWLEDGMENT

The work is supported in part by the National Natural Science Foundation of China under Grants 62072351, 62002273, and 61802293, the Project funded by China Postdoctoral Science Foundation under grant 2018M633461 and 2019M663631, the National Postdoctoral Program for Innovative Talents under grant BX20180238, the Academy of Finland under Grants 308087 and 335262, the Shaanxi Innovation Team project under grant 2018TD-007, the Science and Technology Planning Project of Shaanxi Province under grant 2020JQ-308 and the 111 project under grant B16037, as well as Huawei Technologies Group Co., Ltd.

REFERENCES

[1] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, 2014.

[2] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surv. Tutor.*, vol. 16, no. 4, pp. 1801–1819, 2014.

[3] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things*, vol. 3, no. 5, pp. 637–646, 2016.

[4] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5g: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, 2017.

[5] V. Sharma, I. You, and N. Guizani, "Security of 5G-V2X: Technologies, standardization and research directions," *IEEE Netw.*, 2020.

[6] S. Chandrashekar, A. Maeder, C. Sartori, T. Höhne, B. Vejlgaard, and D. Chandramouli, "5G multi-RAT multi-connectivity architecture," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, 2016, pp. 180–186.

[7] A. Talukdar, M. Cudak, and A. Ghosh, "Handoff rates for millimeterwave 5G systems," in *Proc. 79th IEEE Veh. Technol. Conf. (VTC)*, 2014, pp. 1–5.

[8] R. S. Sandhu and P. Samarati, "Access control: Principle and practice," *IEEE Commun. Mag.*, vol. 32, no. 9, pp. 40–48, 1994.

[9] M. Chlosta, D. Rupprecht, T. Holz, and C. Pöpper, "LTE security disabled: Misconfiguration in commercial networks," in *Proc. 12th ACM Conf. Secur. Priv. Wireless Mobile Netw. (WiSec)*, 2019, pp. 261–266.

[10] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, 2018.

[11] Y.-T. Chang, J.-W. Ding, C.-H. Ke, and I.-Y. Chen, "A survey of handoff schemes for vehicular ad-hoc networks," in *Proc. 6th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, 2010, pp. 1228–1231.

[12] S. Midya, K. Majumder, A. Roy, and D. De, "Vertical handoff mechanisms in VANET: A survey," in *Proc. of the 2nd Int. Conf. Inf. Commun. Technol. Competitive Strategies (ICoICT)*, 2016, pp. 1–6.

[13] Y. Zhou and B. Ai, "Handover schemes and algorithms of high-speed mobile environment: A survey," *Comput. Commun.*, vol. 47, pp. 1–15, 2014.

[14] S. Ferretti, V. Ghini, and F. Panzieri, "A survey on handover management in mobility architectures," *Comput. Netw.*, vol. 94, pp. 390–413, 2016.

[15] M. Khan and K. Han, "A survey of context aware vertical handover management schemes in heterogeneous wirel. netw." *Wirel. Pers. Commun.*, vol. 85, no. 4, pp. 2273–2293, 2015.

[16] J. Márquez-Barja, C. T. Calafate, J.-C. Cano, and P. Manzoni, "An overview of vertical handover techniques: Algorithms, protocols and tools," *Comput. Commun.*, vol. 34, no. 8, pp. 985–997, 2011.

[17] S. Pack, J. Choi, T. Kwon, and Y. Choi, "Fast-handoff support in IEEE 802.11 wirel. netw." *IEEE Commun. Surv. Tutor.*, vol. 9, no. 1, pp. 2–12, 2007.

[18] K. Pahlavan, P. Krishnamurthy, A. Hatami, M. Ylianttila, J.-P. Makela, R. Pichna, and J. Vallstron, "Handoff in hybrid mobile data networks," *IEEE Pers. Commun.*, vol. 7, no. 2, pp. 34–47, 2000.

[19] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; System Architecture for the 5G System (Rel 16)," 3GPP TS, Tech. Rep. 23.501 V16.0.2, Apr 2019.

[20] M. Tayyab, X. Gelabert, and R. Jäntti, "A survey on handover management: From LTE to NR," *IEEE Access*, vol. 7, pp. 118 907–118 930, 2019.

[21] A. Ahmed, L. M. Boulahia, and D. Gaiti, "Enabling vertical handover decisions in heterogeneous wirel. netw.: A state-of-the-art and a classification," *IEEE Commun. Surv. Tutor.*, vol. 16, no. 2, pp. 776–811, 2013.

[22] I. of Electrical and E. Engineers, "IEEE Standard for Local and Metropolitan Area Networks–Part 21: Media Independent Services Framework," IEEE Standard, Tech. Rep., Apr 2017.

[23] 3rd Generation Partnership Project, "Technical Specification group Services and System Aspects; Security Architecture and Procedures for 5G System (Rel 15)," 3GPP TS, Tech. Rep. 33.501 V15.4.0, Mar 2019.

[24] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3gpp 5g networks," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 1, pp. 170–195, 2019.

[25] M. Khan, P. Ginzboorg, K. Järvinen, and V. Niemi, "Defeating the downgrade attack on identity privacy in 5G," in *Int. Conf. Res. Secur. Standardisation*, 2018, pp. 95–119.

[26] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information," in *Proc. 26th Ann. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2019, pp. 24–27.

[27] Y. Park and T. Park, "A survey of security threats on 4G networks," in *Proc. IEEE Global Commun. Conf. Workshops (GLOBECOM)*. IEEE, 2007, pp. 1–6.

[28] T. Wu and G. Gong, "The weakness of integrity protection for LTE," in *Proc. 6th ACM Conf. Secur. Priv. Wireless Mobile Netw. (WiSec)*, 2013, pp. 79–88.

[29] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Service Requirements for the Evolved Packet System (EPS) (Rel 16)," 3GPP TS, Tech. Rep. 22.278 V16.1.0, Sept 2018.

[30] W.-F. Alliance, "Wi-Fi Alliance® introduces Wi-Fi 6," Wi-Fi Alliance, Tech. Rep., October 2018.

[31] W. FORUM, "Network Architecture Wi-Fi®-WiMAX® Interworking," WiMAX FORUM, Tech. Rep., Nov 2010.

[32] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai, "IEEE 802.11 wireless local area networks," *IEEE Commun. Mag.*, vol. 35, no. 9, pp. 116–126, 1997.

[33] M. Vanhoef and F. Piessens, "Release the Kraken: new KRACKs in the 802.11 Standard," in *Proc. 25th ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2018, pp. 299–314.

[34] C. Eklund, R. B. Marks, K. L. Stanwood, and S. Wang, "Ieee Standard 802.16: A technical overview of the WirelessMAN/sup TM/air interface for broadband wireless access," *IEEE Commun. Mag.*, vol. 40, no. 6, pp. 98–107, 2002.

[35] V. K. Jatav and V. Singh, "Collaborative attack model at physical layer of mobile WiMAX network," in *Proc. 6th Int. Conf. Comput. Intell. Commun. Netw. (CICN)*, 2014, pp. 787–792.

[36] H. C. Van Tilborg and S. Jajodia, *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.

[37] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 3, pp. 2027–2051, 2016.

[38] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-Middle attack to the HTTPS protocol," *IEEE Secur. Priv.*, vol. 7, no. 1, pp. 78–81, 2009.

[39] P. Schneider and G. Horn, "Towards 5G security," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 1165–1170.

[40] L. De Alfaro, *Formal verification of probabilistic systems*. Citeseer, 1997, no. 1601.

[41] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 2, pp. 1773–1828, 2018.

[42] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wirel. netw.: Theories, technologies, and challenges," *IEEE Commun. Surv. Tutor.*, vol. 19, no. 1, pp. 347–376, 2016.

[43] H. M. Furqan, M. S. J. Solaija, and H. Arslan, "Intelligent physical layer security approach for V2X communication," *arXiv preprint arXiv:1905.05075*, 2019.

[44] 3rd Generation Partnership Project, "Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description (Rel 15)," 3GPP TS, Tech. Rep. 38.300 V15.7.0, Sept 2019.

[45] 3rd Generation Partnership Project, "Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN) (Rel 15)," 3GPP TS, Tech. Rep. 36.300 V15.5.0, Mar 2019.

[46] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Location Services (LCS) Architecture for 3GPP System-Wireless Local Area Network (WLAN) Interworking (Rel 7)," 3GPP TS, Tech. Rep. 23.837 V1.0.0, Sept 2006.

[47] 3rd Generation Partnership Project, "Technical specification group services and system aspects; architecture enhancements for non-3gpp accesses (Rel 15)," 3GPP TS, Tech. Rep. 38.300, Sept 2018, v15.3.0.

[48] W. J. Song, J.-M. Chung, D. Lee, C. Lim, S. Choi, and T. Yeoum, "Improvements to seamless vertical handover between mobile WiMAX and 3GPP UTRAN through the evolved packet core," *IEEE Commun. Mag.*, vol. 47, no. 4, pp. 66–73, 2009.

[49] J. Cao, M. Ma, and H. Li, "Unified handover authentication between heterogeneous access systems in LTE networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2012, pp. 5308–5313.

[50] J. Cao, M. Ma, and H. Li, "An uniform handover authentication between E-UTRAN and non-3GPP access networks," *IEEE Trans. Wirel. Commun.*, vol. 11, no. 10, pp. 3644–3650, 2012.

[51] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. 21st Ann. Int. Cryptology Conf. (CRYPTO)*, 2001, pp. 213–229.

[52] 3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; 3GPP System to Wireless Local Area Network (WLAN) Interworking; WLAN User Equipment (WLAN UE) to Network Protocols (Rel 12)," 3GPP TS, Tech. Rep. 24.234 V12.2.0, Mar 2015.

[53] A. A. Al Shidhani and V. C. M. Leung, "Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers," *IEEE Trans. Dependable Secur. Comput.*, vol. 8, no. 5, pp. 699–713, 2011.

[54] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, 2014.

[55] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 28–35, 2015.

[56] 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)*, 2016, pp. 1–6.

[57] A. Ozhelvaci and M. Ma, "Secure and efficient vertical handover authentication for 5G HetNets," in *Proc. IEEE Int. Conf. Inf. Commun. Signal Process. (ICICSP)*, 2018, pp. 27–32.

[58] M. J. Alam and M. Ma, "DC and CoMP authentication in LTE-Advanced 5G HetNet," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2017, pp. 1–6.

[59] J. Cao, M. Ma, Y. Fu, H. Li, and Y. Zhang, "CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets," *IEEE Trans. Dependable Secur. Comput.*, 2019.

[60] A. S. Tanenbaum, S. J. Mullender, and R. Van Renesse, "Using sparse capabilities in a distributed operating system," in *Proc. 6th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 1986, pp. 558–563.

[61] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018.

[62] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks," *IEEE Trans. Netw. Sci. Eng.*, 2019.

[63] Y. Zhang, R. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5G HetNets," *IEEE Trans. Dependable Secur. Comput.*, 2019.

[64] H. Krawczyk and T. Rabin, "Chameleon signatures," in *Proc. 7th Netwo. Distrib. Syst. Secur. Symp. (NDSS)*, 2000, pp. 143–154.

[65] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchain-assisted secure device authentication for cross-domain industrial iot," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 942–954, 2020.

[66] S. Guo, F. Wang, N. Zhang, F. Qi, and X. Qiu, "Master-slave chain based trusted cross-domain authentication mechanism in iot," *J. Netw. Comput. Appl.*, vol. 172, p. 102812, 2020.

[67] M. Wang and Z. Yan, "Security in D2D communications: A review," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, 2015, pp. 1199–1204.

[68] M. Wang, Z. Yan, and V. Niemi, "UAKA-D2D: Universal authentication and key agreement protocol in D2D communications," *Mobile Netw. Appl.*, vol. 22, no. 3, pp. 510–525, 2017.

[69] M. Wang and Z. Yan, "Privacy-preserving authentication and key agreement protocols for D2D group communications," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3637–3647, 2018.

[70] A. Kumar and H. Om, "Handover authentication scheme for device-to-device outband communication in 5G-WLAN next generation heterogeneous networks," *Arab. J. Sci. Eng.*, vol. 43, no. 12, pp. 7961–7977, 2018.

[71] J. Cao, M. Ma, and H. Li, "A group-based authentication and key agreement for MTC in LTE networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2012, pp. 1017–1022.

[72] J. Cao, M. Ma, H. Li, Y. Fu, and X. Liu, "EGHR: Efficient group-based handover authentication protocols for mMTC in 5G wirel. netw." *J. Netw. Comput. Appl.*, vol. 102, pp. 1–16, 2018.

[73] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2014, pp. 1011–1016.

[74] L. Eastwood, S. Migaldi, Q. Xie, and V. Gupta, "Mobility using IEEE 802.21 in a heterogeneous IEEE 802.16/802.11-based, IMT-Advanced (4G) network," *IEEE Commun. Lett.*, vol. 15, no. 2, pp. 26–34, 2008.

[75] H. Sun, S. Chen, Y. Chen, H. Chung, and I. Lin, "Secure and efficient handover schemes for heterogeneous networks," in *Proc. IEEE Asia-Pacific Services Comput. Conf. (APSCC)*, 2008, pp. 205–210.

[76] Z. Yan, H. Zhou, H. Zhang, H. Luo, and S. Zhang, "A dual threshold-based fast vertical handover scheme with authentication support," in *Proc. 5th Int. Conf. Mobile Technol. Appl. Syst.*, 2008, pp. 1–4.

[77] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Trans. Wirel. Commun.*, vol. 4, no. 2, pp. 734–742, 2005.

[78] L. Hou and K. X. Miao, "A pre-authentication architecture in WiFi&WiMAX integrated system," in *Proc. 4th EAI Int. Conf. Commun. Netw. (ChinaCom)*, 2009, pp. 1–5.

[79] K.-L. Huang, K.-H. Chi, J.-T. Wang, and C.-C. Tseng, "A fast authentication scheme for WiMAX–WLAN vertical handover," *Wirel. Pers. Commun.*, vol. 71, no. 1, pp. 555–575, 2013.

[80] X. Yang, X. Huang, and J. K. Liu, "Efficient handover authentication with user anonymity and untraceability for mobile cloud computing," *Futur. Gener. Comp. Syst.*, vol. 62, pp. 190–195, 2016.

[81] A. Fu, G. Zhang, Z. Zhu, and Y. Zhang, "Fast and secure handover authentication scheme based on ticket for WiMAX and WiFi heterogeneous networks," *Wirel. Pers. Commun.*, vol. 79, no. 2, pp. 1277–1299, 2014.

[82] C. Wang, Y. Zhang, X. Chen, K. Liang, and Z. Wang, "Sdn-based handover authentication scheme for mobile edge computing in cyber-physical systems," *IEEE Internet Things*, vol. 6, no. 5, pp. 8692–8701, 2019.

[83] A. Kumar and H. Om, "A secure seamless handover authentication technique for wireless LAN," in *Proc. Int. Conf. Inf. Technol. (ICIT)*. IEEE, 2015, pp. 43–47.

[84] C. Xu, X. Huang, M. Ma, and H. Bao, "An anonymous handover authentication scheme based on LTE-A for vehicular networks," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018.

[85] V. Sharma, I. You, F.-Y. Leu, and M. Atiquzzaman, "Secure and efficient protocol for fast handover in 5G mobile Xhaul networks," *J. Netw. Comput. Appl.*, vol. 102, pp. 38–57, 2018.

[86] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Trans. Wirel. Commun.*, vol. 11, no. 1, pp. 48–53, 2011.

[87] A. De La Oliva, X. C. Pérez, A. Azcorra, A. Di Giglio, F. Cavaliere, D. Tiegelbekkers, J. Lessmann, T. Haustein, A. Mourad, and P. Iovanna, "Xhaul: toward an integrated fronthaul/backhaul architecture in 5G networks," *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 32–40, 2015.

[88] R. Chen and D. Peng, "A novel NTRU-based handover authentication scheme for wirel. netw." *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 586–589, 2017.

[89] Q. Wang, C. Cheng, and L. Zuo, "Analysis and improvement of a NTRU-based handover authentication scheme," *IEEE Commun. Lett.*, vol. 23, no. 10, pp. 1692–1695, 2019.

[90] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing," *IEEE Commun. Lett.*, vol. 14, no. 1, pp. 54–56, 2009.

[91] S. Gupta, B. L. Parne, and N. S. Chaudhari, "PSEH: A provably secure and efficient handover AKA protocol in LTE/LTE-A network," *Peer Peer Netw. Appl.*, vol. 12, no. 4, pp. 989–1011, 2019.

[92] A. Fu, Y. Zhang, Z. Zhu, Q. Jing, and J. Feng, "An efficient handover authentication scheme with privacy preservation for IEEE 802.16 m network," *Comput. Secur.*, vol. 31, no. 6, pp. 741–749, 2012.

[93] A. Fu, Y. Zhang, Z. Zhu, and X. Liu, "A fast handover authentication mechanism based on ticket for IEEE 802.16 m," *IEEE Commun. Lett.*, vol. 14, no. 12, pp. 1134–1136, 2010.

[94] R. A. Abouhogail and M. S. Gadelrab, "A new secure and privacy preserved protocol for IEEE 802.11s networks," *Comput. Secur.*, vol. 77, pp. 745–755, 2018.

[95] C. M. Moreira, G. Kaddoum, and E. Bou-Harb, "Cross-layer authentication protocol design for ultra-dense 5G HetNets," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2018, pp. 1–7.

[96] C.-I. Fan, J.-J. Huang, M.-Z. Zhong, R.-H. Hsu, W.-T. Chen, and J. Lee, "ReHand: Secure region-based fast handover with user anonymity for small cell networks in mobile communications," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 927–942, 2019.

[97] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," *IEEE Trans. Wirel. Commun.*, vol. 10, no. 2, pp. 431–436, 2010.

[98] S. H. Islam and M. K. Khan, "Provably secure and pairing-free identity-based handover authentication protocol for wireless mobile networks," *Int. J. Commun. Syst.*, vol. 29, no. 17, pp. 2442–2456, 2016.

[99] H. J. Jo, J. H. Paik, and D. H. Lee, "Efficient privacy-preserving authentication in wireless mobile networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 7, pp. 1469–1481, 2013.

[100] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn. (EUROCRYPT)*, 2001, pp. 453–474.

[101] V. Odelu, S. Zeadally, A. K. Das, M. Wazid, and D. He, "A secure enhanced privacy-preserving key agreement protocol for wireless mobile networks," *Telecommun. Syst.*, vol. 69, no. 4, pp. 431–445, 2018.

[102] X. Yang, Y. Zhang, J. K. Liu, and Y. Zeng, "A trust and privacy preserving handover authentication protocol for wirel. netw." in *Proc. IEEE Trustcom/BigDataSE/ISPA*, 2016, pp. 138–143.

[103] J. Mo, Z. Hu, and Y. Lin, "An efficient privacy-preserving handover authentication scheme for mobile wireless network," in *Proc. Int. Conf. Cloud Comput. Secur. (ICCS)*, 2018, pp. 490–505.

[104] G. Li, Q. Jiang, F. Wei, and C. Ma, "A new privacy-aware handover authentication scheme for wirel. netw." *Wirel. Pers. Commun.*, vol. 80, no. 2, pp. 581–589, 2015.

[105] S. A. Chaudhry, M. S. Farash, H. Naqvi, S. H. Islam, and T. Shon, "A robust and efficient privacy aware handover authentication scheme for wirel. netw." *Wirel. Pers. Commun.*, vol. 93, no. 2, pp. 311–335, 2017.

[106] Y. Xie, L. Wu, N. Kumar, and J. Shen, "Analysis and improvement of a privacy-aware handover authentication scheme for wireless network," *Wirel. Pers. Commun.*, vol. 93, no. 2, pp. 523–541, 2017.

[107] D. He, J. Bu, S. Chan, and C. Chen, "Handauth: Efficient handover authentication with conditional privacy for wirel. netw." *IEEE Trans. Comput.*, vol. 62, no. 3, pp. 616–622, 2012.

[108] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in *Proc. 5th ACM Symp. Inf. Comput. Commun. Secur. (AsiaCCS)*, 2010, pp. 60–69.

[109] Y. Zeng, H. Guang, and G. Li, "Attribute-based anonymous handover authentication protocol for wirel. netw." *Secur. Commun. Netw.*, vol. 2018, 2018.

[110] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A simple and robust handover authentication between HeNB and eNB in LTE networks," *Comput. Netw.*, vol. 56, no. 8, pp. 2119–2131, 2012.

[111] S. Gupta, B. L. Parne, and N. S. Chaudhari, "A proxy signature based efficient and robust handover AKA protocol for LTE/LTE-A networks," *Wirel. Pers. Commun.*, vol. 103, no. 3, pp. 2317–2352, 2018.

[112] Y. Qiu, M. Ma, and X. Wang, "A proxy signature-based handover authentication scheme for LTE wirel. netw." *J. Netw. Comput. Appl.*, vol. 83, pp. 63–71, 2017.

[113] R. Ahmad, E. A. Sundararajan, N. E. Othman, and M. Ismail, "Efficient handover in LTE-A by using mobility pattern history and user trajectory prediction," *Arab. J. Sci. Eng.*, vol. 43, no. 6, pp. 2995–3009, 2018.

[114] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and energy-efficient handover in fog networks using blockchain-based DMM," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 22–31, 2018.

[115] R. Ma, J. Cao, D. Feng, H. Li, Y. Zhang, and X. Lv, "PPSHA: Privacy preserving secure handover authentication scheme for all application scenarios in LTE-A networks," *Ad Hoc Netw.*, vol. 87, pp. 49–60, 2019.

[116] G. Yang, D. S. Wong, and X. Deng, "Anonymous and authenticated key exchange for roaming networks," *IEEE Trans. Wirel. Commun.*, vol. 6, no. 9, pp. 3461–3472, 2007.

[117] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Trans. Wirel. Commun.*, vol. 9, no. 1, pp. 168–174, 2010.

[118] K. Xue, W. Meng, S. Li, D. S. Wei, H. Zhou, and N. Yu, "A secure and efficient access and handover authentication protocol for Internet of Things in space information networks," *IEEE Internet Things*, vol. 6, no. 3, pp. 5485–5499, 2019.

[119] A. Fu, S. Lan, B. Huang, Z. Zhu, and Y. Zhang, "A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks," *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1744–1747, 2012.

[120] J. Cao, H. Li, and M. Ma, "GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2015, pp. 3020–3025.

[121] J. Cao, H. Li, M. Ma, and F. Li, "UPPGHA: Uniform privacy preservation group handover authentication mechanism for mMTC in LTE-A networks," *Secur. Commun. Netw.*, vol. 2018, 2018.

[122] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "Secure handover authentication protocol based on bilinear pairings," *Wirel. Pers. Commun.*, vol. 73, no. 3, pp. 1037–1047, 2013.

[123] W. Wang and L. Hu, "A secure and efficient handover authentication protocol for wirel. netw." *Sensors*, vol. 14, no. 7, pp. 11 379–11 394, 2014.

[124] D. He, S. Chan, and M. Guizani, "Handover authentication for mobile networks: security and efficiency aspects," *IEEE Netw.*, vol. 29, no. 3, pp. 96–103, 2015.

[125] A. Fu, N. Qin, Y. Wang, Q. Li, and G. Zhang, "Nframe: A privacy-preserving with non-frameability handover authentication protocol

based on (t, n) secret sharing for LTE/LTE-A networks," *Wirel. Netw.*, vol. 23, no. 7, pp. 2165–2176, 2017.

[126] H. Jin, D. S. Wong, and Y. Xu, "Efficient group signature with forward secure revocation," in *Proc. Int. Conf. Secur. Technol. (SecTech)*, 2009, pp. 124–131.

[127] C. Zhang, R. Lu, P.-H. Ho, and A. Chen, "A location privacy preserving authentication scheme in vehicular networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2008, pp. 2543–2548.

[128] Q. Jing, Y. Zhang, X. Liu, and A. Fu, "An efficient handover authentication scheme with location privacy preserving for EAP-based wirel. netw." in *Proc. IEEE Int. Conf. Commun. (ICC)*. IEEE, 2012, pp. 857–862.

[129] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 1, pp. 93–105, 2015.

[130] C. Xu, X. Huang, M. Ma, and H. Bao, "GAKAV: Group authentication and key agreement for LTE/LTE-A vehicular networks," in *Proc. 19th IEEE Int. Conf. High Perform. Comput. Commun.; the 15th IEEE Int. Conf. Smart City; the 3rd IEEE Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, 2017, pp. 412–418.

[131] E. Catania and A. La Corte, "Location privacy in virtual cell-equipped ultra-dense networks," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 2018, pp. 1–4.

[132] M. M. Badr, W. Al Amiri, M. M. Fouda, M. M. Mahmoud, A. J. Aljohani, and W. Alasmary, "Smart parking system with privacy preservation and reputation management using blockchain," *IEEE Access*, vol. 8, pp. 150 823–150 843, 2020.

[133] D. Liao, G. Sun, M. Zhang, V. Chang, and H. Li, "Towards location and trajectory privacy preservation in 5g vehicular social network," in *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, vol. 2. IEEE, 2017, pp. 63–69.

[134] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in *Proc. Int. Conf. Theory Appl. Cryptology Inf. Secur. (ASIACRYPT)*, 2001, pp. 514–532.

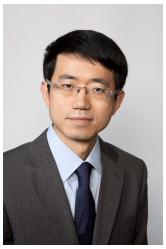
[135] 3rd Generation Partnership Project, "Technical Specification Group Radio Access Network; Study on Scenarios and Requirements for Next Generation Access Technologies (Rel 15)," 3GPP TR, Tech. Rep. 38.913 V15.0.0, Jun 2018.

[136] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 858–880, 2018.

Dongsheng Zhao received bachelor's degree in software engineering from Liaoning University. He is currently working for his master's degree in Cyberspace Security at Xidian University, Xi'an, China. His current research interests include security and privacy in the next generation of mobile communication networks and wireless systems.

Zheng Yan is currently a professor at the Xidian University, China and a visiting professor and Finnish academy research fellow at the Aalto University, Finland. She received the Doctor of Science in Technology from the Helsinki University of Technology, Finland. Before joining academia in 2011, she was a senior researcher at the Nokia Research Center, Helsinki, Finland, since 2000. Her research interests are in trust, security, privacy, and security-related data analytics. She is an associate editor of IEEE Internet of Things Journal, Information Fusion, Information Sciences, IEEE Access, and JNCA. She served as a general chair or program chair for a number of international conferences including IEEE TrustCom 2015. She is a founding steering committee co-chair of IEEE Blockchain conference. She received several awards, including the 2017 Best Journal Paper Award issued by IEEE Communication Society Technical Committee on Big Data and the Outstanding Associate Editor of 2017/2018 for IEEE Access.

Mingjun Wang received the Ph.D. degree in information security from Xidian University, Xi'an, China, in 2017. He is currently a postdoctoral fellow in the State Key Laboratory on Integrated Services Networks at Xidian University. His current research interests include security, privacy and trust management in the next generation mobile communication networks and wireless systems.



Peng Zhang received Doctor degree in computer communication from Beijing University of Posts and Telecommunications in 1999. His current research interests include security and privacy in the next generation of mobile communication networks and wireless systems.

Bin Song received his BS, MS, and PhD in communication and information systems from Xidian University, Xi'an, China in 1996, 1999, and 2002, respectively. He is currently a professor at the Xidian University, Xi'an, China. He has authored over 60 journal papers or conference papers and 30 patents. His research interests are in distributed video coding, compressed sensing-based video coding, content-based image recognition and machine learning, deep reinforcement learning, Internet of Things, big data.