Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes

Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke

Abstract—This paper presents a comprehensive survey of existing authentication and privacy-preserving schemes for 4G and 5G cellular networks. We start by providing an overview of existing surveys that deal with 4G and 5G communications, applications, standardization, and security. Then, we give a classification of threat models in 4G and 5G cellular networks in four categories, including, attacks against privacy, attacks against integrity, attacks against availability, and attacks against authentication. We also provide a classification of countermeasures into three types of categories, including, cryptography methods, humans factors, and intrusion detection methods. The countermeasures and informal and formal security analysis techniques used by the authentication and privacy preserving schemes are summarized in form of tables. Based on the categorization of the authentication and privacy models, we classify these schemes in seven types, including, handover authentication with privacy, mutual authentication with privacy, RFID authentication with privacy, three-factor authentication with privacy, and three-factor authentication with privacy. In addition, we provide a taxonomy and comparison of authentication and privacy-preserving schemes for 4G and 5G cellular networks in form of tables. Based on the current survey, several recommendations for further research are discussed at the end of this paper.

Index Terms—Security, Privacy, Authentication, 5G mobile communication, Cryptography.

I. INTRODUCTION

The fifth-generation mobile networks (5G) will soon supersede 4G in most countries of the world. The next generation wireless network technology is being developed based on recent advances in wireless and networking technologies such as software-defined networking and virtualization. Compared to 4G technologies, 5G is characterized by still higher bit rates with more than 10 gigabits per second as well as by more capacity and very low latency, which is a major asset for the billions of connected objects in the context of Internet of Things (IoT). In the IoT era, 5G will enable a fully mobile and connected society, via creating various new network services such as mobile fog computing, car-to-car communications, smart grid, smart parking, named data networking, blockchain based services, unmanned aerial vehicle (UAV) etc. as shown in Fig. 1. Therefore, telecommunications companies believe that the commercialization of 5G will begin in 2020. In Tab. 1 we list some of the leading projects for 5G cellular networks by various telecommunications companies.

In a 5G environment, the blend different wireless technologies and service providers that share an IP-based core network, will offer the possibility to the mobile devices of switching between providers and technologies, for maintaining a high level

![Image](312x220 to 563x395)

TABLE I

| Time  | Company                        | Program                               |
|-------|--------------------------------|---------------------------------------|
| 2014  | NTT DOCOMO and SK Telecom      | Ericsson 5G delivers 3 Gbps speed     |
| 2015  | Ericsson and SoftBank          | Ericsson and SoftBank completed basic 5G trials on both 15 GHz and 4 GHz spectra |
| 2016  | Ericsson and Telefónica        | Ericsson and Telefónica focused on the Advanced 5G Network Infrastructure for Future Internet Public-Private Partnership (5G PPP) and European Technology Platform for Communications Networks and Services (ETP Network 2020) |
| 2016  | Huawei and Vodafone Group plc | Vodafone Group with Huawei have recently completed a 5G field test in Newbury (UK) that demonstrates the capabilities of a trial system operating at 70 GHz |
| 2017  | Huawei and China Mobile Ltd    | Huawei and China Mobile showcased the 5G 3 GHz prototype and Ka-Band millimeter wave prototype |
| 2017  | Verizon Communications Inc.    | Verizon will begin pilot testing 5G “pre-commercial services” in U.S. cities in the first half of 2017, including Atlanta, Dallas, Denver, Houston, Miami, Seattle, and Washington |
| 2017  | AT&T Inc.                      | AT&T launches Nationwide LTE-M Network for Internet of Things |
| 2017  | Nippon Telegraph and Telephone Corporation (NTT) | Toyota and NTT collaborative to promote 5G standardization for autonomous vehicles |
| 2017  | Huawei and Deutsche Telekom    | Huawei and Deutsche Telekom demonstrate the all Cloud 5G network slicing |

Fig. 1. What will 5G enable?
TABLE II
DEFINITIONS OF ACRONYMS AND NOTATIONS

| Acronym | Definition                                      | Acronym | Definition                                      |
|---------|------------------------------------------------|---------|------------------------------------------------|
| 3GPP    | Third Generation Partnership Project           | IRS     | Intrusion Response System                       |
| 4G      | Fourth-generation mobile network               | LTE     | Long-Term Evolution                             |
| 5G      | Fifth-generation mobile network                | LTE-A   | Long-Term Evolution Advanced                    |
| AES     | Advanced Encryption Standard                   | M2M     | Machine-to-Machine                              |
| AIM     | Advanced Identity Management                   | MAC     | Message Authentication Code                     |
| AKA     | Authentication and Key Agreement               | MD5     | Message Digest 5                                |
| AMAC    | Aggregate Message Authentication Codes         | MIMO    | Multiple-Input Multiple-Output                  |
| AP      | Access point                                   | MITM    | Man-in-the-middle                               |
| BRPCA   | Bayesian Robust Principal Component Analysis   | MME     | Mobility Management Entity                      |
| BS      | Base station                                   | MSS     | Managed security services                       |
| BTS     | Base Transceiver Station                       | MTC     | Machine Type Communication                      |
| CNN     | Controller Area Network                        | NB      | Narrowband                                      |
| CRC     | Cyclic Redundancy Check                        | NFV     | Network Function Virtualization                  |
| CXTPT   | Context transfer protocol                      | P2P     | Peer-to-Peer                                    |
| D2D     | Device-to-Device communication                 | PIN     | Personal identification number                   |
| DNN     | Deep Neural Network                            | PKI     | Public key infrastructure                       |
| DoS     | Denial of Service                              | PT      | Pseudo Trust                                    |
| DSS     | Digital signature standard                     | RAN     | Radio Access Network                            |
| EAP     | Extensible Authentication Protocol             | RF      | Radio Frequency                                 |
| ECC     | Error Correction Codes                         | RFC     | Requests For Comments                           |
| eNB     | eNodeB                                         | RFID    | Radio frequency identification                   |
| FBS     | False Base Station                             | RNN     | Random Neural Network                           |
| FIFO    | First In First Out                             | RNTI    | Radio Network Temporary Identities              |
| GBS-AKA | Group-Based Secure Authentication and Key Agreement | SDN | Software Defined Networking                      |
| HeNB    | Home eNodeB                                     | SHA     | Secure Hash Algorithm                           |
| HMAC    | Keyed-Hash Message Authentication Code         | SIP     | Session Initiation Protocol                     |
| HSS     | Home Service Server                            | TLS     | Transport Layer Security                        |
| HTTP    | Hypertext Transfer Protocol                    | TPM     | Trusted Platform Module                         |
| IDS     | Intrusion Detection system                     | UAA     | Unmanned aerial vehicle                         |
| IEEE    | Institute of Electrical and Electronics Engineers | UE | User Equipment                                  |
| IMSI    | International Mobile Subscriber Identity       | UHF     | UltraHigh Frequency                             |
| IoT     | Internet of Things                             | UMTS    | Universal Mobile Telecommunications System       |

of Quality of Service (QoS). Fast vertical handover and the general openness of the network make the devices susceptible to several vulnerabilities like access control, communication security, data confidentiality, availability and privacy. Furthermore, since the 5G environment is IP-based, it will suffer from all the vulnerabilities that are to IP-specific. Based on these findings, it is obvious that guaranteeing a high level of security and privacy will be one of important aspects for the successful deployment of 5G networks [8].

As mobile devices will be connected to the network all the time, through the vertical handover, they will obtain a notion of social nodes. Such nodes can more easily be tracked down and are more vulnerable in several types of attacks, like impersonation, eavesdropping, man-in-the-middle, denial-of-service, replay and repudiation attack [9]. Maintaining a high level of QoS in terms of delay, when huge volume of data is transferred inside a 5G network, while keeping on the same time high security and privacy level, is critical in order to prevent malicious files from penetrating the system and propagating fast among mobile devices. Thus communications that satisfy zero latency requirements are cumbersome once combined with secure and privacy-preserving 5G networks [10].

For the process of conducting the literature review, we follow the same process conducted by our previous work in [9]. Specifically, the identification of literature for analysis in this paper was based on a keyword search, namely, "authentication and privacy-preserving scheme", "authentication and privacy-preserving protocol", "authentication and privacy-preserving system", and "authentication and privacy-preserving framework". Searching for these keywords in academic databases such as SCOPUS, Web of Science, IEEE Xplore Digital Library, and ACM Digital Library, an initial set of relevant sources were located. Firstly, only proposed authentication and privacy-preserving schemes for 4G and 5G cellular networks were collected. Secondly, each collected source was evaluated against the following criteria: 1) reputation, 2) relevance, 3) originality, 4) date of publication (between 2005 and 2017), and 5) most influential papers in the field. The final pool of papers consists of the most important papers in the field of 4G and 5G cellular networks that focus on the authentication and privacy-preserving as their objective. Our search started
The main contributions of this paper are:

- We discuss the existing surveys for 4G and 5G cellular networks that deal with communications, applications, standardization, and security.
- We provide a classification for the attacks in cellular networks in four categories, including, attacks against privacy, attacks against integrity, attacks against availability, and attacks against authentication.
- We provide a classification for countermeasures used by the authentication and privacy preserving schemes for 4G and 5G cellular networks into three types of categories, including, cryptography methods, humans factors, and intrusion detection methods.
- We present the informal and formal security analysis techniques used by the authentication and privacy preserving schemes for 4G and 5G cellular networks.
- We provide a categorization of authentication and privacy preserving schemes for 4G and 5G cellular networks.
- We provide a classification for authentication and privacy preserving schemes for 4G and 5G cellular networks in seven types, including, handover authentication with privacy, mutual authentication with privacy, RFID authentication with privacy, deniable authentication with privacy, authentication with mutual anonymity, authentication and key agreement with privacy, and three-factor authentication with privacy.
- We outline six recommendations for further research, including, 1) privacy preservation for Fog paradigm-based 5G radio access network, 2) authentication for 5G small cell-based smart grids, 3) privacy preservation for SDN/NFV-based architecture in 5G scenarios, 4) dataset for intrusion detection in 5G scenarios, 5) privacy preserving schemes for UAV systems in 5G heterogeneous communication environment, and 6) authentication for 5G small cell-based vehicular crowdsensing.

The remainder of this paper is organized as follows. Section II presents the existing surveys for 4G and 5G cellular networks that deal with communications, applications, standardization, and security. In Section III we provide a classification for the threat models and countermeasures. Section IV presents various the informal and formal security analysis techniques used by the authentication and privacy preserving schemes for 4G and 5G cellular networks. In Section V we present a side-by-side comparison in a tabular form for the current state-of-the-art of authentication and privacy preserving schemes for 4G and 5G cellular networks. Then, we discuss open issues and recommendations for further research in Section VI. Finally, we draw our conclusions in Section VII. Table II lists the acronyms and notations used in the paper.

II. EXISTING SURVEYS FOR 4G AND 5G CELLULAR NETWORKS

There are around fifty survey articles published in the recent years that deal with 4G and 5G communications, applications, standardization and security. These survey articles are categorized as shown in tables III and IV. From these survey articles only seven of them deal with security and privacy issues for 3G, 4G and 5G cellular networks and none of the previous works covers the authentication and privacy preserving issues of 4G and 5G networks. This work is the first on the literature that thoroughly covers authentication and privacy preservation threat models, countermeasures and schemes that we recently proposed from the research community.

For these fifty survey articles that were retrieved from SCOPUS and Web of Science and were published from 2007 to 2017 we performed a categorization which is presented in table III. Based on this categorization it is obvious that except from three big categories of articles, one dealing with scheduling and interference mitigation [11], [12], [13], [14], [15], [8], the other with D2D Communication [16], [17], [18], [19], [20], [21] and the third with security and privacy issues [22], [23], [24], [25], [8], [26], [27], all areas of research that are somehow related to 3G, 4G and 5G networks were surveyed and presented in previous surveys from at least one review article. As the technology progress and the networks evolve from 3G to 4G, 5G and even 6G [28], the number of articles that survey 4G and 5G networks increases from only one that was published back in 2007, to over twenty articles published in 2016. This increase on the number reveals an increase on the importance that researchers from around the world give on the new technology and the issues that arise regarding standardization [29], [30], [31], mobile internet applications [32], resource and mobility management [33], [34], energy [35], MIMO techniques [34], [20], [36], social perspectives [37] and so on (See Table III for detailed categorization).

Among the aforementioned surveys, the security and privacy issues that are related to the 4G and 5G networks were thoroughly covered and analyzed in previous works [22], [23], [24], [25], [8], [26], [27]. As it is shown in Tab. IV authentication and privacy preservation was only covered partially from Cao et al. [24] while the rest of the articles did not cover this major security aspect. In this article we survey authentication and privacy preserving protocols for 4G/5G networks. Based on this thorough analysis open issues and future directions are identified, that combine both innovative research and novel implementations, along with application of properly adapted existing solutions from other fields. We believe that this study will help researchers focus on the important aspects of authentication and privacy preservation issues in the 4G and 5G area and will guide them towards their future research.

III. THREAT MODELS AND COUNTERMEASURES

A. Threat models

In this subsection, we discuss the threat models in 4G and 5G Cellular Networks. We found thirty-five attacks, which are analyzed and prevented by authentication and privacy preserving schemes for 4G and 5G Cellular Networks. The classification of threat models in cellular networks frequently mentioned in literature is done using different criteria such as passive or active, internal or external etc. In our survey article, we classify the attacks in cellular networks in four categories as shown in Fig. 2 including, 1) attacks against privacy, 2)
TABLE III
AREAS OF RESEARCH OF EACH SURVEY ARTICLE FOR 4G AND 5G CELLULAR NETWORKS

| Ref. | SIM | SP | HD | VN | GCN | STD | MIA | RC | RDIM | D2D | DO | BM | SDN | US | ENE | BN | DNMA | MIMO | Soc | CC | mmWave | Archi |
|------|-----|----|----|----|-----|-----|-----|----|------|-----|----|----|-----|----|-----|----|------|------|-----|-----|--------|-------|
| [22] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [38] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [47] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [11] |    |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [12] |    |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [13] |    |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [14] |    |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [15] |    |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [32] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [42] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [43] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [44] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [29] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [30] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [31] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [33] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [34] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [20] |    |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [49] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [50] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [51] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [52] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [53] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [54] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [55] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [56] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |
| [57] | √   |    |  |    |     |     |     |  |      |  |  |    |    |    |  |    |    |     |     |     |        |       |

Fig. 2. Classification of attacks in 4G and 5G Cellular Networks

attacks against integrity, 3) attacks against availability, and 4) attacks against authentication. Note that our classification is based on the behavior of the attack in 4G and 5G cellular networks.

1) Attacks against privacy: We classify fourteen attacks in this category, namely, eavesdropping attack, parallel session attack, replay attack, Man-In-The-Middle (MITM) attack, impersonation attack, collaborated attack, tracing attack, spoofing attack, privacy violation, adaptive chosen ciphertext attack, chosen-plaintext attack, stalking attack, masquerade attack, and disclosure attack. The most serious attack among them is the MITM attack. According to Conti et al. [61], the MITM attack in cellular networks is based on False Base Station (FBS) attack, when malicious third party masquerades its Base Transceiver Station (BTS) as a real network’s BTS. Using a temporary confidential channel, Chen et al. [62] proposed an idea that only requires minimum number of human interaction for detecting and avoiding the MITM attack in cellular networks. Mayrhofer et al. [63] proposed a unified cryptographic authentication protocol framework to use with arbitrary auxiliary channels in order to detect the MITM attack
TABLE IV
YEAR OF PUBLICATION

| Year | Ref. |
|------|------|
| 2007 | [29] |
| 2010 | [30] |
| 2011 | [31] |
| 2012 | [32] |
| 2013 | [33] |
| 2014 | [34] |
| 2015 | [35] |
| 2016 | [36] |
| 2017 | [37] |

TABLE V
COMPARISON OF RELATED SURVEYS IN THE LITERATURE (SURVEY ON SECURITY AND PRIVACY FOR 4G AND 5G CELLULAR NETWORKS)
√: indicates fully supported; X: indicates not supported; 0: indicates partially supported.

| Ref. | SG | 4G | 5G | Author. | Privacy-preserving | Comments |
|------|----|----|----|--------|-------------------|----------|
| Pak, Y. and Pak, T. (2007) [29] | y | X | X | X | Presented some security threats on 4G networks. |
| Aish et al. (2010) [30] | y | X | 0 | X | Reviewed the X.805 standard for the AKA protocol. |
| Soldhpf et al. (2008) [31] | y | X | X | X | Surveyed the security advances for MAC layer in 4G technologies LTE and WiMAX. |
| Biken and Silemas (2013) [32] | 0 | y | X | X | Presented the cryptographic algorithms for LTE. |
| Cao et al. (2014) [33] | X | y | 0 | X | Presented the security archectures and mechanisms specified by the 3GPP standard. |
| Lichtman et al. (2016) [34] | X | y | X | X | Surveyed the jamming and spoofing mitigation techniques for LTE. |
| Panwar et al. (2016) [35] | X | X | y | X | Presented the challenges in security and privacy in 5G networks. |
| Our Work | 0 | y | y | y | y | Surveyed the authentication and privacy-preserving schemes for 4G and 5G Cellular Networks. |

in cellular networks. Based on the combination of learning parity with noise, circulant matrix, and multivariate quadratic, Li et al. [54] introduced an entity authentication protocol, which is proved that it is secure against all probabilistic polynomial-time adversaries under MITM attack model. However, note that the MITM attack is a particular case of a replay attack. By support mutual authentication, Chen et al. [65] proposed the improved smart-card-based password authentication and key agreement scheme that can easily detect a replay attack by checking the timestamp. The question we ask here is: Does detecting the replay attack is sufficient to detect the MITM attack? The privacy-preserving authentication scheme proposed recently by Waddad et al. [66] can answer this question where he can prove that the idea of checking the timestamp to detecting the MITM attack is not sufficient, but it is necessary to use the private keys that are not known to the attackers. Yao et al. [67] proposed a group-based secure authentication scheme, named, GBS-AKA, which he can detect the MITM attack using the session keys and timestamp during the authentication procedure. Through the MITM attack, the attacker can launch the other attacks of this category such as eavesdropping attacks to intercept keys and messages by unintended receivers.

2) Attacks against integrity: We classify six attacks in this category, namely, spam attack, message blocking, cloning attack, message modification attack, message insertion attack, and tampering attack. Note that the Spam attack can be classified in the category of attacks against availability. An attack against integrity is based on the modification of a data exchanged between the 5G access points and the mobile users. However, the authentication and privacy preserving schemes for 4G and 5G cellular networks use mostly the hash functions for assuring integrity of transmitted data. The SHA-1 and MD5 algorithms are frequently used as hash functions, which can easily detect the attacks against integrity by verifying an incorrect hash value.

3) Attacks against availability: We classify six attacks in this category, namely, First In First Out (FIFO) attack, redirection attack, physical attack, skimming attack, and free-riding attack. The goal of an attack against availability is to make a service as unavailable, e.g., the data routing service. By gathering entering time and exiting time intervals, the FIFO attack can be launched by a strong adversary. Gao et al. [68] discuss the FIFO attack and propose a trajectory mix-zones graph model. The redirection attack is easily possible when an adversary gets the correct user entity information by increase its signal strength to redirect or by impersonating a base station in the 4G and 5G cellular networks. To protect the network from redirection attack, Saxena et al. [69] and Li et al. [70] proposed the same idea that uses a MAC to maintain the integrity of tracking area identity, while Yao et al. [62] uses the local area identifier embedded with MAC. Therefore, the free-riding attack can cause a serious threat and reduces the system availability of D2D communication in the 4G and 5G cellular networks. By keeping a record of the current status of the user equipment and realize reception non-repudiation by key hint transmission, the proposed protocol by Zhang et al. [71] can detect the free-riding attack.

4) Attacks against authentication: We classify ten attacks in this category, namely, password reuse attack, password stealing attack, dictionary attack, brute force attack, desynchronization attack, forgery attack, leak of verifier attack, partial-message collision attack, and stolen smart card attack. The goal of an attack against authentication is to disrupt the client-to-server authentication and the server-to-client authentication. The password reuse attack and password stealing attack disrupt the password-based authentication schemes, which the attacker pretends to be legitimate user and attempts to login on to the server by guessing different words as password from a dictionary. The stolen smart card attack and off-line guessing attack disrupt the smart-card-based remote user password authentication schemes, which if a user’s smart card is stolen, the attacker can extract the stored information without knowing any passwords.

B. Countermeasures

In this subsection, we discuss the countermeasures used by the authentication and privacy preserving schemes for 4G and 5G cellular networks. Tab. V presents all the countermeasures used by the authentication and privacy preserving schemes for 4G and 5G cellular networks. These countermeasures can be classified into three types of categories, including, cryptography methods, humans factors, and intrusion detection methods, as presented in Fig. 9.

1) Cryptography methods: Cryptographic methods are the most used by the authentication and privacy preserving
schemes for 4G and 5G cellular networks, which can be classified into three types of categories, including, public-key cryptography, symmetric-key cryptography, and unkeyed cryptography.

The schemes \cite{74, 115, 116, 97, 98} use the public key infrastructure (PKI) \cite{125} in order to identify the genuine access point (AP) or base station (BS). Both schemes \cite{109, 118} use the Paillier cryptosystem \cite{126}, which is based on three algorithms, namely, generation of keys, encryption, and decryption. The generation of keys is based on two large, independent and random prime numbers: \( p \) and \( q \). Let \( m \) be a message to be encrypted, the encryption algorithm computes \( c = (1 + N)^m \cdot r^N \mod N^2 \) where \( 0 \leq m < N \), \( r \) is a random integer \( 0 < r < N \), and the public key \( N = p \cdot q \). To find the clear text \( m \), the decryption algorithm computes \( m = (\frac{c \cdot r^{-N} \mod N^2}{N})^\frac{1}{N} \). The scheme \cite{80} uses both Blind signature \cite{127} and Rabin’s public key cryptosystem \cite{128}. The blind signature involves two entities, namely: 1) a signer and 2) a signature requester, in which the content of a message is disguised from its signature. Rabin’s public key cryptosystem is characterized by its asymmetric computational cost and requires a large amount of computation effort. The Group signatures with verifier local revocation \cite{129} is used by the scheme \cite{101} in order to provide conditional anonymity. Furthermore, Boneh et al. \cite{130} proposed short group signatures due to group signatures based on Strong-RSA are too long for some applications. The digital signature standard (DSS) \cite{131} is used by the PT scheme \cite{75} in order to provide confidentiality and integrity to data exchanges after authentication as well as to simplify the key exchange protocol.

The symmetric encryption is used by four schemes, namely, \cite{62, 96, 69, 78}, in order to provide user anonymity. Specifically, Chen et al. \cite{62} use the Advanced Encryption Standard (AES) as the symmetric data encryption algorithm for mobile devices. Based on the idea that symmetric key algorithms faster than asymmetric key algorithms, Saxena et al. \cite{69} proposed an authentication protocol that is entirely based on the symmetric key cryptosystem for an IoT-enabled LTE network. Therefore, the question we ask here is: can the strategy of only using symmetric key techniques to achieve user anonymity is reliable? The improved privacy-preserving authentication scheme proposed recently by Wang et al. in \cite{96} can answer this question where he can prove that the strategy of only using symmetric-key techniques to achieve user anonymity is intrinsically infeasible. In addition, Lu et al. \cite{78} use semantic secure symmetric encryption in order to preserve the location privacy.

Hash functions are used almost in all the authentication and privacy preserving schemes in order to provide data integrity for the encrypted messages. We note that these schemes use

\( \text{TABLE VI} \)

| Countermeasures | Authentication and privacy preserving schemes for 4G and 5G cellular networks |
|-----------------|--------------------------------------------------------------------------------|
| Secure hash function | 61, 62, 75, 96, 77, 78, 79, 80, 81, 109, 118 |
| Index pseudonym | 63, 83 |
| UMTS-AKA mechanism | 63, 73 |
| Message Authentication Code (MAC) | 63, 73, 74, 75, 76, 77 |
| Electronic Product Code (EPC) | 63, 77 |
| Intrusion Detection Message Exchange Format (IDMEF) and Intrusion Detection Exchange Protocol (IDAP) | 63, 77 |
| Digital certificate and signature | 64, 78 |
| Public Key Infrastructure (PKI) | 64, 78, 74, 115, 116, 97, 98 |
| Advanced Encryption Standard (AES) | 64 |
| APIS protocol and Digital signature standard (DSS) | 64 |
| Password | 64 |
| Transport Layer Security (TLS) | 64 |
| Trusted Platform Module (TPM) | 64 |
| Keyed-Hash Message Authentication Code (HMAC) | 64 |
| Password Number Generator (PNG) | 64 |
| Elliptic Curve Cryptography (ECC) | 64 |
| Homomorphic Encryption | 64 |
| Paillier cryptosystem | 64 |
| Forward security technique | 64 |
| Error Correction Codes (ECC) | 64 |
| Anonymous ticket | 64 |
| Biometrics | 65 |
| Blind signature and Rabin’s public key cryptosystem | 65 |
| Elliptic Curve Diffie-Hellman protocol (ECDH) | 65 |
| Bootstrapping Pseudonym (BPP), Home Fast Pseudonym (HFP), and Visited Fast Pseudonym (VFP) | 65 |
| Advanced Identity Management (AIM) | 65 |
| Physically Unclonable Function (PUF) | 65 |
| Linear Feedback Shift Register (LFSR) | 65 |
| Personal Identification Number (PIN) | 65 |
| Semantic secure symmetric encryption | 65 |
| Smart cards | 65 |
| Proxy-signature scheme | 65 |
| Network domain security (NDS)/IP | 65 |
| Trusted Node Authentication (TNA) | 65 |
| Advertisement protocol | 65 |
| Parallel-Location Switching (PLS) | 65 |
| Symmetric encryption | 65 |
| Hierarchical identity-based signature | 65 |
| Mobile vector network protocol | 65 |
| Hamming weight of vector | 65 |
| International Mobile Subscriber Identity (IMSI) | 65 |
| Radio Network Temporary Identity (RNTI) | 65 |
| Source centroid | 65 |
| Constraint revocation | 65 |
| Group signature with verifier local revocation | 65 |
| Group-based access authentication | 65 |
| Aggregate Message Authentication Codes (AMAC) | 65 |
| Designated verifier proxy signature (DVPSS) | 65 |

![Fig. 3. Classification of countermeasures used by the authentication and privacy preserving schemes for 4G and 5G cellular networks](image-url)
three popular methods, namely, the Message Authentication Code (MAC) [132], the Keyed-Hash Message Authentication Code (HMAC) [133], and the Aggregate Message Authentication Codes (AMAC) [134].

2) Humans factors: The humans’ factors-based countermeasures are proposed to ensure authentication. The research community has proposed three factors, namely, 1) what you know (e.g., passwords, personal identification number (PIN)), 2) what you have (e.g., token, smart cards, passcodes, RFID), and 3) who are you (e.g., biometrics like fingerprints and iris scan, signature or voice). The methods based on what you know (e.g., passwords) might be divulged or forgotten, and the methods based on what you have (e.g., smart cards) might be shared, lost, or stolen. In contrast, the methods based on who are you (e.g., fingerprints or iris scans) have no such drawbacks. Note that these three factors can be used together or alone.

3) Intrusion detection methods: Intrusion Detection systems (IDS) are the second stage of defense. In situations when an intruder has already managed to bypass all existing countermeasures and has already taken control of a legal entity of the network, an IDS must spot misbehavior fast enough in order to be efficient. There are a lot of new methods that have been proposed during the previous years for detecting intruders in 4G and 5G networks. In [135] authors propose a novel IDS based on Bayesian Robust Principal Component Analysis (BRPCA). Based on the observation that network traffic variables are non-stationary and exhibit 24 h periodicity, the proposed anomaly detection approach represents network traffic as a sequence of traffic variable vectors. The method was evaluated against two synthetic datasets that represent a DOS and femtocell-based attack respectively. Trying to combat a similar attack, a virtual jamming attack, authors in [136] proposed a novel hybrid NIDS based on Dempster-Shafer (DS) Theory of Evidence. The performance of the method, that combines a signature-based and an anomaly based IDS, was evaluated on an experimental IEEE 802.11 network testbed.

In [137] authors propose an adaptive intrusion detection system that uses a hidden Markov Model for detecting intrusions on small cell access point in a 5G wireless communication network. Authors focused on the bandwidth spoofing attack. During this attack, the attacker tries to acquire the bandwidth that is going to be assigned from the BS to the SCA, thus blocking its communication. The method is proved to be capable of detecting and removing the intruder which is executing a bandwidth spoofing attack on the SCA (small cell access) in a 5G WCN. In [138] authors proposed an RNN-based (Random Neural Network) approach for detecting of large scale Internet anomalies based on the analysis of captured network data. Authors mostly interested in investigating application specific anomalies and conducted the evaluation of their proposed method on semi-synthetic data, derived from real traffic traces. Relying on fuzzy logic principles, authors propose in [139] a novel Intrusion Detection System. The proposed IDS uses an Adaptive Neuro-Fuzzy Inference System and is created for 5G Wireless Communication Network (WCN). The proposed IDS is a fuzzy inference system integrated with neural networks taking advantage of the benefits of both systems [140]. Authors evaluated their method against DOS attacks, like the previous methods in [135], [136], [137], [138] using the KDD cup 99 dataset. In a scenario where malicious data packets coming from a 3G, 4G or Wi-Fi network that the vehicle use in order to communicate with surrounding vehicles, manage to enter into the in-vehicle CAN bus is investigated in [141]. Authors in [141] propose IDS that uses a deep neural network (DNN) in order to detect an attack after it has entered the CAN (controller area network). The proposed IDS provides a real-time response to the attack with good accuracy.

Dealing with attacks in LTE networks, authors in [142] propose a random packet inspection scheme. The proposed scheme has an inspection rate that can be dynamically adjusted based on the perceived intrusion period of the session. This way the IDS performs a deep packet inspection, which is necessary in order to reveal the presence of signatures or malicious codes, while on the same time being an efficient and quick way of inspection. This method provides an effective tool for balancing induced inspection cost with detection latency in
LTE core networks. In [143] authors cope with intrusions in wireless sensor networks. The authors having identified the key aspects of such a network, e.g. Highly dynamic network conditions, limited bandwidth and transmission of sensitive data, propose TermID and test its efficiency using the Aegean wireless intrusion dataset version 2 [144]. The proposed method achieves both low network footprint and user privacy. Taking in mind privacy along with security, authors in [114] propose a location aware mobile IDS system. The proposed mIPS is a location-aware intrusion detection and prevention system with enhanced privacy handling.

Intelligence of intruders affects the effectiveness of IDS. This situation is investigated in [145] where authors implemented two AI-enabled intrusion algorithms and evaluated the impact of intruder’s intelligence on the intrusion detection capability of a WSN under various circumstances. Moving one step further, authors in [146] review the area of Intrusion Response Systems (IRS). An IRS taking in mind the current situation on the network may choose the optimal response option. Based on the research of the authors, IRS cannot handle false alarms that are produced from the IDS and in the future a false alarm handler is an important component that must be integrated in every IDS/IRS.

IV. INFORMAL AND FORMAL SECURITY ANALYSIS TECHNIQUES

Researchers in the Security and Privacy fields use the formal and informal techniques to analyze, prove, and verify the reliability of their proposed security scheme, and especially for schemes that are based on cryptography as a tool for achieving the authentication and privacy. Therefore, we classify these techniques on two classes, including, 1) Without an implementation tool and 2) With an implementation tool, as presented in Fig. [4]. In addition, Tab. VII summarizes the informal and formal security analysis techniques used in authentication and privacy preserving schemes for 4G and 5G Cellular Networks.

For the first class, we classify in 'without an implementation tool' eight techniques, including, Zero-Knowledge Proof [148]. Mathematical difficulties, GNY logic [150], CK security model [151], Random oracle model [156], Game theory [157], Probabilistic functions [159], and BAN logic [162]. To analyze the completeness of a cryptographic protocol, both schemes [161] and [79] use the GNY logic [150]. The scheme [93] use random oracle model [156] to show that there is an adversary A can construct an algorithm to solve the CDH problem or the k-CAA problem separately. The scheme [106] uses the BAN logic [162] to demonstrate that the scheme is valid and practical. The mathematical difficulties is used by the scheme [109] to achieve security and privacy using discrete logarithm and computational Diffie-Hellman problems. Furthermore, the game theory [157] is used by the scheme [62] to prove the security of the bipartite protocol by designing a game that turns a CDH instance into the protocol. According to Manshaei et al. [157], the game approach is related to the security problem to be solved, e.g., the stackelberg game for Jamming/Eavesdropping, the static security cost game for Interdependent Security, and the static non-zerosum game for Vendor Patch Management.

For the second class, we classify in 'with an implementation tool' four techniques, including, AVISPA tool [153]. Open-source MIT Kerberos implementation v.1.6.3 [154], OpenUAT [158], and ProVerif [155]. The Open-source MIT Kerberos [154] is used especially for evaluate the performance of the enhanced Kerberos protocol such as the scheme [120]. The OpenUAT [158] is used by the scheme [63] to implement some intuitive authentication methods in a common library. To verify the secrecy of the real identity and the resistance against known attacks, four schemes [108], [102], [101], and [101] use the ProVerif [155], which is an automatic cryptographic protocol verifier, in the formal model, called Dolev-Yao model. Specifically, the ProVerif takes as input a model of the protocol in an extension of the pi calculus with cryptography. For more details about the ProVerif, we refer the reader to the work of Blanchet in [165]. Therefore, five schemes [163], [164], [87], [88], and [82] use the AVISPA tool [153] based on the HLPSL language [153] to verify the security of these schemes against insider attacks and outsider attacks.

V. AUTHENTICATION AND PRIVACY PRESERVING SCHEMES FOR 4G AND 5G CELLULAR NETWORKS

In this section, we will discuss the comparison of authentication and privacy preserving schemes for 4G and 5G Cellular Networks in term of authentication and privacy models. After reviewing around 50 papers published between 2005 and 2017, which are indexed in Scopus and Web of Science, we categorized the authentication and privacy models, as presented in Fig. [5] TabVIII and Tab IX. Based on this categorization, we classify the schemes in seven types (as presented in Fig. 9), including, 1) Handover authentication with privacy, 2) Mutual authentication with privacy, 3) RFID authentication with privacy, 4) Deniable authentication with privacy, 5) Authentication with mutual anonymity, 6) Authentication and key agreement with privacy, and 7) Three-factor authentication with privacy. Tab. XI summarizes the authentication and privacy preserving schemes for 4G and 5G Cellular Networks.

A. Handover authentication with privacy

Based on the cryptographic primitives, the existing handover authentication schemes for LTE wireless networks can be classified into three categories, including, 1) Symmetrical key-based scheme, 2) Public key-based scheme, and 3) Hybrid scheme. In LTE wireless networks, there are two types of base stations, namely, Home eNodeB (HeNB) and eNodeB (eNB). According to Cao et al. [87], the 3GPP project suggested handover from an eNB/HeNB to a new eNB/HeNB cannot achieve backward security in handover procedures. Specifically, the authors proposed a handover authentication scheme for the mobility scenarios in the LTE networks. Based on the idea of proxy signature, the scheme [87] provide several security features, including, perfect forward and backward secrecy. In addition, the scheme [87] is efficient in terms of computational cost and communication overhead compared with the handover scheme in [176], but the identity privacy is not considered. Similar to the scheme [87], Cao et al. [89]
proposed a handover authentication scheme to fit in with all of the mobility scenarios in the LTE networks. The scheme can provide strong security guarantees including perfect forward secrecy, master key forward secrecy, and user anonymity. The scheme [89] is efficient in terms of computational cost, communication cost, and storage cost. As a matter of fact, these both two schemes [87, 89] do not consider the identity and location privacy. To solve this problem, the idea of Gao et al. [68] can be applied with both schemes [87] and [89].

IEEE 802.16m is proposed as an advanced air interface to meet the requirements of the fourth generation (4G) systems. To preserves the identity privacy for IEEE 802.16m network,
and 3) Privacy preservation. In addition, the scheme [88] is efficient in terms of computation and communication overhead compared with Fu et al. scheme [177]. The scheme [88] does not consider k-anonymity, which is a privacy protection scheme with the context of location privacy. The following question is: Is it necessary to apply the k-anonymity improve user privacy in future 5G networks? Niu et al. [123] show us that we need to generate and select the dummy users who can contribute to improving users privacy. As an additional benefit, the users can improve their location privacy significantly by applying the idea of pseudo-location swapping [123].

To provide the security key derivation and anonymity for all of the mobility scenarios in LTE-A networks, Cao et al. [124] proposed a group-based anonymity handover protocol, named NAHAP. The NAHAP protocol is efficient in terms of the signaling cost, the communication cost and the computational cost compared with the LTE-A handover mechanism. Similar to NAHAP scheme, the same authors proposed another uniform group-based handover authentication protocol, named UGHA, which is efficient in term of computational cost compared with the scheme [178]. Using software-defined networking, Duan and Wang [179] proposed an authentication

Fu et al. (2012) [88] proposed a privacy-preserving fast handover authentication scheme based on the pseudonym. Based on the 3-way handshake procedure, the scheme [88] can achieve the following research objectives, including, 1) Fast handover, 2) Mutual authentication and key agreement, and 3) Privacy preservation. In addition, the scheme [88] is efficient in terms of computation and communication overhead compared with Fu et al. scheme [177]. The scheme [88] does not consider k-anonymity, which is a privacy protection scheme with the context of location privacy. The following question is: Is it necessary to apply the k-anonymity improve user privacy in future 5G networks? Niu et al. [123] show us that we need to generate and select the dummy users who can contribute to improving users privacy. As an additional benefit, the users can improve their location privacy significantly by applying the idea of pseudo-location swapping [123].

To provide the security key derivation and anonymity for all of the mobility scenarios in LTE-A networks, Cao et al. [124] proposed a group-based anonymity handover protocol, named NAHAP. The NAHAP protocol is efficient in terms of the signaling cost, the communication cost and the computational cost compared with the LTE-A handover mechanism. Similar to NAHAP scheme, the same authors proposed another uniform group-based handover authentication protocol, named UGHA, which is efficient in term of computational cost compared with the scheme [178]. Using software-defined networking, Duan and Wang [179] proposed an authentication
### TABLE XI

**SUMMARY OF AUTHENTICATION AND PRIVACY PRESERVING SCHEMES FOR 4G AND 5G CELLULAR NETWORKS**

| Scheme | Network model | Auth. model | Privacy model | Performances (+) and limitations (-) | Complexity |
|--------|----------------|-------------|----------------|----------------------------------------|------------|
| Saxena et al. [69] | - LTE cellular system with four entities, including, user equipment (UE), mobility management entity (MME), home service server (HSS), and radio access point | - Mutual authentication | - Untraceability; - Forward privacy; - Anonymity; | + Secure against replay attack, man-in-the-middle attack, redirection attack, impersonation attack, and message modification attack; + Provide the untraceability, forward privacy, and anonymity; + Provide the security key derivation and anonymity; + Reduce bandwidth consumption during authentication; - The scalability is not considered compared to three schemes [117], [74], and [75]. | Bandwidth consumption: - Between UE and MME = 697 bits; - Between MME and HSS = 886 bits; |
| Wang et al. [90] | - Roaming service in mobile networks | - Password-based authentication | - User anonymity | + Can achieve user anonymity; + Can withstand offline password guessing attack even if the victim’s smart card is lost; + Efficient in term of computation cost on user side compared to five schemes Li et al. [168], Isawa-Morii [169], He et al. [170], Zhou-Xu [171], and Xu et al. [172]. + The proposed scheme needs to be evaluated in term of communication overhead; - The handover delays are not measured; | Computation cost on user side: 1TSE + 4H + 2H |
| Cao et al. [124] | - Machine Type Communication (MTC) in LTE-A networks with three entities, including, the MTC device domain, the 3GPP network domain, and the MTC application domain | - Group-based handover authentication | - Anonymity | + Resistance to replay attack, eavesdropping attack, masquerade attack, and man-in-the-middle attack; + Provide the security key derivation and anonymity; - The scheme is not proven using the formal security analysis techniques. | Computation cost on user side: 3Tm + 7H |
| He and Wang [106] | - Multiserver environment | - Biometrics-based authentication | - Anonymity | + Provide mutual authentication; + Provide perfect forward secrecy; + Suitable for the multiserver environment; + Resistance to attacks, including, replay attack, stolen verifier attack, user impersonation attack, server spoofing attack, modification attack, and man-in-the-middle attack; + The desynchronization attack is not considered. | Computation cost on user side: 3Tm + 7H |
| Fu et al. [108] | - Machine-type communication (MTC) model in LTE advanced networks | - Group authentication; | - Anonymity; - Unlinkability; - Traceability; | + Provide robust privacy preserving including user anonymity, unlinkability, and traceability; + Guarantee mutual authentication and congestion avoidance; + Secure against four attacks, including, replay attack, impersonation attack, man-in-the-middle attack, and DoS attack; - The desynchronization attack is not considered. | Computation overhead: (8n + 6 m) TH + (3n + m) TM ; Signaling overhead: n + 6m |
| Mahmoud et al. [109] | - LTE network-based advanced metering infrastructure (AMI) | - Anonymous authentication | - Location privacy | + Secure against impersonation attack, DoS attack, replay attack, and man-in-the-Middle attack; + Verify the authenticity and integrity of the aggregated bids; + Can achieve the privacy requirements with almost negligible performance degradation; + The proposed scheme is not compared with other related schemes. | The aggregated signature needs only 56 bytes |
| Ramadan et al. [110] | - LTE cellular system with four entities, including, user equipment, mobility management entity, home service server, and radio access point | - Mutual authentication and key agreement | - Identity privacy | + Secure against presentation and impersonation attacks, fake base station attack, and replay attack; + Provide the security architecture with flexibility and reliability; + Provide forward/backward secrecy; - The man-in-the-middle attack is not considered compared to the scheme [64]. | Computation cost on user side : 4TECC + 2TH + 2Tm + TM |
| Hashem et al. [166] | - Multi-tier 5G enabled vehicular network with six entities, including, HetNets, D2D communications, a cloud platform, department of motor vehicles (DMV), trust authority (TA), and law enforcement agency (LEA) | - Mutual authentication | - Conditional anonymity; - Traceability of misbehaving participants | + Achieve the conditional anonymity and privacy; + Resistant to traffic analysis attack, Sybil attack, eavesdropping attack, and fabrication attack; + 5G enabled vehicular networks; - The desynchronization attack is not considered. | Computation cost on user side : 6TH + 2TS; - TCOM =13.3s |
| Harandi et al. [163] | - LTE wireless network | - Mutual authentication with key agreement | - Location privacy | + Secure against replay attacks; + Minimizes the use of both symmetric and asymmetric key encryption due to its excessive overhead; - The untraceability and forward privacy are not considered. | Signaling overhead: Case with global random identity = 128 bits; |
| Li et al. [70] | - Machine-type communication (MTC) model in LTE advanced network | - Group-based authentication | - N/A | + Secure against replay attack, redirection attack, man-in-the-middle attack, DoS attack, and impersonation attack; + Can reduce the communication overhead and alleviates the burden between machine type communication devices; - The known-key secrecy and the perfect forward secrecy are not considered compared to the scheme [109]. | Computation cost: (Th + Th + Tm + n) |
| Zhang et al. [103] | - Roaming services in global mobility network | - Roaming authentication | - Anonymity | + Preserve the non-reputation, user anonymity, and untraceability; + Provide the perfect forward secrecy; + Prevention of impersonation attacks; - The DoS attack is not considered; | Computation cost: 4TM + 4TH + 10FS |
| Fu et al. [164] | - LTE/LTE-A network with the public switch telephone network | - Handover authentication | - Anonymity; - Unlinkability; - Traceability; - Non-frameability; | + Protection against Man-in-the-Middle attack, DoS attack, and replay attack; + Efficient in terms of computation cost and communication overhead compared to three schemes, namely, HALP scheme [173], Pair-Hand scheme [174], and UHAEN scheme [175]. - The perfect forward and backward secrecy are not considered compared to the scheme [57]. | Computation cost on user side : 5TM |
handover scheme with privacy protection in 5G heterogeneous network communications. Recently, Fu et al. [108] proposed a novel group authentication protocol with privacy-preserving to provide unlinkability and traceability in 4G/5G communications. The scheme [108] is efficient in terms of the signaling overhead and computation overhead compared to two schemes, including, Cao’s scheme [180] and SE-AKA [181]. To fit in with all of the mobility scenarios in the LTA/LTA-A networks, Fu et al. [164] proposed a privacy-preserving non-frameability authentication protocol, called Nframe. To guarantee users’ privacy, unlinkability and traceability, the Nframe protocol uses a pseudonym-based scheme. To achieve a simple authentication process without a complex key management and minimize message exchange time, the Nframe protocol uses pairing-free identity-based cryptography. In addition, the Nframe protocol is efficient in terms of computation cost and communication overhead compared to three schemes, namely, HALP scheme [173], Pair-Hand scheme [174], and UHAEN scheme [175], but the perfect forward and backward secrecy are not considered compared to the scheme [87]. For more details in the field of handover authentication protocols using identity-based public key cryptography, we refer the reader to the recent work of He in [182].

B. Mutual authentication with privacy

To achieve the mutual authentication with privacy, the proposed security schemes for 4G/5G networks need to preserve the Location privacy, Identity privacy, Data integrity, and Authenticity, as shown in Fig. 7. However, Dimitriadis and Polemi (2006) [111] proposed a protocol, named IDM3G, to achieving the mutual authentication and identity privacy in 3G. The IDM3G protocol use two phases, namely, 1) the authentication of the UMTS Subscriber Identity Module (USIM) by providing a personal identification number and 2) the mutual authentication between the USIM and the mobile operator. By using the authentication request based on HTTP, the IDM3G

Fig. 5. Categorization of authentication and privacy models

Fig. 6. Classification of authentication and privacy preserving schemes for 4G and 5G Cellular Networks

Fig. 7. Classification of mutual authentication with privacy schemes
is efficient in terms of the number of messages exchanged in the path, which is lower compared to both protocols [183] [184], but the location privacy is not considered. Similar to the IDMS3 protocol, Dimitriadis and Shaikh (2007) [112] proposed a protocol, called BIO3G, for establishing secure and privacy friendly biometric authentication in 3G mobile environments. The BIO3G protocol cannot resist against the DoS attacks and the location and identity privacy are not considered compared to the IDMS3 protocol [111]. He et al. [74] proposed three categories of authentication scenarios for the 4G system. The main idea of [74] is the use of Self-Certified Public-Key, which need not be accompanied by a separate digital certificate. The advantage of the protocol [74] is that it considers the identity privacy, but its disadvantage is the location privacy of mobile users. The following question is: Is it necessary to preserve the location privacy in future 5G networks? According to Lu et al. [78], ensuring location privacy in a cellular network is an effort to prevent any other party from learning the mobile users current and past locations. The recent idea in [135] and [136] can be applied for privacy preserving the social application under 4G/5G communications.

Location privacy is one of the most important models for privacy, as discussed in our previous surveys in [9] [187]. To the best of our knowledge, Lu et al. [78] proposed the first study that deals with the mutual authentication with location privacy. Specifically, the authors proposed a novel mutual authentication protocol with provable link-layer location privacy. With the help of the Preset in Idle technique, the protocol [78] is efficient in terms of the packet delay time and the total packet time cost compared with the protocol [188]. On the other hand, mutual authentication with identity privacy can also be preserved using the identity management mechanism proposed by Abdelkader et al. [82]. The authors proposed an advanced Identity Management scheme, called AIM, in order to guarantee mutual authentication, privacy, and tracking avoidance for 4G networks. According to Saxena et al. [69], the EPS-AKA protocol of the LTE network does not support Internet of Things (IoT). Specifically, the authors proposed an authentication protocol for an IoT-Enabled LTE Network that is entirely based on the symmetric key cryptosystem.

For the security of future fifth generation telecommunication services, a service provider will need to apply the managed security services (MSS) as network security services. According to Ulltveit-Moe et al. [114], the security services may be required for all mobile terminals such as antivirus, firewalls, Intrusion Detection Systems (IDS), integrity checking and security profiles. Specifically, the authors proposed a location-aware mobile intrusion prevention system with enhanced privacy, named mIPS, which is integrated into MSS. The mIPS system can preserve the personal privacy profile, but he needs to be evaluated in the future for 5G communications. Using identification parameters, including, the International Mobile Subscriber Identity (IMSI) and the Radio Network Temporary Identities (RNTI), Jang et al. [95] proposed an authentication protocol to safely transmit identification parameters in different cases of the initial attach under 4G mobile communications.

According to Madueno et al. [189], the LTE network is a promising solution for cost-efficient connectivity of the smart grid monitoring equipment. To ensure the security of this equipment, Haddad et al. [66] proposed a privacy-preserving scheme to secure the communications of an automatic metering infrastructure via LTE-A networks. To share keys, the scheme [66] uses a key agreement protocol between the smart meters, the utility company, and the LTE network. The scheme [66] cannot only achieve the mutual authentication, key agreement, and key evolution but also can preserve the confidentiality/data integrity and authenticity. Recently, Mahmoud et al. [109] proposed a privacy preserving power injection querying scheme over LTE cellular networks, to solve the problem of privacy exposure of storage unit owners. Therefore, the 4G/5G communications can be used by the traffic information systems [101]. Gisdakis et al. [101] addressed the security and privacy protection aspects of smartphone-based traffic information systems. More specifically, the authors proposed a privacy-preserving system using the architecture presented in [190]. This system is based on three main phases, namely, 1) System initialization, 2) Device authentication and report submission, and 3) Device eviction. In addition, the system [101] can provide the anonymity and the report unlinkability.

C. RFID authentication with privacy

Radio Frequency Identification (RFID) systems are low cost and convenient in identifying an object without physical contact, which consists of radio frequency (RF) tags, or transponders, and RF tag readers, or transceivers. According to Sun and Ting [117], RF technology can provide three functions: item awareness, information searching, and quality control. In addition, an RFID application contains three basic roles: 1) tag, 2) reader, and 3) back-end database [191]. As presented in Fig. 8 RFID authentication protocols with RFID privacy 1) Generation-2 Protocol, e.g., the Gen2 protocol in [192]. 2) CRC-Based Protocol, e.g., the SASI protocol in [162]. 3) Minimalist Cryptography, e.g., the protocol in [193]. 4) Protocol with Substring Function, e.g., the protocols in [194] and [195]. and 5) ECC-Based Protocol, e.g., the protocol in [167]. Similar to Sun and Ting [117], Dubrova et al. [105] proposed a message authentication scheme based on Cyclic Redundancy Check (CRC) codes for 5G Mobile Technology.
Chien [167] proposed an ultralightweight RFID authentication protocol, called SASI, to providing strong authentication and integrity protection. The SASI protocol uses only simple bit-wise operations on the tag. Chien and Chen [113] addressed the weaknesses of two schemes [196] [192] and proposed a mutual authentication scheme for GEN-2 RFID. The scheme [113] can preserve the privacy and resist against DOS attack compared to both schemes [196] [192]. Liu and Bailey proposed another interesting protocol that can achieve both privacy and authentication in [77]. Specifically, the authors proposed a privacy and authentication protocol for passive RFID tags, called PAP. The PAP protocol is based on four main phases, namely, In-store, Checkout, Out-store, and Return. PAP can resist against replay attack, but vulnerable to some attacks such as desynchronization attack and tracing attack. The following question is: Is it really necessary to detect the tracing attack? According to Sun and Ting [117], with tracing attack, an adversary have both a "malicious active reader" and several "malicious passive" loggers. The authors proposed a solution, called Gen2+, for RFID application with focusing on the protection of UltraHigh Frequency (UHF) passive tags from malicious readers. The Gen2+ scheme can detect the tracing attack, also efficient in terms of the number of rounds required, and the period of key update compared to three schemes [167], [192], and [194].

To achieve RFID authentication with anonymity/untraceability, and even availability, Chien and Laih [119] proposed a RFID authentication protocol based on Error Correction Codes (ECC) [197]. The protocol [119] can achieve mutual authentication between the tags and the reader based on the successful verification of the PRNG function applied on the secret key. The protocol [119] is efficient in term of computation complexity compared to the protocol LMAP [198]. According to Kulseng et al. [122], the lightweight solution such as LMAP [198] has been either broken or weakened. In fact, the authors in [122] proposed a protocol in which only the authenticated readers and tags can successfully communicate with each other. Then, they designed protocols that achieve secure ownership transfer in three-party and two party low-cost RFID systems, but these protocols need to be examined using real hardware. Especially for detection of man-in-the-middle attack, Li et al. [64] proposed an authentication protocol, named LCMQ, which is proved secure in a general man-in-the-middle model. The LCMQ protocol can achieve RFID authentication and also efficient in terms of the tag’s computation, storage, and communication costs compared with traditional cryptographic primitives such as RSA, DSA, and SHA.

Furthermore, Zhou et al. [83] proposed a lightweight anti-desynchronization RFID authentication protocol, which is suitable for the low-cost RFID environment. Based on the idea of Index-pseudonym, the protocol [83] cannot only ensure the privacy of the tag, but also provide the forward security, location privacy, integrity, and tag anonymity. The strong advantage of the protocol [83] is in desynchronization resistance compared to the protocol [122]. By using a modified EAP-AKA protocol [199] for authentication with the access network, Sharma and Leung [90] proposed a robust one-pass IMS authentication mechanism in LTE-fem to cell heterogeneous networks. The mechanism is 50 percent improvement over the existing multi-pass authentication scheme published before 2012. Liao and Hsiao [98] proposed a secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, which is efficient in terms of computational cost and communication overhead compared to the scheme of Tuyls et al. [200].

To preserve the authentication for IoT in 5G, Fan et al. [161] proposed a lightweight RFID mutual authentication protocol with cache in the reader, named LRMAPC. Using an ultralightweight RFID mutual authentication protocol with cache in the reader, the LRMAPC protocol can achieve mutual authentication and provide forward security. Recently, Sun et al. [201] formulated secure and privacy preserving object finding via mobile crowdsourcing. Then, they proposed a scheme, called SecureFind. Based on the initial object-finding request, the SecureFind scheme can obtain the information the service provider. Based on the vulnerability of two published protocols RRAP [202] and RCIA [203], Luo et al. [204] proposed recently a new ultra-lightweight mutual authentication protocol, which doesn’t use any unbalanced operations like OR and AND.

D. Deniable authentication with privacy

The deniable authentication differs from traditional authentication in a way that the Receiver cannot convince a third party [205]. Therefore, Lee et al. [72] proposed a protocol based on the non-interactive manner in order to achieve deniable authentication. Based on the shared session secret and the ElGamal signature scheme [206], the protocol [72] does not only consider the security issues proposed in [207], including forgery attack, impersonation attack, denialility, and completeness but can also sustain the security when the session secret has already been compromised. Therefore, the use of message authentication codes (MACs) [132] between two parties in cellular networks can achieving the deniable authentication.

To providing a lower degree of scalability and security, Bersani and Tschofenig [73] defined an experimental protocol for the Internet community, called EAP-PSK, under the

---

**Fig. 9. Classification of methods based on EAP authentication framework**

---
RFC 4764. The Extensible Authentication Protocol (EAP) is an authentication frequently used in wireless networks that defined in RFC 3748 [208], RFC 2284 [209], and was updated by RFC 5247 [210]. As detailed in Fig. 9, there are many EAP authentication framework-based methods, which published as RFCs [211] as Internet Standards. However, Chen et al. [76] proposed two strong devices and user authentication schemes for Wi-Fi and WiMAX inter-networked wireless cities. The idea of [76] is based on the modified Transport Layer Security (TLS) protocol [212], which leverage Trusted Platform Module (TPM) technologies [213]. The work [76] does not consider the identity and location privacy. Besides, the following question is: can we use the EAP to achieve the identity privacy? According to Pereniguez et al. [121], if the authentication mechanism does not have an adequate level of privacy, the identity and location can be revealed. Pereniguez et al. [121] proposed a privacy-enhanced fast re-authentication, named 3PFH, for EAP-based 4G of mobile communications. The main idea of 3PFH is defined by a multi-layered pseudonym architecture to achieve user anonymity and untraceability. The 3PFH is applicable when the handoff takes place between different network operators. In addition, Arul et al. [214] proposed a caching mechanism, called UPP-KC, where the keys are cached only along a predicted path for broadband wireless networks.

E. Authentication with mutual anonymity

Anonymity is an important security aspect of cellular communications, since it protects the privacy of the users, as discussed in our previous survey in [9]. Lu et al. [78] proposed an anonymous zero-knowledge authentication protocol, called PT, for Peer-to-peer (P2P) systems. We note here that we have selected this protocol because it can apply as an authentication protocol in 4G and 5G cellular communications. Besides, the PT protocol can support trust management in anonymous environments and scalable in both static and dynamic environments. To provide integrity to data exchanges after authentication, the PT protocol uses a Diffie-Hellman Key Exchange protocol into the authentication procedure to generate a session key.

To achieving the privacy preserving context transfer for 4G networks, Terzis et al. (2011) [84] proposed four privacy preserving schemes for Context transfer protocol (CTXP) [215]. These schemes are efficient in terms of application handoff service time compared to CTX, while at the same time guarantee the privacy of the end-user. To verify the identity of a user or a host over 4G network, the network authentication protocol, called Kerberos, can be used. The Kerberos protocol is proposed under IETF RFC 4120 [216], where he composed with several entities, including, 1) The client (C) with its own secret key, 2) The server (S) with its secret key, 3) Ticket-granting service, and 4) Key distribution center. As presented in Fig. 10 the Kerberos protocol provides several authentication models, including, 1) More efficient authentication to servers, 2) Interoperability, 3) Single authentication, 4) Delegated authentication, and 5) Mutual authentication. However, According to Pereniguez et al. [120], the Kerberos protocol suffers from two issues, namely, user anonymity and service access untraceability. The authors proposed a two-level privacy architecture, named PrivaKerB, to preserves the privacy of the user during activity with Kerberos. Based on two different levels of privacy: level 1, which provides user anonymity through pseudonyms, and level 2 where, apart from user anonymity, service access untraceability is assured. In addition, PrivaKerB is efficient in terms of service times, resource and network utilization compared to the standard Kerberos protocol [216].

Recently, Zhang et al. [71] proposed a secure data sharing strategy for Device-to-Device (D2D) in 4G LTE-advanced network, called SeDS. To ensures data confidentiality, integrity, non-repudiation, and system availability, the SeDS strategy uses the digital signature and symmetric encryption. In addition, the SeDS strategy is efficient in terms of computational overhead, communication overhead and availability in a practical D2D communication environment. The idea of Hashem Eiza et al. [166] can be applied for cloud-assisted video reporting service in 5G enabled vehicular networks.

F. Authentication and key agreement with privacy

The Authentication and Key Agreement (AKA) protocol is a challenge-response based mechanism that uses symmetric cryptography. The Universal Mobile Telecommunication System (UMTS) has adopted the AKA protocol of 3GPP, known as a standard of 3G with RFC 3310. Therefore, Deng et al. [115] proposed an improved authentication and key agreement protocol based on public key cryptosystem. The protocol [115] is vulnerable to some attacks, such as replay attack, man-in-the-middle attack, and DoS attack. The following question is: Is it really necessary to hiding communication content from the external adversary under AKA protocol? Hamandi et al. [163] proposed a hybrid scheme based on modifications to the LTE-AKA scheme, which employs both symmetric and asymmetric key encryption in order to detect and avoid both insider and outsider attacks. Using an efficient access-policy updating method, Li et al. [70] proposed a group-based AKA protocol, called GR-AKA. The GR-AKA can reduce the communication overhead and alleviates the burden between machine type communication devices, but the known-key secrecy and the perfect forward secrecy are not considered compared to the scheme.
To avoid the signal congestion in 3GPP networks, Yao et al. [67] proposed a group-based authentication for machine-to-machine (M2M), which is efficient in terms of bandwidth consumption.

According to Zhu et al. [80], the AKA protocol can easily be extended to provide revocable privacy by adopting the fair blind signature technique [127]. Specifically, Zhu et al. [80] proposed an anonymous authenticated key agreement protocol, called PPAB, to achieve scalable, authentication and billing in the context of interdomain roaming in the wireless metropolitan area sharing networks (WMSNs). The PPAB protocol considers five levels of privacy protection, namely, 1) content privacy, 2) external privacy, 3) internal privacy I, 4) internal privacy II, and 5) internal privacy III. The content privacy is hiding communication content from the external adversary. The external privacy is hiding identity information of mobile users from the external adversary. The internal privacy I is hiding identity information of mobile users from the wireless Internet service providers. The internal privacy II is hiding identity information of mobile users from the roaming broker. The internal privacy III is hiding identity information of mobile users from adversary for each handoff event [80]. Besides, PPAB is efficient in terms of energy consumption compared to the scheme [128], but the deniability and completeness are not considered. To the best of our knowledge, the work of Zhu et al. [80] is the first study on the issues of localized authentication, billing, and privacy in the context of interdomain roaming in the WMSNs. To achieve the protection of user privacy, anonymity and untraceability for roaming network, Zhang et al. [103] proposed a privacy-preserving authentication scheme based on elliptic curve cryptography.

The Session Initiation Protocol (SIP) is proposed by IETF under RFC 3261 in full and a number of extension RFCs including RFC 6665 (event notification) and RFC 3262 (reliable provisional responses). The SIP protocol is an IP-based telephony protocol for multimedia telecommunications (sound, image, etc.) in 3G mobile networks and over Internet Protocol (IP) networks. According to Wu et al. [61], the SIP protocol does not include any specific security mechanisms. Specifically, Wu et al. [61] proposed a provably secure authentication and key agreement protocol for SIP using elliptic curve cryptography, called NAKE, in order to achieve the perfect forward secrecy. The NAKE protocol is preferable in the applications that require low memory and rapid transactions. However, the disadvantage of the NAKE protocol is that it does not preserve the location privacy compared to the scheme [80]. To provide the location and identity privacy, Karopoulos et al. (2011) [116] proposed two solutions in SIP, where the first the ID of the caller is protected while in the second both IDs of the caller and the callee are protected. Both solutions consider the identity privacy and are efficient in terms of mean server response delays compared to standard SIP, but the key agreement is not considered.

To improve the security of both schemes, including, Wu et al.’s scheme [217] and Yoon et al.’s scheme [218]. He [93] proposed a new user authentication and key agreement protocol using bilinear pairings for mobile client–server environment. The idea of [93] is based on the bilinear pairing under the computational Diffie–Hellman (CDH) and collision attack assumption and in the random oracle model. The scheme [93] can achieve the client-to-server authentication, the server-to-client authentication and key agreement under the random oracle model, but the privacy is not considered compared to the scheme [88]. However, using a temporary confidential channel, Chen et al. [62] designed three types of authentication, including, 1) Bipartite authentication protocol, 2) Tripartite authentication protocol, and 3) Multipartite transitive authentication.

Based on three main categories of auxiliary channels, including, input, transfer, and verification, Mayrhofer et al. [62] proposed a unified auxiliary channel authentication protocol, named UACAP, which releases a specific implementation in the form of the Open-source Ubiquitous Authentication Toolkit (OpenUAT) [158]. Using two main phases, namely, 1) Diffie–Hellman key exchange with precommitment and 2) Out-of-band key verification, the UACAP protocol can exploit any combination of security guarantees from arbitrary auxiliary channels. Recently, Ramadan et al. [110] proposed a user-to-user mutual authentication and key agreement scheme, which is more compatible with the LTE security architecture. The scheme [110] is based on four phases, namely, 1) Setup and key generation, 2) Authentication between the users and the mobility management entity, 3) User-to-User authentication, and 4) Establish a shared secret key.

G. Three-factor authentication with privacy

The three-factor authentication schemes with privacy can mainly be classified into three categories: 1) Smart cards-based protocol, 2) Passwords-based protocol, and 3) Biometrics-based protocol, as presented in Fig. [11] The following question is: can we use the three factors together? According to Fan and Lin [79], this three different data types can be used together in an authentication protocol, where smart cards show what you have, passwords represent what you know, and biometrics mean what you are. Specifically, the authors proposed a truly three-factor authentication scheme to achieving the strong biometrics privacy. Based on the login and authentication phase, the server accepts only if each factor (password, smart card, and biometric data) passes the authentication. The protocol [79] is efficient in terms of low computation for smart cards.

![Classification of three-factor authentication schemes with privacy](image-url)
comparing to three-factor authentication schemes in [219] and [220]. Therefore, according to Blasco et al. [221], the biometric systems can mainly be classified into three categories: 1) Traditional Biometric Systems (e.g., Windows Hello [222]), 2) Wearable biometric systems (e.g., Using a smartphone), and 3) Hybrid biometric systems (e.g., Hybrid systems arises in telecare services [223]). For more details in the field of wearable biometric and in the security and privacy issues in implantable medical devices, we refer the reader to the both recent surveys [221] and [222].

For security of 4G and 5G networks using Biometric-based identification, it is required that the client does not learn anything on the database. Therefore, according to Barni et al. [118], the fingerprint is likely to be used in applications that need higher reliability. Specifically, the authors proposed a privacy-preserving system for fingerprint-based authentication. Based on the Fingerprint representation introduced in [225], the identification protocol [118] is efficient in term of bandwidth usage compared to both schemes Erkin et al. [224] and Sadeghi et al. [227]. Especially for multiserver environment, He and Wang [106] proposed a biometrics-based authentication scheme, which is overcome the weaknesses in Yoon and Yoo’s scheme [228] and Kim et al.’s scheme [229].

The password-based-authentication protocols are a reliable solution to provide identity protection and satisfy strong mutual authentication in 4G and 5G networks. Moreover, Sood et al. [85] presented a cryptanalysis of the Hsiang and Shih protocol [230] in order to propose a secure dynamic identity-based authentication protocol for multi-server architecture. The protocol [85] is efficient in term of computational complexity compared to related smart card based multi-server authentication protocols. [230] [231]. Similar to [85], Lee et al. [86] presented a cryptanalysis of Hsiang et al. scheme [230] where the authors have found that Hsiang et al. scheme is still vulnerable to a masquerade attack, server-spoofing attack, and is not easily repairable. Then, the authors [86] proposed a scheme to solve these weaknesses. In addition, Lee et al. scheme [86] is efficient in term of communication cost of the login and verification phase compared to three schemes, namely, Hsiang et al. scheme [230], Liao-Wang scheme [231], and Chang-Lee scheme [232]. Li et al. [91] out that the protocol [85] is still not secure. Based on the cryptanalysis of the protocol [85], the authors [86] proposed a security dynamic identity-based authentication protocol for multi-server architecture. The protocol [91] provide the user’s anonymity, proper mutual authentication, and session key agreement. In addition, the protocol [91] is efficient in terms of computational complexity compared to some related dynamic ID based multi-server authentication protocols, including, [85], [230], and [231]. Similar to [62], Liu and Liang [94] proposed a hierarchical identity-based access authentication protocol, named HA-HIBS-VN, which can be applied for 4G and 5G cellular networks. The HA-HIBS-VN protocol [94] can provide the private key privacy and signature unforgeability. By combining the peer group tree (PGT), identity-based signature, and designed mobile vector network protocol (MVNP), the HA-HIBS-VN protocol [94] is efficient in term of handover delays compared with the protocol in [233].

Previous works in this area, i.e., password-based-authentication, have come short of providing solutions to detecting password reuse attacks. Moreover, Sun et al. [92] proposed the first user authentication protocol to prevent password stealing (i.e., phishing, keylogger, and malware) and password reuse attacks simultaneously. The authors proposed a user authentication, called oPass, to thwart this both attacks. The idea of oPass is to adopt one-time passwords, which they expired when the user completes the current session. Based on two main processes, including, 1) Login phase and 2) Recovery phase, the oPass can protect the information on the cellphone from a thief. Hence, the oPass protocol can be applied for 4G and 5G cellular networks. To provide privacy-preserving and secure roaming service for 4G and 5G cellular networks, Wang et al. [96] revisited the privacy-preserving two-factor authentication scheme presented by Li et al. in [168], which they showed that the scheme [234] suffers from offline password guessing attack. The study of Wang et al. [96] can withstand offline password guessing attack even if the victim’s smart card is lost. As an additional benefit, the Wang et al. scheme [96] is efficient in term of computation cost on user side compared to fives schemes Li et al. [168], Isawa-Morii [169], He et al. [170], Zhou-Xu [171] and Xu et al. [172]. To overcome the weaknesses of Das scheme [235], Li et al. [100] a three-factor remote user authentication and key agreement scheme using biometrics. Based on discrete logarithm problem [236], the Li et al. scheme [100] can ensure the known-key secrecy and provide the perfect forward secrecy.

Similar to [96], Chen et al. (2014) [65] proposed an improved smart-card-based password authentication and key agreement scheme. Based on the review of the Xu et al. scheme [237] and Sood et al. scheme [238], the scheme [65] can achieve mutual authentication and guarantees forward secrecy. In addition, the scheme [65] is efficient in term of computation cost on server side compared to three schemes Xu et al. [237] Sood et al. [238], and Song [239]. Therefore, if the authentication stored in the memory device is exposed, Jiang et al. pointed out that the scheme [65] suffers from offline password guessing attacks.

Based on the cryptanalysis of two schemes of Chen et al. [85] and Wen–Li [240], Ma et al. [97] proposed three principles designing more robust schemes in the future, which can be applied for 4G and 5G cellular networks. To overcome the weaknesses of Chang et al.’s scheme [241], Kumari et al. [99] proposed an improved user authentication scheme with session key agreement facility. Compared to the Chang et al.’s scheme [241], the Kumari et al.’ scheme [99] cannot only provide forward secrecy, but the user is anonymous and untraceable. To overcome the weaknesses of Kumari et al.’s scheme [242], Chaudhry et al. [102] proposed an enhanced remote user authentication scheme, which can ensures privacy and anonymity.

VI. FUTURE DIRECTIONS

As shown in Fig. 12 authentication and privacy-preserving schemes for 4G and 5G cellular networks focus on four...
A. Privacy preservation for Fog paradigm-based 5G radio access network

To meet the requirements of mission-critical applications in 5G radio access network (RAN), two system design paradigms can be used, including, cloud and fog. Recently, Ku et al. [243] proposed a Fog-cloud integrated RAN architecture, named F-RAN. To integrate the computing functionality to 5G cellular networks, F-RAN adopts two approaches, including, loosely-coupled and tightly-coupled. However, several attacks against privacy can be launched, such as man-in-the-middle attack and replay attack, which can reveal the location and identity of Fog nodes in F-RAN architecture. How to provide the location and identity privacy for Fog paradigm-based 5G radio access network? Hence, privacy preservation for Fog paradigm-based 5G radio access network should be exploited in the future.

B. Authentication for 5G small cell-based smart grids

The smart grid deployment requires a faster communication medium in the long run, which can be achieved by the 5G wireless from data and control plane isolation. With evolved multimedia broadcast and multicast communication, between aggregators (small cells) and smart grid consumers, Saxena et al. [244] introduced a planning of 5G small cells, for optimal demand response in smart grids. This idea can reduce energy production cost by 30%, but this is calculated without taking in mind possible network attacks that also affect energy consumption. Even though numerous authentication schemes have been designed in recent years to protect communication in smart grids but these schemes are not reliable to detect and prevent common attacks as well as reducing energy production cost for 5G small cell-based smart grids. Therefore, how do we reduce the cost of energy under network attacks? Hence, authentication for 5G small cell-based smart grids is another possible future direction.

C. Privacy preservation for SDN/NFV-based architecture in 5G scenarios

Software Defined Networking (SDN) and Network Function Virtualization (NFV) technologies considered as key drivers to paving the way towards the 5G era, as discussed in a recent survey published in 2017 [245]. Specifically, Nguyen et al. reviews the state of the art of SDN/NFV-based mobile packet core network architectures, none of them carries study for the privacy preservation. A possible research direction in this topic could be related to privacy preservation for SDN/NFV-based architecture in 5G scenarios such as location privacy, identity privacy, anonymity, etc. Last but not least, guaranteeing the authentication between the mobile users and devices are also important factors when realizing the network sharing based on SDN/NFV in 5G scenarios.

D. Dataset for intrusion detection in 5G scenarios

As we have seen in subsection III-B, data mining and machine learning methods are used to help discover, determine, and identify unauthorized use and destruction of information systems, such as 4G and 5G cellular networks [246]. Buczak
and Guven [246] have found that the most intrusion detection systems used the DARPA 1998, DARPA 1999, DARPA 2000, or KDD 1999 data sets. Therefore, the question we ask here is: Can these data sets be used in 5G scenarios? In other words, the threat models discussed in subsection III-A are simulated in these data sets? We believe that further research is needed to develop a new data set to build a network intrusion detector under 5G environment.

E. Privacy preserving schemes for UAV systems in 5G heterogeneous communication environment

In a connected society, i.e., IoT, the intelligent deployment of Unmanned Aerial Vehicle (UAVs) in 5G heterogeneous communication environment will play a major role in improving peoples’ lives. With the limitation of wireless communication and computing capability of drones, the application of UAV is becoming more and more complicated, especially for security and privacy issues. In a work published in 2017, He et al. [247] categorized threat models on the drone-assisted public safety network, in four categories, namely, attacks on confidentiality, attacks on integrity, attacks on availability, and attacks on authenticity. One possible future direction is to develop a privacy preserving schemes for UAV systems in 5G heterogeneous communication environment.

F. Authentication and privacy-preserving schemes for 5G small cell-based vehicular crowdsensing

Vehicular crowdsensing entails serious security and privacy issues, where it is important to protect user identity, location privacy, among others. Using Fog computing, Basudan et al. [248] proposed a new idea for privacy preserving for vehicular crowdsensing. Specifically, this idea introduced a certificateless aggregate signcryption scheme, named CLASC, which is highly efficient in term of low communication overhead and fast verification. Moreover, the system model considers that the road surface condition monitoring system comprises a control center, vehicles, smart devices, roadside units, and cloud servers. Since we are moving to the 5G communications, a new emerging paradigm will appear, named 5G small cell-based vehicular crowdsensing, in order to meet the requirements for new applications in vehicular ad hoc networks such as parking navigation, road surface monitoring, and traffic collision reconstruction. The future works addressing the limitations of authentication and privacy-preserving schemes for vehicular crowdsensing will have an important contribution for 5G small cell-based vehicular crowdsensing.

VII. CONCLUSIONS AND LESSONS LEARNED

In this article, we surveyed the state-of-the-art of authentication and privacy-preserving schemes for 4G and 5G cellular networks. Through an extensive research and analysis that was conducted, we were able to classify the threat models in cellular networks into attacks against privacy, attacks against integrity, attacks against availability, and attacks against authentication. In addition, we were able to classify the countermeasures into cryptography methods, humans factors, and intrusion detection methods. For the cryptographic methods, the surveyed schemes use three types of cryptographic, including, public-key cryptography, symmetric-key cryptography, and unkeyed cryptography. To ensure authentication, the surveyed schemes use three factors, including, what you know (e.g., passwords), what you have (e.g., smart cards), and 3) who are you (e.g., biometrics). For intrusion detection methods, the surveyed schemes use three systems, including, signature-based system, anomaly-based system, and hybrid IDS.

From security analysis point, there are twelve informal and formal security analysis techniques used in authentication and privacy preserving schemes for 4G and 5G cellular networks, namely, zero-knowledge proof, mathematical difficulties, GNY logic, CK security model, random oracle model, game theory, probabilistic functions, BAN logic, AVISPA tool, Open-source MIT Kerberos, OpenUAT, and ProVerif. We were able to classify these techniques in two classes, including, without an implementation tool and with an implementation tool.

Based on the categorization of authentication and privacy models, we were able to classify the surveyed schemes in seven types, including, handover authentication with privacy, mutual authentication with privacy, RFID authentication with privacy, deniable authentication with privacy, authentication with mutual anonymity, authentication and key agreement with privacy, and three-factor authentication with privacy.

Based on the vision for the next generation of connectivity, we proposed six open directions for future research about authentication and privacy-preserving schemes, namely, Fog paradigm-based 5G radio access network, 5G small cell-based smart grids, SDN/NFV-based architecture in 5G scenarios, dataset for intrusion detection in 5G scenarios, UAV systems in 5G environment, and 5G small cell-based vehicular crowdsensing.

References

[1] “Ericsson press.” [Online]. Available: https://www.ericsson.com/en/press-releases/2014/4/ericsson-5g-delivers-5-gbps-speeds

[2] Ericsson Press Releases.” [Online]. Available: http://www.ericsson.com/en/press-releases/2014/3/softbank-and-ericsson-to-demonstrate-5g-28ghz

[3] “Vodafone News.” [Online]. Available: http://www.vodafone.com/content/index/what/technology-blog/5g-high-frequency.html

[4] “Huawei News.” [Online]. Available: http://news.huawei.com/en/events/mwc2017/

[5] “Reuters News.” [Online]. Available: http://www.reuters.com/article/us-verizon-5g-atuskbn161569

[6] “AT&T Newsroom.” [Online]. Available: http://about.att.com/story/att_intsa[5]6gstep_forward_to_5g.html

[7] “NTT Press Releases.” [Online]. Available: http://www.ntt.co.jp/news20171703e/170327a.html

[8] N. Panwar, S. Sharma, and A. K. Singh, “A survey on 5G: The next generation of mobile communication,” Phys. Commun., vol. 18, pp. 64–84, mar 2016.

[9] M. A. Ferrag, L. Maglaras, and A. Ahmim, “Privacy-preserving schemes for Ad Hoc Social Networks: A Survey,” IEEE Commun. Surv. Tutorials, pp. 1–1, 2017.

[10] P. Basaras, I. Belikaidis, L. Maglaras, and D. Katsaros, “Blocking epidemic propagation in vehicular networks,” in Wireless On-demand Network Systems and Services (WONS), 2016 12th Annual Conference on. IEEE, 2016, pp. 1–8.

[11] R. Kwan and C. Leung, “A Survey of Scheduling and Interference Mitigation in LTE,” J. Electr. Comput. Eng., vol. 2010, pp. 1–10, 2010.

[12] F. Capozzi, G. Piro, L. Grieco, B. Boggia, and P. Camarda, “Downlink Packet Scheduling in LTE Cellular Networks: Key Design Issues and a Survey,” IEEE Commun. Surv. Tutorials, vol. 15, no. 2, pp. 678–700, Jan 2013.
[106] D. He and D. Wang, “Robust Biometrics-Based Authentication Scheme for Multiserver Environment,” IEEE Syst. J., vol. 9, no. 3, pp. 816–823, sep 2015.

[107] Q. Jiang, J. Ma, G. Li, and X. Li, “Improvement of robust smart-card-based password authentication scheme,” Int. J. Commun. Syst., vol. 28, no. 2, pp. 383–397, jan 2015.

[108] A. Fujii, J. Song, S. Li, G. Zhang, and Y. Zhang, “A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks,” Secur. Commun. Networks, pp. n/a–n/a, 2016.

[109] M. Mahmoud, N. Saputo, P. Akula, and K. Akkaya, “Privacy-Preserving Power Injection over a Hybrid AM/AM LTE Smart Grid Network,” IEEE Internet Things J., pp. 1–1, 2016.

[110] M. Ramadan, F. Li, C. Xu, A. Mohamed, H. Abdalla, and A. A. Ali, “User-to-User Mutual Authentication and Key Agreement Scheme for LTE Cellular System.” J. Netw. Secur., vol. 18, no. 4, pp. 769–781, 2016.

[111] C. K. Dimitriadis and D. Polemi, “An identity management protocol for Internet applications over 3G mobile networks,” Comput. Secur., vol. 25, no. 1, pp. 45–51, feb 2006.

[112] C. K. Dimitriadis and S. A. Shaikh, “A Biometric Authentication Protocol for 3G Mobile Systems: Modelled and Validated Using CSP and Rank Functions.” J. Netw. Secur., vol. 5, no. 1, pp. 99–111, 2007.

[113] H.-Y. Chien and C.-H. Chen, “Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards,” Proc. IEEE, vol. 29, no. 2, pp. 254–259, feb 2007.

[114] N. Ullivest-Moe, V. A. Oleshchak, and G. M. Kien, “Location-Aware Mobile Intrusion Detection with Enhanced Privacy in a 5G Context,” Wirel. Pers. Commun., vol. 57, no. 3, pp. 317–338, apr 2011.

[115] Yaping Deng, Hong Fu, Xianzhong Xie, Jihua Zhou, Yucheng Zhang, and Jinling Shi, “A novel 3GPP SA6 authentication and key agreement protocol,” in 2009 IEEE Int. Conf. Netw. Infrastruct. Digit. Content. IEEE, nov 2009, pp. 557–561.

[116] G. Karopoulos, G. Kambourakis, and S. Gritzalis, “PriviSIP: Ad-hoc identity privacy in SIP.” Comput. Stand. Interfaces, vol. 33, no. 3, pp. 301–314, mar 2011.

[117] Hung-Min Sun and Wei-Chih Ting, “A Gen2-Based RFID Authentication Protocol for Security and Privacy,” IEEE Trans. Mob. Comput., vol. 8, no. 8, pp. 1052–1062, aug 2009.

[118] M. Barmi, F. Scotti, A. Piva, T. Bianchi, D. Catalano, M. Di Raimondo, G. Karopoulos, G. Kambourakis, and S. Gritzalis, “PrivaSIP: Ad-hoc identity privacy in SIP,” in Proc. 12th ACM Int. Conf. Comput. Secur., vol. 76, no. 4, pp. 395–416, apr 2011.

[119] A. Gupta, R. K. Jha, and S. Jain, “Attack modeling and intrusion detection system for 5G wireless communication network,” Int. J. Commun. Syst., vol. 30, no. 10, p. e3237, jul 2017.

[120] P. Casas, A. D’Alconzo, P. Fiadino, and C. Callegari, “Detecting and diagnosing anomalies in cellular networks using Random Neural Networks,” in 2016 Int. Wirel. Commun. Mob. Comput. Conf. IEEE, sep 2016, pp. 351–356.

[121] R. Devi, R. K. Jha, A. Gupta, S. Jain, and P. Kumar, “Implementation of Intrusion Detection System using Adaptive Neuro-Fuzzy Inference System for 5G wireless communication network,” AEU - Int. J. Electron. Commun., vol. 74, pp. 94–106, apr 2017.

[122] A. Li-Eldin, J. van den Berg, and H. A. Ali, “A risk evaluation approach for authorization decisions in social pervasive applications,” Comput. Electr. Eng., vol. 55, pp. 59–72, oct 2016.

[123] M.-I. Kang and J.-W. Kang, “Intrusion detection system using deep neural network for in-vehicle network security,” PLoS One, vol. 11, no. 6, p. e0155781, 2016.

[124] S.-I. Sou and C.-S. Lin, “Random Packet Inspection Scheme for Network Intrusion Prevention in LTE Core Networks.” IEEE Trans. Veh. Technol., pp. 1–1, 2017.

[125] C. Kolias, V. Kolias, and G. Kambourakis, “TermID: A distributed smart intelligence-based approach for wireless intrusion detection,” Int. J. Inf. Secur., vol. 16, no. 4, pp. 401–416, aug 2017.

[126] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, “Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset,” IEEE Commun. Surv. Tutorials, vol. 18, no. 1, pp. 184–208, jan 2016.

[127] Y. Wang, W. Chu, S. Fields, C. Heinemann, and Z. Reiter, “Detection of Intelligent Intruders in Wireless Sensor Networks,” Future Internet, vol. 8, no. 1, p. 2, jan 2016.

[128] S. Anwar, J. Mohamad Zain, M. F. Zolkipli, Z. Inayat, S. Khan, B. Anthony, and V. Chang, “From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions,” Algorithms, vol. 10, no. 2, p. 39, mar 2017.

[129] C. A. R. Houre, “Communicating Sequential Processes,” in Orig. Concord Program. New York, NY: Springer New York, 1978, pp. 413–443.

[130] S. Goldwasser, S. Micali, and C. Rackoff, “The Knowledge Complexity of Interactive Proof Systems,” SIAM J. Comput., vol. 18, no. 1, pp. 186–208, feb 1989.

[131] F. J. Thayer Fábrega, J. C. Herzog, and J. D. Guttman, “Strand spaces: proving security protocols correct,” J. Comput. Secur., vol. 7, no. 2–3, pp. 191–230, apr 1999.

[132] L. Gong, R. Needham, and R. Yahalom, “Reasoning about belief in cryptographic protocols,” in Proceedings. 1990 IEEE Comput. Soc. Symp. Res. Secur. Priv. IEEE, 1990, pp. 234–248.

[133] R. Canetti and H. Krawczyk, “Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels,” in Proc. Int. Conf. Res. Secur. Priv. IEEE, 1990, pp. 234–248.

[134] R. Canetti, H. Krawczyk, and M. Roeder, “Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels,” in Proc. Int. Conf. Res. Secur. Priv. IEEE, 1990, pp. 234–248.

[135] S. Papadopoulos, A. Drosou, N. Dimitriou, O. H. Abdelrahman, G. Gorbil, and D. Tzovaras, “A BRPCA Based Approach for Anomaly Detection in Mobile Networks,” in Inf. Sci. Syst., 2016, pp. 115–125.

[136] S. Santoro, G. Escudero-Andreu, K. G. Kyrakiopoulos, F. J. Aparicio-Navarro, D. J. Parish, and M. Vadursi, “A hybrid intrusion detection system for virtual jamming attacks on wireless networks,” Measurement, vol. 109, pp. 79–87, oct 2017.

[137] R. Canetti and H. Krawczyk, “Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels,” in Proc. Int. Conf. Res. Secur. Priv. IEEE, 1990, pp. 234–248.
2005, p. 112.

[206] L. Harn and Y. Xu, “Design of generalised ElGamal type digital signature schemes based on discrete logarithm,” Electron. Lett., vol. 30, no. 24, pp. 2025–2026, 1994.

[207] S. Khawaja, “Efficient deniable authentication protocol based on generalized ElGamal signature scheme,” Comput. Stand. Interfaces, vol. 26, no. 5, pp. 449–454, sep 2004.

[208] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkovetz, “Extensible authentication protocol (EAP),” Tech. Rep., 2004.

[209] L. J. Blunk, “PPP extensible authentication protocol (EAP),” RFC 2284, 1998.

[210] B. Aboba, H. Levkovetz, D. Simon, and P. Eronen, “Extensible authentication protocol (EAP) key management framework,” RFC 5247, 2008.

[211] “IETF.” [Online]. Available: https://www.ietf.org/rfc.html

[212] R. Arul, G. Raja, K. Kottursamy, P. Sathianarayanan, and S. Venkataraman, “User Path Prediction Based Key Caching and Authentication Mechanism for Broadband Wireless Networks,” Wirel. Pers. Commun., vol. 94, no. 4, pp. 2645–2664, jun 2017.

[213] J. Loughney, M. Nakhiiri, C. Perkins, and R. Koodli, “Context transfer protocol (CXTF),” Tech. Rep., 2005.

[214] C. Neuman, S. Hartman, T. Yu, and K. Raeburn, “The Kerberos network authentication service (N5),” IETF RFC 4120, 2005.

[215] T.-Y. Wu and Y.-M. Tseng, “An efficient user authentication and key exchange protocol for mobile client-server environment,” Comput. Networks, vol. 54, no. 9, pp. 1520–1530, jun 2010.

[216] E.-J. Yoon and K.-Y. Yoo, “A new efficient id-based user authentication and key exchange protocol for mobile client-server environment,” in 2010 IEEE Int. Conf. Wirel. Inf. Technol. Syst., IEEE, aug 2010, pp. 1–4.

[217] J. Lee, S. Ryu, and K. Yoo, “Fingerprint-based remote user authentication scheme using smart cards,” Electron. Lett., vol. 38, no. 12, p. 554, 2002.

[218] C.-H. Lin and Y.-Y. Lai, “A flexible biometrics remote user authentication scheme,” Comput. Stand. Interfaces, vol. 27, no. 1, pp. 19–23, nov 2004.

[219] J. Blasco, T. M. Chen, J. Tapiador, and P. Peris-Lopez, “A Survey of Wearable Biometric Recognition Systems,” ACM Comput. Surv., vol. 49, no. 3, pp. 1–35, sep 2016.

[220] C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” EURASIP J. Inf. Secur., vol. 2011, no. 1, p. 3, dec 2011.

[221] C. Camara, P. Peris-Lopez, and J. E. Tapiador, “Human Identification Using Compressed ECG Signals,” J. Med. Syst., vol. 39, no. 11, p. 148, nov 2015.

[222] ——, “Security and privacy issues in implantable medical devices: A comprehensive survey,” J. Biomed. Inform., vol. 55, pp. 272–289, jun 2015.

[223] A. Jain, S. Prabhakar, L. Hong, and S. Pankanti, “Filterbank-based fingerprint matching,” IEEE Trans. Image Process., vol. 9, no. 5, pp. 846–859, may 2000.

[224] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, “Privacy-Preserving Face Recognition,” in Int. Symp. Priv. Enhancing Technol. Symp., 2009, pp. 235–253.

[225] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, “Efficient Privacy-Preserving Face Recognition,” in Int. Conf. Inf. Secur. Cryptol., 2010, pp. 229–244.

[226] E.-J. Yoon and K.-Y. Yoo, “Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem,” J. Supercomput., vol. 63, no. 1, pp. 235–255, jan 2013.

[227] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, “Cryptanalysis and Improvement of a Biometrics-Based Multi-server Authentication with Key Agreement Scheme,” in Inf. Conf. Comput. Sci. Its Appl., 2012, pp. 391–406.

[228] H.-C. Hsiang and W.-K. Shih, “Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment,” Comput. Stand. Interfaces, vol. 31, no. 6, pp. 1118–1123, nov 2009.