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, deniable authentication with privacy, authentication with mutual anonymity, authentication and key agreement 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. I, 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

(Corresponding author: Mohamed Amine Ferrag)
M. A. Ferrag is with Department of Computer Science, Guelma University, 24000, Algeria, and also with Networks and Systems Laboratory (LRS), Badji Mokhtar-Annaba University, 23000 Annaba, Algeria e-mail: mohamed.amine.ferrag@gmail.com phone: +213661-873-051
L. Maglaras and H. Janicke are with School of Computer Science and Informatics, De Montfort University, Leicester, UK e-mails: {leandros.maglaras, heljanic}@dmu.ac.uk
A. Argyriou and D. Kosmanos are with Department of Electrical and Computer Engineering, University of Thessaly, Greece e-mails: anargyr@gmail.com, dimitriskosmanos@gmail.com
Manuscript received 2017.

TABLE I
THE LEADING PROJECTS FOR 5G

Time	Company	Program
2014	NTT DOCOMO and SK Telecom	Ericsson 5G delivers 5 Gbps speeds [1]
2016	Ericsson and SoftBank	Ericsson and SoftBank completed basic 5G trials on both 15 GHz and 4.5GHz spectrums [2]
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 Networld 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 [3]
2017	Huawei and China Mobile Ltd.	Huawei and China Mobile showcased the 5G 3.5GHz prototype and Ka-Band millimeter wave prototype [4]
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 [5]
2017	AT&T Inc.	AT&T launches Nationwide LTE-M Network for Internet of Things [6]
2017	Nippon Telegraph and Telephone Corporation (NTT)	Toyota and NTT collaborate to promote 5G standardization for automotive vehicles [7]
2017	Huawei and Deutsche Telekom	Huawei and Deutsche Telekom demonstrate the all Cloud 5G network slicing [4]

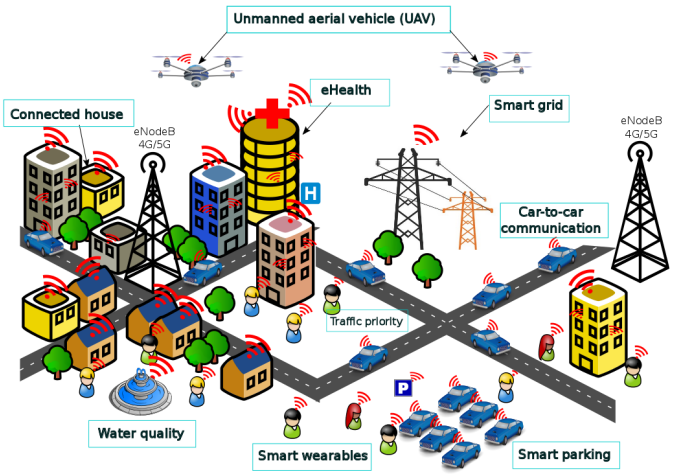

Fig. 1. What will 5G enable?

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 Advenced
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
CXTP	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	UAV	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 devises 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

on 15/01/2017 and continued until the submission date of this paper.

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 models for 4G and 5G cellular networks.
- We provide a classification of 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. V 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

SIM: Scheduling and Interference Mitigation; SP: Security and Privacy; HD: Heterogeneous Deployments; VN: Vehicular Networking; GCN: Green Cellular Networks; STD: Standardization; MIA: Mobile Internet Applications; RC: Random access channel; D2D: Device-to-Device Communication; RMM: Resource & Mobility Management; DO: Data Offloading; HM: Handover Management; SDN: Software-defined networking; US: Unlicensed Spectrum; ENE: Energy; BN: Backhaul network; DNMA: Downlink Non-orthogonal Multiple Access; MIMO: Multiple-Input Multiple-Output technologies; Soc: Social perspective; CC: Cloud Computing; mmWave: millimeter wave communications; Archi: Architecture.

Ref.	SIM	SP	HD	VN	GCN	STD	MIA	RC	RMM	D2D	DO	HM	SDN	US	ENE	BN	DNMA	MIMO	Soc	CC	mmWave	Archi
[11] [12] [13] [14] [15] [8]	√																					
[22] [23] [24] [25] [8] [26] [27]		√																				
[38] [39] [40] [41]			√																			
[42] [43]				√																		
[44] [45] [46]					√																	
[29] [30] [31]						√																
[32]							√															
[47] [8]								√														
[33] [34]									√													
[16] [17] [18] [19] [20] [21]										√												
[48]											√											
[49]												√										
[50] [51]													√									
[52]														√								
[35]															√							
[53] [54]																√						
[55] [56]																	√					
[57] [20] [36]																		√				
[37]																			√			
[58] [59]																				√		
[60]																					√	
[20]																						√

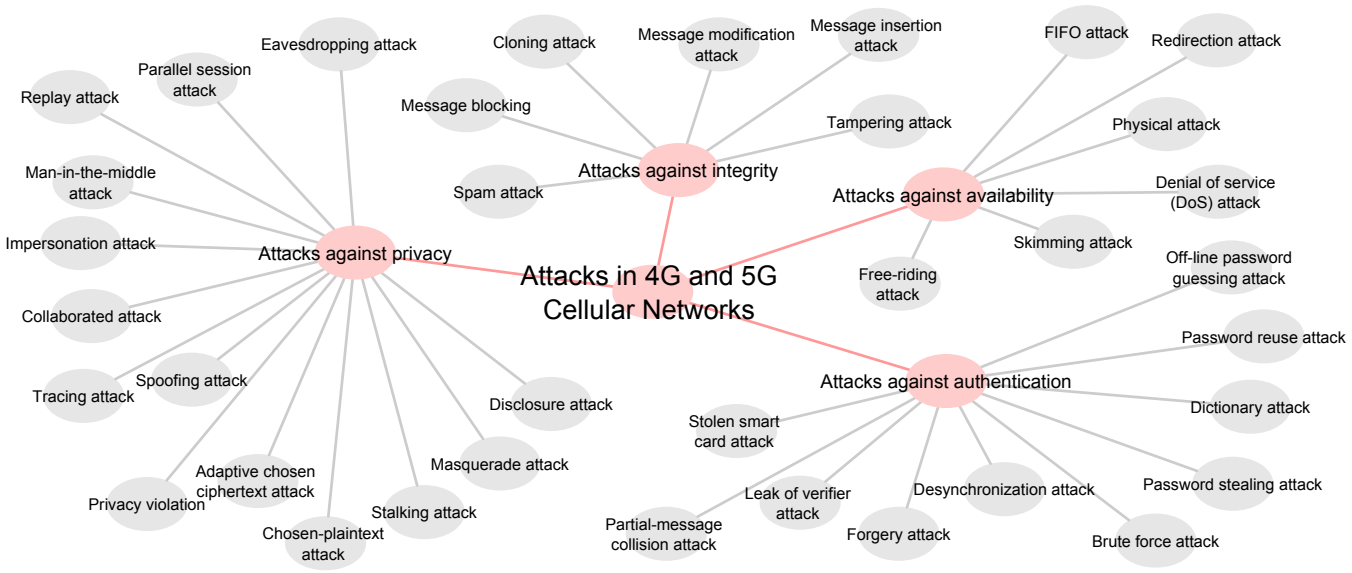

Fig. 2. Classification of attacks in 4G and 5G Cellular Networks

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

Ref.	Year
[26]	2007
[11] [22] [27]	2010
[38]	2011
[44]	2012
[12] [42] [29] [32] [23]	2013
[47] [24] [33] [16] [13] [21] [31]	2014
[45] [17] [48] [49] [14] [34] [60] [20] [59] [36]	2015
[50] [25] [15] [52] [51] [39] [18] [43] [35] [53] [40] [8] [55] [57] [19] [34] [30] [54] [46] [58]	2016
[14] [37] [41] [56]	2017

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.	3G	4G	5G	Authen.	Privacy-preserving	Comments
Park, Y. and Park, T. (2007) [26]	√	X	X	X	X	- Presented some security threats on 4G networks.
Aiash et al. (2010) [27]	√	X	X	0	X	- Reviewed the X.805 standard for the AKA protocol.
Seddigh et al. (2010) [22]	√	X	X	X	X	- Surveyed the security advances for MAC layer in 4G technologies LTE and WiMAX.
Bikos and Sklavos (2013) [23]	0	√	X	X	X	- Presented the cryptographic algorithms for LTE.
Cao et al. (2014) [24]	X	√	X	0	X	- Presented the security architectures and mechanisms specified by the 3GPP standard.
Lichtman et al. (2016) [25]	X	√	X	X	X	- Surveyed the jamming and spoofing mitigation techniques for LTE.
Panwar et al. (2016) [8]	X	X	√	X	X	- Presented the challenges in security and privacy in 5G networks.
Our Work	0	√	√	√	√	- 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. [64] 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 Haddad 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. [67] 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. VIpresents 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. 3.

1) Cryptography methods: Cryptographic methods are the most used by the authentication and privacy preserving

TABLE VI
COUNTERMEASURES USED BY THE AUTHENTICATION AND PRIVACY PRESERVING SCHEMES FOR 4G AND 5G CELLULAR NETWORKS

Countermeasures	Authentication and privacy preserving schemes that use the countermeasure
Secure hash function	[72] , [73], [74], [75], [76], [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87], [88], [89], [90], [91], [92], [93], [62], [94], [63], [64], [95], [96], [65], [97], [98], [99], [100], [66], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [71]
Index-pseudonym	[83]
UMTS-AKA mechanism	[111], [112]
Message Authentication Code (MAC)	[112], [75], [88], [62]
Electronic Product Code (EPC)	[113], [77]
Intrusion Detection Message Exchange Format (IDMEF) and Intrusion Detection Exchange Protocol (IDXP)	[114]
Digital certificate and signature	[74], [71]
Public Key Infrastructure (PKI)	[74], [115], [116] , [97], [98]
Advanced Encryption Standard (AES)	[73]
APFS protocol and Digital signature standard (DSS)	[75]
Password	[76], [79], [85], [86], [91], [92]
Transport Layer Security (TLS)	[76], [116]
Trusted Platform Module (TPM)	[76]
Keyed-Hash Message Authentication Code (HMAC)	[77], [84], [63], [69], [71]
Pseudorandom Number Generator (PRNG)	[117], [83], [105]
Cyclic Redundancy Code (CRC-16)	[117], [105]
Homomorphic Encryption	[109], [118]
Paillier cryptosystem	[109], [118]
Forward security technique	[78]
Error Correction Codes (ECC)	[98], [119]
Anonymous ticket	[120]
Biometrics	[79]
Blind signature and Rabin's public key cryptosystem	[80]
Elliptic Curve Diffie–Hellman protocol (ECDH)	[103], [106], [81], [89]
Bootstrapping Pseudonym (BP), Home Fast Pseudonym (HFP), and Visited Fast Pseudonym (VFP)	[121]
Advanced Identity Management (AIM)	[82]
Physically Unclonable Function (PUF)	[122]
Linear Feedback Shift Register (LFSR)	[122]
Personal Identification Number (PIN)	[111]
Semantic secure symmetric encryption	[78]
Smart cards	[99], [100], [102], [106], [79]
Proxy-signature scheme	[87]
Network domain security (NDS)/IP	[89]
Trusted Node Authentication (TNA)	[90]
Schnorr's signature scheme	[93]
Pseudo-Location Swapping (PLS)	[123]
Symmetric encryption	[62], [96], [69]
Hierarchical identity-based signature	[94]
Mobile vector network protocol	[94]
Hamming weight of vector	[64]
International Mobile Subscriber Identity (IMSI)	[95], [110], [69]
Radio Network Temporary Identities (RNTI)	[95]
Fuzzy extractor	[100], [106]
Certificate revocation	[66]
Group signatures with verifier local revocation	[101]
Group-based access authentication	[124]
Aggregate Message Authentication Codes AMAC	[104], [108]
Designated verifier proxy signature (DVPS)	[110]

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 [74], [115], [116], [97], and [98] use the public key infrastructure (PKI) [125] in order to identify the genuine access point (AP) or base station (BS). Both schemes [109], [118] use the Paillier cryptosystem [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

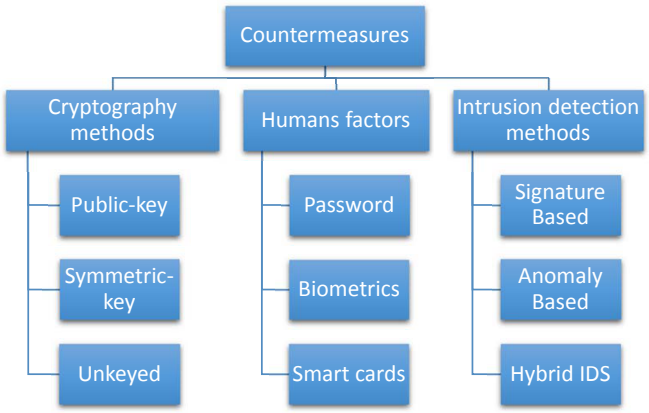

Fig. 3. Classification of countermeasures used by the authentication and privacy preserving schemes for 4G and 5G cellular networks

m be a message to be encrypted, the *encryption* algorithm computes $c = (1+N)^m \cdot r^N \bmod N^2$ 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 $m = \frac{(c.r^{-N} \bmod N^2)-1}{N}$. The scheme [80] uses both Blind signature [127] and Rabin's public key cryptosystem [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 [129] is used by the scheme [101] in order to provide conditional anonymity. Furthermore, Boneh et al. [130] proposed short group signatures due to group signatures based on Strong-RSA are too long for some applications. The digital signature standard (DSS) [131] is used by the PT scheme [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, [62], [96], [69], [78], in order to provide user anonymity. Specifically, Chen et al. [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. [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 [96] can answer this question where he can proved that the strategy of only using symmetric-key techniques to achieve user anonymity is intrinsically infeasible. In addition, Lu et al. [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

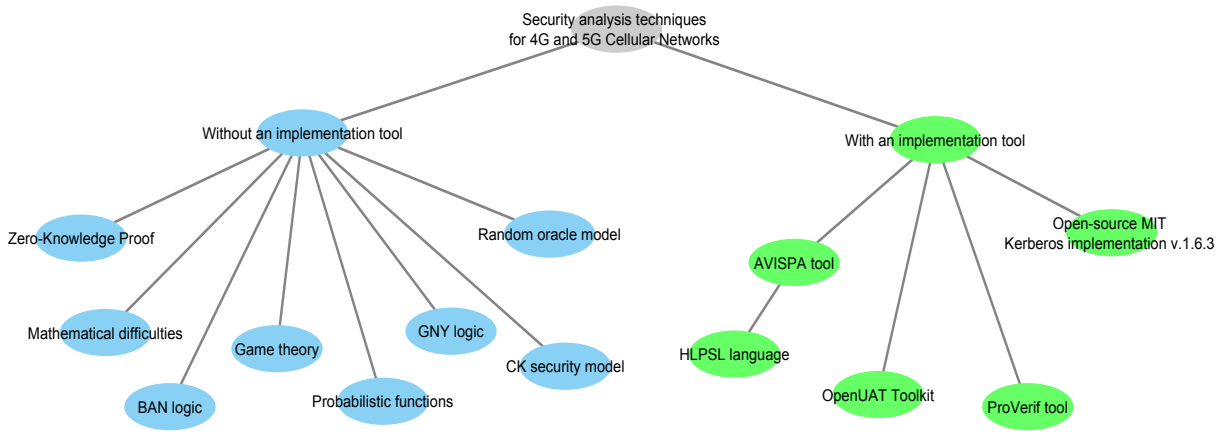

Fig. 4. Classification of security analysis techniques

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 networks. 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 we 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. 6), 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]

TABLE VII
INFORMAL AND FORMAL SECURITY ANALYSIS TECHNIQUES USED IN AUTHENTICATION AND PRIVACY PRESERVING SCHEMES FOR 4G AND 5G CELLULAR NETWORKS

Ref.	Year	Tool	Authentication model to prove	Privacy model to prove	Main results	Implem.
[112]	2007	- Communicating Sequential Processes (CSP) [147]; - Rank Functions;	- Mutual authentication - Biometric authentication	- Data privacy	- Formalize the authentication and key establishment properties of the IDM3G protocol as trace specifications.	No
[75]	2008	- Zero-Knowledge Proof [148]	- User authentication	- Mutual anonymity	- Analyze the anonymity degree of the PT protocol.	No
[115]	2009	- Strand spaces model [149]	- Authentication and Key Agreement	- Confidentiality	- Analyze security performance of the authentication and key agreement protocol.	No
[79]	2009	- GNY logic [150]	- Three-factor authentication - Remote user authentication	- Privacy of the biometric data	- Analyze the completeness of a cryptographic protocol.	No
[81]	2009	- CK security model [151]	- Mutual authentication and key agreement	- N/A	- Prove that the NAKE protocol is probably secure.	No
[121]	2010	- Network Address Identifier (NAI) format [152]	- Fast re-authentication	- Identity privacy	- Test the privacy solution behavior.	No
[82]	2010	- AVISPA tool [153]; - HLPSL language [153];	- Mutual authentication	- Identity privacy	- Prove the efficiency of the identity management mechanism.	Yes
[120]	2011	- Open-source MIT Kerberos implementation v.1.6.3 [154]	- Cross-realm authentication	- Anonymity; - Service access untraceability;	- Evaluate the performance of the enhanced Kerberos protocol.	Yes
[87]	2012	- AVISPA tool [153]; - HLPSL language [153];	- Handover authentication	- N/A	- Show that the scheme can work correctly to achieve robust security properties.	Yes
[88]	2012	- AVISPA tool [153]; - HLPSL language [153];	- Handover authentication	- Identity privacy	- Ensure the security of the handover authentication scheme.	Yes
[92]	2012	- ProVerif [155]	- Identity based authentication	- N/A	- Guarantee the necessary security features claimed by the oPass protocol.	Yes
[93]	2012	- Random oracle model [156]	- Authentication and key agreement	- N/A	- Show that there is an adversary A can construct an algorithm to solve the CDH problem or the k-CAA problem separately.	No
[62]	2013	- Game theory [157]	- Authentication and key agreement	- N/A	- Prove the security of the bipartite protocol by designing a game that turns a CDH instance into the protocol.	No
[63]	2013	- OpenUAT [158]	- Multichannel authentication	- N/A	- Implement some intuitive authentication methods in a common library based.	Yes
[64]	2013	- Probabilistic functions [159]	- RFID authentication	- N/A	- Define formally security models for the LCMQ authentication system.	No
[101]	2015	- ProVerif [155]	- Mutual authentication	- Location privacy	- Verify the system in $\pi - Calculus$ with ProVerif.	Yes
[102]	2015	- ProVerif [155] - Game theory [157]	- Remote user authentication	- Anonymity	- Verify the resistance against known attacks.	Yes
[103]	2015	- Bellare–Rogaway [160]	- Roaming authentication	- Anonymity	- Prove the security of scheme under Elliptic Curve Diffie–Hellman (ECDH) assumption.	No
[161]	2015	- GNY logic [150]	- RFID mutual authentication	- N/A	- Prove the correctness of the LRMAPC protocol.	No
[106]	2015	- BAN logic [162]	- Biometrics-based authentication	- Anonymity	- Demonstrate that the scheme is valid and practical.	No
[108]	2016	- ProVerif [155]	- Group authentication;	- Anonymity; - Unlinkability; - Traceability;	- Verify the secrecy of the real identity.	Yes
[109]	2016	- Mathematical difficulties	- Anonymous authentication	- Location privacy	- Achieve security and privacy using discrete logarithm and computational Diffie-Hellman problems.	No
[163]	2016	- AVISPA tool [153]	- Mutual authentication with key agreement	- Location privacy	- Verify the protocol security against insider attacks and outsider attacks.	Yes
[164]	2016	- AVISPA tool [153]	- Handover authentication	- Anonymity; - Unlinkability; - Traceability; - Non-frameability;	- Show that *Nframe* can maintain the security requirements in frequent handover authentication semantics.	Yes

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,

TABLE VIII
AUTHENTICATION MODELS ACHIEVED BY SECURITY SCHEMES FOR 4G AND 5G CELLULAR NETWORKS

	Authentication models										
Schemes	**Mutual authen.**	**Identity-based authen.**	**Remote user authen.**	**Key agreement**	**RFID authen.**	**Fast re-authen.**	**Three-factor authen.**	**Password-based authen.**	**Deniable authen.**	**Biometric authen.**	**Handover authen.**
[111] [112] [73] [74] [78] [80] [81] [82] [84] [123] [95] [65] [97] [99] [66] [101] [110] [69] [166] [163]	■										
[112] [79] [106]										■	
[167] [113] [77] [117] [119] [122] [83] [64] [98] [161]					■						
[72] [76]									■		
[115] [80] [81] [88] [89] [91] [93] [62] [65] [99] [66] [104] [110] [163]				■							
[79] [100]							■				
[79] [86] [100] [102]			■								
[121]						■					
[85] [96] [107]								■			
[87] [88] [89] [124] [104] [164]											■
[91] [92] [94]		■									

TABLE IX
PRIVACY MODELS ACHIEVED BY SECURITY SCHEMES FOR 4G AND 5G CELLULAR NETWORKS

	Privacy models								
Schemes	**Identity privacy**	**Location privacy**	**Anonymity**	**RFID privacy**	**Untraceability**	**Non-frameability**	**Traceability**	**Conditional privacy**	**Forward privacy**	**Privacy preserving data aggregation**
[108] [164]							■			
[71] [166]								■		
[111] [74] [121] [82] [118] [116] [88] [110] [85]	■									
[164]						■				
[113] [167] [83] [96] [98] [101] [102] [103] [124] [106] [108] [69] [166] [164] [120]			■							
[77] [117] [119]				■						
[78] [83] [84] [68] [123] [98] [101] [109] [163]		■								
[121] [120] [103] [69]					■					
[69]									■	
[66]										■

TABLE X
NOTATIONS USED IN COMPARISON OF COMPUTATIONAL COST AND COMMUNICATION OVERHEAD

Notation	Definition
T_E	The time complexity for exponentiation
T_{SE}	The time complexity for small-exponent exponentiation
T_H	The time complexity for hash function
T_S	The time complexity for symmetric encryption/decryption
T_M	The computation cost of multiplication operation
T_{ECC}	The time complexity for ECC-based scalar multiplication
T_{COM}	The time to upload the encrypted traffic using 5G communication links
T_L	Lagrange component time
e	The cost between the MTC device and the eNB
η	The cost between mobility management entities
n	The number of MTC device
m	The number of groups

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] is 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
See Tab. X for the notations used.

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; + IoT-enabled LTE network; + 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. [96]	- 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 fives 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 : $1T_{SE} + 4T_H + 1T_S$
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.	- Signaling cost : $3n + 5$; - Communication cost : $3en + 4 + \eta$
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 is not considered.	- Computation cost on user side : $3T_M + 7T_H$
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: $(8n + 6\ m)\ T_H + (3n + m)\ T_M$; - 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 pro ling attack, false 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 : $4T_{ECC} + 2T_H + 2T_P + T_M$
Hashem Eiza et al. [166]	-Multi-tier 5G enabled vehicular network with six entites, 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 : $6T_H + 2T_S$; - T_{COM}=13.3s
Hamandi 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 [100].	- Computation cost: $(T_L + T_H + 2T_M)n$
Zhang et al. [103]	- Roaming services in global mobility network	- Roaming authentication	- Anonymity	+ Preserve the non-repudiation, user anonymity, and untraceability; + Provide the perfect forward secrecy; + Prevention of impersonation attacks; - The DoS attack is not considered;	- Computation cost: $4T_M + 4T_H + 10T_S$
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 [87].	- Computation cost on user side : $5T_M$

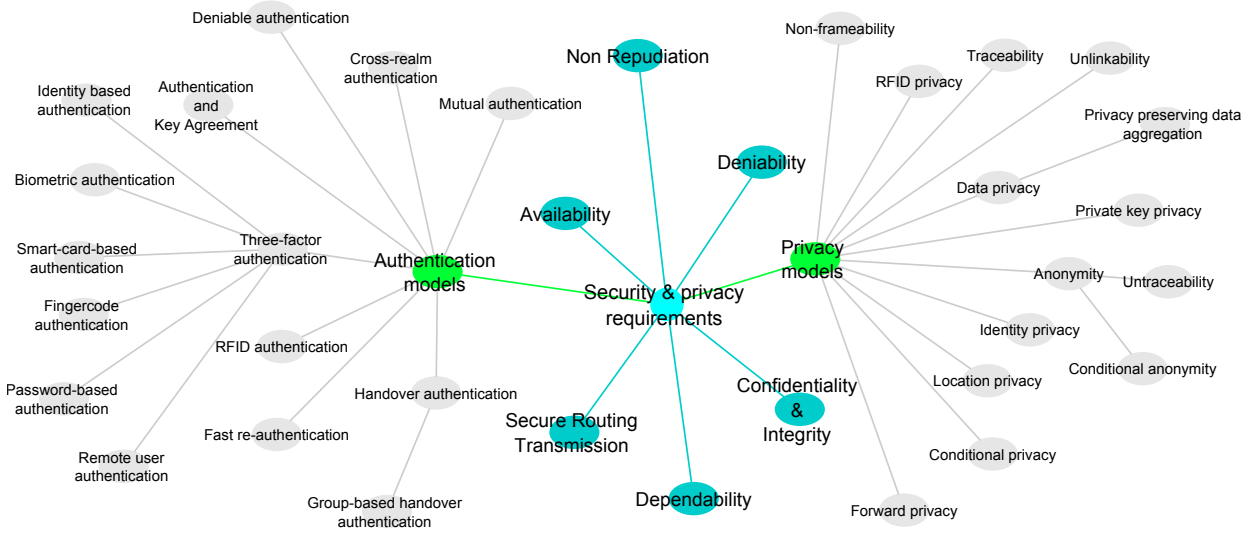

Fig. 5. Categorization of authentication and privacy models

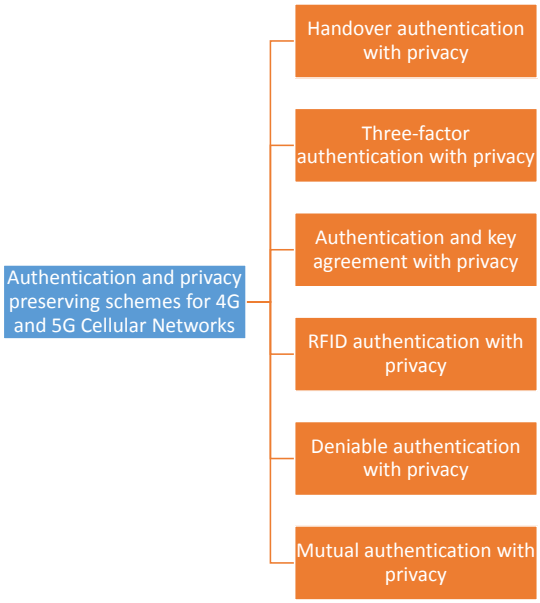

Fig. 6. Classification of authentication and privacy preserving schemes for 4G and 5G Cellular Networks

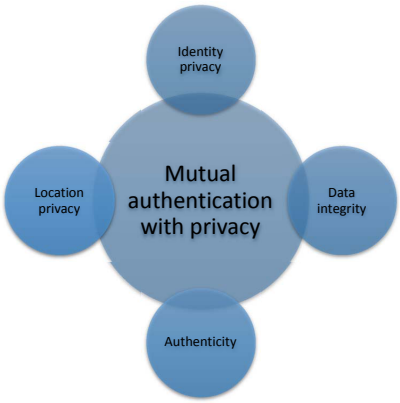

Fig. 7. Classification of mutual authentication with privacy schemes

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/5 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 with 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

is efficient in term 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 IDM3G 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 IDM3G 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 [185] and [186] 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 telecommunications, 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.

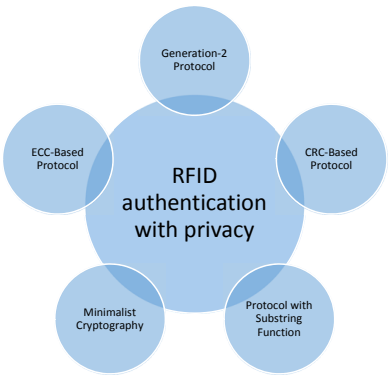

Fig. 8. Classification of RFID authentication protocols with RFID privacy

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 convenience 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 privac1) Generation-2 Protocol, e.g., the Gen2 protocol in [192], 2) CRC-Based Protocol, e.g., the SASI protocol in [167], 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]. Similair 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 an 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 theses 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

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

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, deniability, 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

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. [75] 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 (CXTP) [215]. These schemes are efficient in terms of application handoff service time compared to CXTP, 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

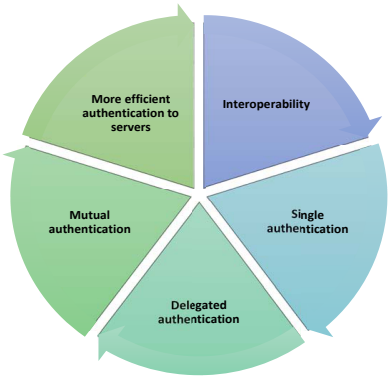

Fig. 10. Different models offered by the Kerberos protocol

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

[100]. 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 term 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 term 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. [81], the SIP protocol does not include any specific security mechanisms. Specifically, Wu et al. [81] proposed a provably secure authentication and key agreement protocol for SIP using elliptic curve cryptography, called NAKE, in order to achieving 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 term 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 type of authentication, including, 1) Bipartite authentication protocol, 2) Tripartite authentication protocol, and 3) Multipartite transitive authentication.

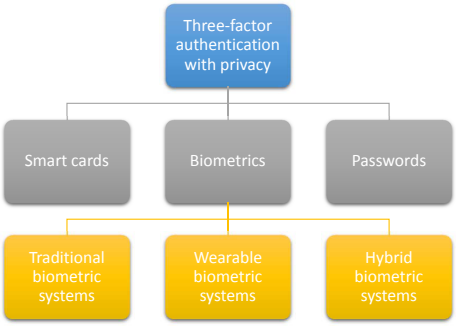

Fig. 11. Classification of three-factor authentication schemes with privacy

Based on three main categories of auxiliary channels, including, *input*, *transfer*, and *verification*, Mayrhofer et al. [63] 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 term of low computation for smart cards

compared 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 biometrics and in the security and privacy issues in implantable medical devices, we refer the reader to the both recent surveys [221] and [224].

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 Fingercode representation introduced in [225], the identification protocol [118] is efficient in term of bandwidth usage compared to both schemes Erkin et al. [226] 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 computation 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 reparable. 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 with 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

Fig. 12. Number of papers vs. Authentication models

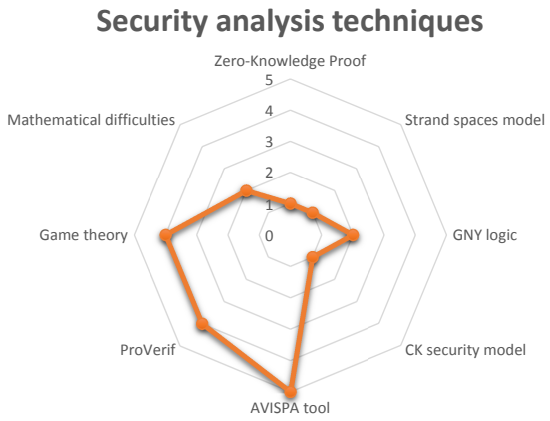

Fig. 13. Number of papers vs. Security analysis techniques

authentication models, namely, proper mutual authentication, session key agreement, RFID authentication, and handover authentication. When security analysis techniques are used, the surveyed schemes use AVISPA tool, ProVerif, Game theory, and GNY logic, as shown in Fig.13 . In addition, the surveyed schemes focus on different areas of privacy models, namely, identity privacy, RFID privacy, untraceability, anonymity, and location privacy, as shown in Fig.14. To complete our overview of authentication and privacy-preserving schemes for 4G and 5G cellular networks, open directions for future research are described below.

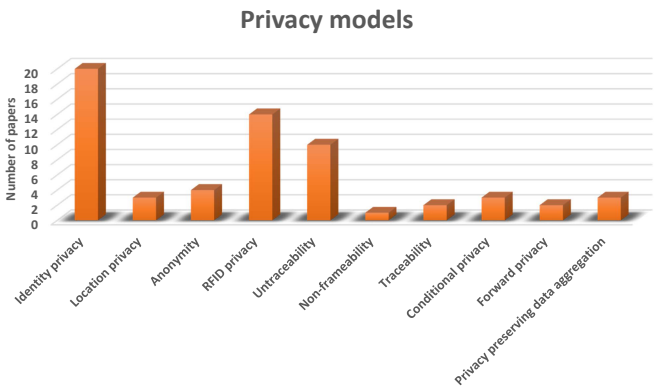

Fig. 14. Number of papers vs. Privacy models

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/2014/7/ericsson-5g-delivers-5-gbps-speeds

[2] "Ericsson Press Releases." [Online]. Available: https://www.ericsson.com/en/press-releases/2017/3/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://www.huawei.com/en/events/mwc/2017/

[5] "Reuters News." [Online]. Available: http://www.reuters.com/article/us-verizon-5g-idUSKBN1611S9

[6] "AT&T Newsroom." [Online]. Available: http://about.att.com/story/att{_}launches{_}lte{_}m{_}network{_}a{_}step{_}forward{_}to{_}5g.html

[7] "NTT Press Releases." [Online]. Available: http://www.ntt.co.jp/news2017/1703e/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, G. 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.

[13] N. Abu-Ali, A.-E. M. Taha, M. Salah, and H. Hassanein, "Uplink Scheduling in LTE and LTE-Advanced: Tutorial, Survey and Evaluation Framework," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1239–1265, jan 2014.

[14] M. Yassin, M. A. AboulHassan, S. Lahoud, M. Ibrahim, D. Mezher, B. Cousin, and E. A. Sourour, "Survey of ICIC techniques in LTE networks under various mobile environment parameters," *Wirel. Networks*, vol. 23, no. 2, pp. 403–418, feb 2017.

[15] M. A. Mehaseb, Y. Gadallah, A. Elhamy, and H. Elhennawy, "Classification of LTE Uplink Scheduling Techniques: An M2M Perspective," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1310–1335, jan 2016.

[16] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-Device Communication in LTE-Advanced Networks: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 1923–1940, jan 2015.

[17] F. Ghavimi and H.-H. Chen, "M2M Communications in 3GPP LTE/LTE-A Networks: Architectures, Service Requirements, Challenges, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 2, pp. 525–549, jan 2015.

[18] P. Gandotra and R. K. Jha, "Device-to-Device Communication in Cellular Networks: A Survey," *J. Netw. Comput. Appl.*, vol. 71, pp. 99–117, aug 2016.

[19] M. Noura and R. Nordin, "A survey on interference management for Device-to-Device (D2D) communication and its challenges in 5G networks," *J. Netw. Comput. Appl.*, vol. 71, pp. 130–150, aug 2016.

[20] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[21] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 86–92, may 2014.

[22] N. Seddigh, B. Nandy, R. Makkar, and J. Beaumont, "Security advances and challenges in 4G wireless networks," in *2010 Eighth Int. Conf. Privacy, Secur. Trust*. IEEE, aug 2010, pp. 62–71.

[23] A. N. Bikos and N. Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks," *IEEE Secur. Priv.*, vol. 11, no. 2, pp. 55–62, mar 2013.

[24] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 283–302, jan 2014.

[25] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 54–61, apr 2016.

[26] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks," in *2007 IEEE Globecom Work.* IEEE, nov 2007, pp. 1–6.

[27] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, "Providing Security in 4G Systems: Unveiling the Challenges," in *2010 Sixth Adv. Int. Conf. Telecommun.* IEEE, 2010, pp. 439–444.

[28] K. David, "Beyond Fifth Generation: Let's Start Talking Sixth Generation [From the Editor]," *IEEE Veh. Technol. Mag.*, vol. 11, no. 4, pp. 3–4, dec 2016.

[29] G. E. M. Zhioua, H. Labiod, N. Tabbane, and S. Tabbane, "LTE Advanced Relaying Standard: A Survey," *Wirel. Pers. Commun.*, vol. 72, no. 4, pp. 2445–2463, oct 2013.

[30] L. Gavrilovska, V. Rakovic, and V. Atanasovski, "Visions Towards 5G: Technical Requirements and Potential Enablers," *Wirel. Pers. Commun.*, vol. 87, no. 3, pp. 731–757, apr 2016.

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

[32] M. Gupta, S. C. Jha, A. T. Koc, and R. Vannithamby, "Energy impact of emerging mobile internet applications on LTE networks: issues and solutions," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 90–97, feb 2013.

[33] D. Xenakis, N. Passas, L. Merakos, and C. Verikoukis, "Mobility Management for Femtocells in LTE-Advanced: Key Aspects and Survey of Handover Decision Algorithms," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 64–91, jan 2014.

[34] T. O. Olwal, K. Djouani, and A. M. Kurien, "A Survey of Resource Management Toward 5G Radio Access Networks," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 1656–1686, jan 2016.

[35] S. Buzzi, C.-L. I, T. E. Klein, H. V. Poor, C. Yang, and A. Zappone, "A Survey of Energy-Efficient Techniques for 5G Networks and Challenges Ahead," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 697–709, apr 2016.

[36] O. Elijah, C. Y. Leow, T. A. Rahman, S. Nunoo, and S. Z. Iliya, "A Comprehensive Survey of Pilot Contamination in Massive MIMOâĂŤ5G System," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 905–923, jan 2016.

[37] S. Singh, N. Saxena, A. Roy, and H. Kim, "A Survey on 5G Network Technologies from Social Perspective," *IETE Tech. Rev.*, vol. 34, no. 1, pp. 30–39, jan 2017.

[38] A. Damnjanovic, J. Montojo, Y. Wei, T. Ji, T. Luo, M. Vajapeyam, T. Yoo, O. Song, and D. Malladi, "A survey on 3GPP heterogeneous networks," *IEEE Wirel. Commun.*, vol. 18, no. 3, pp. 10–21, jun 2011.

[39] D. Liu, L. Wang, Y. Chen, M. Elkashlan, K.-K. Wong, R. Schober, and L. Hanzo, "User Association in 5G Networks: A Survey and an Outlook," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1018–1044, jan 2016.

[40] F. Han, S. Zhao, L. Zhang, and J. Wu, "Survey of Strategies for Switching Off Base Stations in Heterogeneous Networks for Greener 5G Systems," *IEEE Access*, vol. 4, pp. 4959–4973, 2016.

[41] M. Wang, J. Chen, E. Aryafar, and M. Chiang, "A Survey of Client-Controlled HetNets for 5G," *IEEE Access*, vol. 5, pp. 2842–2854, 2017.

[42] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: a survey," *IEEE Commun. Mag.*, vol. 51, no. 5, pp. 148–157, may 2013.

[43] H. Seo, K.-D. Lee, S. Yasukawa, Y. Peng, and P. Sartori, "LTE evolution for vehicle-to-everything services," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 22–28, jun 2016.

[44] L.-C. Wang and S. Rangapillai, "A survey on green 5G cellular networks," in *2012 Int. Conf. Signal Process. Commun.* IEEE, jul 2012, pp. 1–5.

[45] J. Wu, Y. Zhang, M. Zukerman, and E. K.-N. Yung, "Energy-Efficient Base-Stations Sleep-Mode Techniques in Green Cellular Networks: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 2, pp. 803–826, jan 2015.

[46] S. Zhang, Q. Wu, S. Xu, and G. Y. Li, "Fundamental Green Tradeoffs: Progresses, Challenges, and Impacts on 5G Networks," apr 2016.

[47] A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the Random Access Channel of LTE and LTE-A Suitable for M2M Communications? A Survey of Alternatives," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 4–16, jan 2014.

[48] F. Rebecchi, M. Dias de Amorim, V. Conan, A. Passarella, R. Bruno, and M. Conti, "Data Offloading Techniques in Cellular Networks: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 2, pp. 580–603, jan 2015.

[49] G. Gódor, Z. Jakó, Á. Knapp, and S. Imre, "A survey of handover management in LTE-based multi-tier femtocell networks: Requirements, challenges and solutions," *Comput. Networks*, vol. 76, pp. 17–41, jan 2015.

[50] V.-G. Nguyen, T.-X. Do, and Y. Kim, "SDN and Virtualization-Based LTE Mobile Network Architectures: A Comprehensive Survey," *Wirel. Pers. Commun.*, vol. 86, no. 3, pp. 1401–1438, feb 2016.

[51] N. T. Le, M. A. Hossain, A. Islam, D.-y. Kim, Y.-J. Choi, and Y. M. Jang, "Survey of Promising Technologies for 5G Networks," *Mob. Inf. Syst.*, vol. 2016, pp. 1–25, 2016.

[52] R. Bajracharya, R. Shrestha, Y. B. Zikria, and S. W. Kim, "LTE in the Unlicensed Spectrum: A Survey," *IETE Tech. Rev.*, pp. 1–13, nov 2016.

[53] M. Jaber, M. A. Imran, R. Tafazolli, and A. Tukmanov, "5G Backhaul Challenges and Emerging Research Directions: A Survey," *IEEE Access*, vol. 4, pp. 1743–1766, 2016.

[54] R. K. Saha, P. Saengudomlert, and C. Aswakul, "Evolution Toward 5G Mobile Networks - A Survey on Enabling Technologies," *Eng. J.*, vol. 20, no. 1, pp. 87–119, jan 2016.

[55] Z. Wei, J. Yuan, D. W. K. Ng, M. Elkashlan, and Z. Ding, "A Survey of Downlink Non-orthogonal Multiple Access for 5G Wireless Communication Networks," sep 2016.

[56] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-s. Kwak, "Power-Domain Non-Orthogonal Multiple Access (NOMA) in 5G Systems: Potentials and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 2, pp. 721–742, jan 2017.

[57] M. Agiwal, A. Roy, and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 1617–1655, jan 2016.

[58] M. Abu-Lebdeh, J. Sahoo, R. Glitho, and C. W. Tchouati, "Cloudifying the 3GPP IP multimedia subsystem for 4G and beyond: A survey," *IEEE Commun. Mag.*, vol. 54, no. 1, pp. 91–97, jan 2016.

[59] M. Chen, Y. Zhang, L. Hu, T. Taleb, and Z. Sheng, "Cloud-based Wireless Network: Virtualized, Reconfigurable, Smart Wireless Network to Enable 5G Technologies," *Mob. Networks Appl.*, vol. 20, no. 6, pp. 704–712, dec 2015.

[60] Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges," *Wirel. Networks*, vol. 21, no. 8, pp. 2657–2676, nov 2015.

[61] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2027–2051, jan 2016.

[62] Chien-Ming Chen, King-Hang Wang, Tsu-Yang Wu, Jeng-Shyang Pan, and Hung-Min Sun, "A Scalable Transitive Human-Verifiable Authentication Protocol for Mobile Devices," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 8, pp. 1318–1330, aug 2013.

[63] R. Mayrhofer, Fub, and I. Ion, "UACAP: A Unified Auxiliary Channel Authentication Protocol," *IEEE Trans. Mob. Comput.*, vol. 12, no. 4, pp. 710–721, apr 2013.

[64] Z. Li, G. Gong, and Z. Qin, "Secure and Efficient LCMQ Entity Authentication Protocol," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 4042–4054, jun 2013.

[65] B.-L. Chen, W.-C. Kuo, and L.-C. Wuu, "Robust smart-card-based remote user password authentication scheme," *Int. J. Commun. Syst.*, vol. 27, no. 2, pp. 377–389, feb 2014.

[66] Z. Haddad, M. Mahmoud, S. Taha, and I. A. Saroit, "Secure and privacy-preserving AMI-utility communications via LTE-A networks," in *2015 IEEE 11th Int. Conf. Wirel. Mob. Comput. Netw. Commun.* IEEE, oct 2015, pp. 748–755.

[67] J. Yao, T. Wang, M. Chen, L. Wang, and G. Chen, "GBS-AKA: Group-Based Secure Authentication and Key Agreement for M2M in 4G Network," in *2016 Int. Conf. Cloud Comput. Res. Innov.* IEEE, may 2016, pp. 42–48.

[68] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun, "TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 6, pp. 874–887, jun 2013.

[69] N. Saxena, S. Grijalva, and N. S. Chaudhari, "Authentication Protocol for an IoT-Enabled LTE Network," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–20, dec 2016.

[70] J. Li, M. Wen, and T. Zhang, "Group-Based Authentication and Key Agreement With Dynamic Policy Updating for MTC in LTE-A Networks," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 408–417, jun 2016.

[71] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, "SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2659–2672, apr 2016.

[72] W.-B. Lee, C.-C. Wu, and W.-J. Tsaur, "A novel deniable authentication protocol using generalized ElGamal signature scheme," *Inf. Sci. (Ny).*, vol. 177, no. 6, pp. 1376–1381, mar 2007.

[73] F. Bersani and H. Tschofenig, "The EAP-PSK protocol: A pre-shared key extensible authentication protocol (EAP) method," *RFC 4764*, 2007.

[74] Dake He, Jianbo Wang, and Yu Zheng, "User authentication scheme based on self-certified public-key for next generation wireless network," in *2008 Int. Symp. Biometrics Secur. Technol.* IEEE, apr 2008, pp. 1–8.

[75] Li Lu, Jinsong Han, Yunhao Liu, Lei Hu, Jin-Peng Huai, L. Ni, and Jian Ma, "Pseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 10, pp. 1325–1337, oct 2008.

[76] Y.-T. Chen, A. Studer, and A. Perrig, "Combining TLS and TPMs to Achieve Device and User Authentication for Wi-Fi and WiMAX Citywide Networks," in *2008 IEEE Wirel. Commun. Netw. Conf.* IEEE, mar 2008, pp. 2804–2809.

[77] A. X. Liu and L. A. Bailey, "PAP: A privacy and authentication protocol for passive RFID tags," *Comput. Commun.*, vol. 32, no. 7-10, pp. 1194–1199, may 2009.

[78] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, and Xuemin Shen, "A Novel Anonymous Mutual Authentication Protocol With Provable Link-Layer Location Privacy," *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1454–1466, mar 2009.

[79] Chun-I Fan and Yi-Hui Lin, "Provably Secure Remote Truly Three-Factor Authentication Scheme With Privacy Protection on Biometrics," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 4, pp. 933–945, dec 2009.

[80] Haojin Zhu, Xiaodong Lin, Minghui Shi, Pin-Han Ho, and Xuemin Shen, "PPAB: A Privacy-Preserving Authentication and Billing Architecture for Metropolitan Area Sharing Networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 5, pp. 2529–2543, 2009.

[81] L. Wu, Y. Zhang, and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC," *Comput. Stand. Interfaces*, vol. 31, no. 2, pp. 286–291, feb 2009.

[82] M. Abdelkader, M. Hamdi, and N. Boudriga, "A novel advanced identity management scheme for seamless handoff in 4G wireless networks," in *2010 IEEE Globecom Work.* IEEE, dec 2010, pp. 2075–2080.

[83] S. Zhou, Z. Zhang, Z. Luo, and E. C. Wong, "A lightweight anti-desynchronization RFID authentication protocol," *Inf. Syst. Front.*, vol. 12, no. 5, pp. 521–528, nov 2010.

[84] I. Terzis, G. Kambourakis, G. Karopoulos, and C. Lambrinoudakis, "Privacy preserving context transfer schemes for 4G networks," *Wirel. Commun. Mob. Comput.*, vol. 11, no. 2, pp. 289–302, feb 2011.

[85] S. K. Sood, A. K. Sarje, and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," *J. Netw. Comput. Appl.*, vol. 34, no. 2, pp. 609–618, mar 2011.

[86] C.-C. Lee, T.-H. Lin, and R.-X. Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards," *Expert Syst. Appl.*, may 2011.

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

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

[89] Jin Cao, Maode Ma, and Hui Li, "Unified handover authentication between heterogeneous access systems in LTE networks," in *2012 IEEE Glob. Commun. Conf.* IEEE, dec 2012, pp. 5308–5313.

[90] M. J. Sharma and V. C. Leung, "IP Multimedia subsystem authentication protocol in LTE-heterogeneous networks," *Human-centric Comput. Inf. Sci.*, vol. 2, no. 1, p. 16, 2012.

[91] X. Li, Y. Xiong, J. Ma, and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *J. Netw. Comput. Appl.*, vol. 35, no. 2, pp. 763–769, mar 2012.

[92] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 651–663, apr 2012.

[93] D. He, "An efficient remote user authentication and key agreement protocol for mobile client and server environment from pairings," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1009–1016, aug 2012.

[94] H. Liu and M. Liang, "Efficient identity-based hierarchical access authentication protocol for mobile network," *Secur. Commun. Networks*, vol. 6, no. 12, pp. 1509–1521, dec 2013.

[95] U. Jang, H. Lim, and H. Kim, "Privacy-Enhancing Security Protocol in LTE Initial Attack," *Symmetry (Basel).*, vol. 6, no. 4, pp. 1011–1025, dec 2014.

[96] D. Wang, P. Wang, and J. Liu, "Improved privacy-preserving authentication scheme for roaming service in mobile networks," in *2014 IEEE Wirel. Commun. Netw. Conf.* IEEE, apr 2014, pp. 3136–3141.

[97] C.-G. Ma, D. Wang, and S.-D. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," *Int. J. Commun. Syst.*, vol. 27, no. 10, pp. 2215–2227, oct 2014.

[98] Y.-P. Liao and C.-M. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," *Ad Hoc Networks*, vol. 18, pp. 133–146, jul 2014.

[99] S. Kumari, M. K. Khan, and X. Li, "An improved remote user authentication scheme with key agreement," *Comput. Electr. Eng.*, vol. 40, no. 6, pp. 1997–2012, aug 2014.

[100] X. Li, J. Niu, Z. Wang, and C. Chen, "Applying biometrics to design three-factor remote user authentication scheme with key agreement," *Secur. Commun. Networks*, pp. n/a–n/a, apr 2013.

[101] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, "Secure and Privacy-Preserving Smartphone-Based Traffic Information Systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 3, pp. 1428–1438, jun 2015.

[102] S. A. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, and M. K. Khan, "An enhanced privacy preserving remote user authentication scheme with provable security," *Secur. Commun. Networks*, vol. 8, no. 18, pp. 3782–3795, dec 2015.

[103] G. Zhang, D. Fan, Y. Zhang, X. Li, and X. Liu, "A privacy preserving authentication scheme for roaming services in global mobility networks," *Secur. Commun. Networks*, vol. 8, no. 16, pp. 2850–2859, nov 2015.

[104] J. Cao, H. Li, M. Ma, and F. Li, "UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks," in *2015 IEEE Int. Conf. Commun.* IEEE, jun 2015, pp. 7246–7251.

[105] E. Dubrova, M. Naslund, and G. Selander, "CRC-Based Message Authentication for 5G Mobile Technology," in *2015 IEEE Trust.* IEEE, aug 2015, pp. 1186–1191.

[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. 383–393, jan 2015.

[108] A. Fu, 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. Saputro, P. Akula, and K. Akkaya, "Privacy-Preserving Power Injection over a Hybrid AMI/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." *IJ 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." *IJ 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," *Comput. Stand. Interfaces*, vol. 29, no. 2, pp. 254–259, feb 2007.

[114] N. Ulltveit-Moe, V. A. Oleshchuk, and G. M. Køien, "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 SAE 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, "PrivaSIP: 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. Barni, F. Scotti, A. Piva, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, and V. Piuri, "Privacy-preserving fingercode authentication," in *Proc. 12th ACM Work. Multimed. Secur. - MM&Sec '10*. New York, New York, USA: ACM Press, 2010, p. 231.

[119] H.-Y. Chien and C.-S. Laih, "ECC-based lightweight authentication protocol with untraceability for low-cost RFID," *J. Parallel Distrib. Comput.*, vol. 69, no. 10, pp. 848–853, oct 2009.

[120] F. Pereniguez, R. Marin-Lopez, G. Kambourakis, S. Gritzalis, and A. Gomez, "PrivaKERB: A user privacy framework for Kerberos," *Comput. Secur.*, vol. 30, no. 6-7, pp. 446–463, sep 2011.

[121] F. Pereniguez, G. Kambourakis, R. Marin-Lopez, S. Gritzalis, and A. Gomez, "Privacy-enhanced fast re-authentication for EAP-based next generation network," *Comput. Commun.*, vol. 33, no. 14, pp. 1682–1694, sep 2010.

[122] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight Mutual Authentication and Ownership Transfer for RFID Systems," in *2010 Proc. IEEE INFOCOM*. IEEE, 2010, pp. 1–5.

[123] Ben Niu, Xiaoyan Zhu, Haotian Chi, and Hui Li, "3PLUS: Privacy-preserving pseudo-location updating system in location-based services," in *2013 IEEE Wirel. Commun. Netw. Conf.* IEEE, apr 2013, pp. 4564–4569.

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

[125] A. Salomaa, *Public-key cryptography*. Springer Science & Business Media, 2013.

[126] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *Adv. Cryptol. EUROCRYPT '99*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 223–238.

[127] D. Chaum, "Blind Signatures for Untraceable Payments," in *Adv. Cryptol.* Boston, MA: Springer US, 1983, pp. 199–203.

[128] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Massachusetts Institute of Technology (MIT), Tech. Rep., 1979.

[129] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proc. 11th ACM Conf. Comput. Commun. Secur. - CCS '04*. New York, New York, USA: ACM Press, 2004, p. 168.

[130] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," in *Annu. Int. Cryptol. Conf.*, 2004, pp. 41–55.

[131] A. Biryukov, "Digital Signature Standard," in *Encycl. Cryptogr. Secur.* Boston, MA: Springer US, 2011, pp. 347–347.

[132] J. R. Black, *Message authentication codes*. University of California, Davis, 2000.

[133] H. Krawczyk, M. Bellare, and R. Canetti, "RFC2104 - HMAC: Keyed-hashing for message authentication," Tech. Rep., 1997.

[134] J. Katz and A. Y. Lindell, "Aggregate Message Authentication Codes," in *Top. Cryptol. âĂŞ CT-RSA 2008*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 155–169.

[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] D. Santoro, G. Escudero-Andreu, K. G. Kyriakopoulos, 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] 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.

[138] 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.

[139] 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.

[140] A. Ali-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.

[141] M.-J. 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.

[142] 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.

[143] C. Kolias, V. Kolias, and G. Kambourakis, "TermID: a distributed swarm intelligence-based approach for wireless intrusion detection," *Int. J. Inf. Secur.*, vol. 16, no. 4, pp. 401–416, aug 2017.

[144] 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.

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

[146] 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.

[147] C. A. R. Hoare, "Communicating Sequential Processes," in *Orig. Concurr. Program.* New York, NY: Springer New York, 1978, pp. 413–443.

[148] 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.

[149] 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.

[150] 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.

[151] R. Canetti and H. Krawczyk, "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels," in *Int. Conf. Theory Appl. Cryptogr. Tech.*, 2001, pp. 453–474.

[152] A. DeKok, "The network access identifier," *RFC 7542*, 2015.

[153] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron, "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications," in *Int. Conf. Comput. Aided Verif.*, 2005, pp. 281–285.

[154] "MIT Kerberos Distribution." [Online]. Available: https://web.mit.edu/kerberos/

[155] B. Blanchet, "ProVerif: Cryptographic Protocol Verifier Formal Model." [Online]. Available: http://www.proverif.ens.fr/

[156] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *J. ACM*, vol. 51, no. 4, pp. 557–594, jul 2004.

[157] M. H. Manshaei, Q. Zhu, T. Alpcan, T. BacÅ§ar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, pp. 1–39, jun 2013.

[158] R. Mayrhofer, "Towards an Open Source Toolkit for Ubiquitous Device Authentication," in *Fifth Annu. IEEE Int. Conf. Pervasive Comput. Commun. Work.* IEEE, mar 2007, pp. 247–254.

[159] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," in *Secur. pervasive Comput.*, 2004, pp. 201–212.

[160] M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution," in *Adv. Cryptol. CRYPTO' 93*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 232–249.

[161] K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G," *Secur. Commun. Networks*, vol. 9, no. 16, pp. 3095–3104, nov 2016.

[162] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, feb 1990.

[163] K. Hamandi, J. Bou Abdo, I. H. Elhajj, A. Kayssi, and A. Chehab, "A privacy-enhanced computationally-efficient and comprehensive LTE-AKA," *Comput. Commun.*, vol. 98, pp. 20–30, jan 2017.

[164] A. Fu, N. Qin, Y. Wang, Q. Li, and G. Zhang, "Nframe: A privacy-preserving with non-frameability handover authentication protocol based on (t, n) secret sharing for LTE/LTE-A networks," *Wirel. Networks*, apr 2016.

[165] B. Blanchet, "Modeling and verifying security protocols with the applied pi calculus and ProVerif," *Found. Trends{®} Priv. Secur.*, vol. 1, no. 1-2, pp. 1–135, 2016.

[166] M. Hashem Eiza, Q. Ni, and Q. Shi, "Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868–7881, oct 2016.

[167] Hung-Yu Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity," *IEEE Trans. Dependable Secur. Comput.*, vol. 4, no. 4, pp. 337–340, oct 2007.

[168] Huixian Li, Yafang Yang, and Liaojun Pang, "An efficient authentication protocol with user anonymity for mobile networks," in *2013 IEEE Wirel. Commun. Netw. Conf.* IEEE, apr 2013, pp. 1842–1847.

[169] R. Isawa and M. Morii, "Anonymous authentication scheme without verification table for wireless environments," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 95, no. 12, pp. 2488–2492, 2012.

[170] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," *Comput. Commun.*, vol. 34, no. 3, pp. 367–374, mar 2011.

[171] T. Zhou and J. Xu, "Provable secure authentication protocol with anonymity for roaming service in global mobility networks," *Comput. Networks*, vol. 55, no. 1, pp. 205–213, jan 2011.

[172] J. Xu, W.-T. Zhu, and D.-G. Feng, "An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks," *Comput. Commun.*, vol. 34, no. 3, pp. 319–325, mar 2011.

[173] Q. Jing, Y. Zhang, X. Liu, and A. Fu, "An efficient handover authentication scheme with location privacy preserving for EAP-based wireless networks," in *2012 IEEE Int. Conf. Commun.* IEEE, jun 2012, pp. 857–862.

[174] D. He, C. Chen, S. Chan, and J. Bu, "Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions," *IEEE Trans. Wirel. Commun.*, vol. 11, no. 1, pp. 48–53, jan 2012.

[175] J. Cao, M. Ma, and H. Li, "An Uniform Handover Authentication between E-UTRAN and Non-3GPP Access Networks," *IEEE Trans. Wirel. Commun.*, vol. 11, no. 10, pp. 3644–3650, oct 2012.

[176] A. Bohák, L. Buttyán, and L. Dóra, "An authentication scheme for fast handover between WiFi access points," in *Proc. ACM Wirel. Internet Conf.*, 2007.

[177] A. Fu, Y. Zhang, Z. Zhu, and X. Liu, "A Fast Handover Authentication Mechanism Based on Ticket for IEEE 802.16m," *IEEE Commun. Lett.*, vol. 14, no. 12, pp. 1134–1136, dec 2010.

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

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

[180] Jin Cao, Maode Ma, and Hui Li, "A group-based authentication and key agreement for MTC in LTE networks," in *2012 IEEE Glob. Commun. Conf.* IEEE, dec 2012, pp. 1017–1022.

[181] C. Lai, H. Li, R. Lu, and X. S. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Comput. Networks*, vol. 57, no. 17, pp. 3492–3510, dec 2013.

[182] D. He, S. Zeadally, L. Wu, and H. Wang, "Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography," *Comput. Networks*, dec 2016.

[183] S. Cantor, J. Kemp, and Others, "Liberty ID-FF Protocols and Schema Specification," *Version*, vol. 183, pp. 1–2, 2003.

[184] D. P. Kormann and A. D. Rubin, "Risks of the Passport single signon protocol," *Comput. Networks*, vol. 33, no. 1-6, pp. 51–58, jun 2000.

[185] N. Shen, J. Yang, K. Yuan, C. Fu, and C. Jia, "An efficient and privacy-preserving location sharing mechanism," *Comput. Stand. Interfaces*, vol. 44, pp. 102–109, feb 2016.

[186] M. A. Ferrag, M. Nafa, and S. Ghanemi, "EPSA: an efficient and privacy-preserving scheme against wormhole attack on reactive routing for mobile ad hoc social networks," *Int. J. Secur. Networks*, vol. 11, no. 3, p. 107, 2016.

[187] M. A. Ferrag, L. A. Maglaras, H. Janicke, and J. Jiang, "A Survey on Privacy-preserving Schemes for Smart Grid Communications," nov 2016. [Online]. Available: http://arxiv.org/abs/1611.07722

[188] F. Armknecht, J. Girao, A. Matos, and R. L. Aguiar, "Who Said That? Privacy at Link Layer," in *IEEE INFOCOM 2007 - 26th IEEE Int. Conf. Comput. Commun.* IEEE, 2007, pp. 2521–2525.

[189] G. C. Madueno, J. J. Nielsen, D. M. Kim, N. K. Pratas, C. Stefanovic, and P. Popovski, "Assessment of LTE Wireless Access for Monitoring of Energy Distribution in the Smart Grid," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 675–688, mar 2016.

[190] V. Manolopoulos, P. Papadimitratos, S. Tao, and A. Rusu, "Securing smartphone based ITS," in *2011 11th Int. Conf. ITS Telecommun.* IEEE, aug 2011, pp. 201–206.

[191] S. A. Weis, "Security and privacy in radio-frequency identification devices," Ph.D. dissertation, Massachusetts Institute of Technology, 2003.

[192] D. N. Duc, H. Lee, and K. Kim, "Enhancing security of EPCglobal Gen-2 RFID against traceability and cloning," *Auto-ID Labs Inf. Commun. Univ. White Pap.*, 2006.

[193] A. Juels, "Minimalist Cryptography for Low-Cost RFID Tags (Extended Abstract)," in *Int. Conf. Secur. Commun. Networks*, 2005, pp. 149–164.

[194] Y.-z. Li, Y.-b. Cho, N.-k. Um, and S.-h. Lee, "Security and Privacy on Authentication Protocol for Low-cost RFID," in *2006 Int. Conf. Comput. Intell. Secur.* IEEE, nov 2006, pp. 1101–1104.

[195] H.-Y. Chien and C.-W. Huang, "A Lightweight RFID Protocol Using Substring," in *Embed. Ubiquitous Comput.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 422–431.

[196] S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography," in *Proc. 3rd ACM Work. Secur. ad hoc Sens. networks - SASN '05*. New York, New York, USA: ACM Press, 2005, p. 63.

[197] D. Costello, J. Hagenauer, H. Imai, and S. Wicker, "Applications of error-control coding," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2531–2560, 1998.

[198] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estévez-Tapiador, and A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags," in *Proc. 2nd Work. RFID Secur.*, 2006, p. 6.

[199] A. Al Shidhani and V. Leung, "Pre-Authentication Schemes for UMTS-WLAN Interworking," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, no. 1, p. 806563, 2009.

[200] P. Tuyls and L. Batina, "RFID-Tags for Anti-counterfeiting," in *Cryptogr. Track RSA Conf.*, 2006, pp. 115–131.

[201] J. Sun, R. Zhang, X. Jin, and Y. Zhang, "SecureFind: Secure and Privacy-Preserving Object Finding via Mobile Crowdsourcing," *IEEE Trans. Wirel. Commun.*, vol. 15, no. 3, pp. 1716–1728, mar 2016.

[202] X. Zhuang, Y. Zhu, and C.-C. Chang, "A New Ultralightweight RFID Protocol for Low-Cost," *Wirel. Pers. Commun.*, vol. 79, no. 3, pp. 1787–1802, dec 2014.

[203] U. Mujahid, M. Najam-ul Islam, and M. A. Shami, "RCIA: A New Ultralightweight RFID Authentication Protocol Using Recursive Hash," *Int. J. Distrib. Sens. Networks*, vol. 11, no. 1, p. 642180, jan 2015.

[204] H. Luo, G. Wen, J. Su, and Z. Huang, "SLAP: Succinct and Lightweight Authentication Protocol for low-cost RFID system," *Wirel. Networks*, jun 2016.

[205] M. Di Raimondo and R. Gennaro, "New approaches for deniable authentication," in *Proc. 12th ACM Conf. Comput. Commun. Secur. - CCS '05*. New York, New York, USA: ACM Press, 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] Z. Shao, "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. Levkowetz, "Extensible authentication protocol (EAP)," Tech. Rep., 2004.

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

[210] B. Aboba, H. Levkowetz, 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] T. Dierks, "The transport layer security (TLS) protocol version 1.2," *RFC 5246*, 2008.

[213] R. Perez, R. Sailer, L. van Doorn, and Others, "vTPM: virtualizing the trusted platform module," in *Proc. 15th Conf. USENIX Secur. Symp.*, 2006, pp. 305–320.

[214] R. Arul, G. Raja, K. Kottursamy, P. Sathiyanarayanan, and S. Venkatraman, "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.

[215] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli, "Context transfer protocol (CXTP)," Tech. Rep., 2005.

[216] C. Neuman, S. Hartman, T. Yu, and K. Raeburn, "The Kerberos network authentication service (V5)," *IETF RFC 4120*, 2005.

[217] 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.

[218] 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.

[219] 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.

[220] 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.

[221] 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.

[222] 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.

[223] 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.

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

[225] 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.

[226] 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.

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

[228] 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.

[229] 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 *Int. Conf. Comput. Sci. Its Appl.*, 2012, pp. 391–406.

[230] 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.

[231] Y.-P. Liao and S.-S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," *Comput. Stand. Interfaces*, vol. 31, no. 1, pp. 24–29, jan 2009.

[232] Chin-Chen Chang and Jung-San Lee, "An Efficient and Secure Multi-Server Password Authentication Scheme using Smart Cards," in *2004 Int. Conf. Cyberworlds*. IEEE, pp. 417–422.

[233] L. Dang, W. Kou, H. Li, J. Zhang, X. Cao, B. Zhao, and K. Fan, "Efficient ID-based registration protocol featured with user anonymity in mobile IP networks," *IEEE Trans. Wirel. Commun.*, vol. 9, no. 2, pp. 594–604, feb 2010.

[234] V. Scarlata, B. Levine, and C. Shields, "Responder anonymity and anonymous peer-to-peer file sharing," in *Proc. Ninth Int. Conf. Netw. Protoc. ICNP 2001*. IEEE Comput. Soc, pp. 272–280.

[235] A. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Inf. Secur.*, vol. 5, no. 3, p. 145, 2011.

[236] S. Bruce, "Applied cryptography: protocols, algorithms, and source code in C," *New York Wiley*, 1996.

[237] J. Xu, W.-T. Zhu, and D.-G. Feng, "An improved smart card based password authentication scheme with provable security," *Comput. Stand. Interfaces*, vol. 31, no. 4, pp. 723–728, jun 2009.

[238] S. K. Sood, A. K. Sarje, and K. Singh, "An improvement of Xu et al.'s authentication scheme using smart cards," in *Proc. Third Annu. ACM Bangalore Conf. - Comput. '10*. New York, New York, USA: ACM Press, 2010, pp. 1–5.

[239] R. Song, "Advanced smart card based password authentication protocol," *Comput. Stand. Interfaces*, vol. 32, no. 5-6, pp. 321–325, oct 2010.

[240] F. Wen and X. Li, "An improved dynamic ID-based remote user authentication with key agreement scheme," *Comput. Electr. Eng.*, vol. 38, no. 2, pp. 381–387, mar 2012.

[241] Y.-F. Chang, W.-L. Tai, and H.-C. Chang, "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update," *Int. J. Commun. Syst.*, pp. n/a–n/a, may 2013.

[242] S. Kumari, M. K. Gupta, M. K. Khan, and X. Li, "An improved timestamp-based password authentication scheme: comments, cryptanalysis, and improvement," *Secur. Commun. Networks*, vol. 7, no. 11, pp. 1921–1932, nov 2014.

[243] Y.-J. Ku, D.-Y. Lin, C.-F. Lee, P.-J. Hsieh, H.-Y. Wei, C.-T. Chou, and A.-C. Pang, "5g radio access network design with the fog paradigm: Confluence of communications and computing," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 46–52, 2017.

[244] N. Saxena, A. Roy, and H. Kim, "Efficient 5g small cell planning with embms for optimal demand response in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1471–1481, 2017.

[245] A. Brunstrom, K.-J. Grinnemo, J. Taheri *et al.*, "Sdn/nfv-based mobile packet core network architectures: A survey," *IEEE Communications Surveys & Tutorials*, 2017.

[246] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[247] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," *IEEE Communications Magazine*, 2017.

[248] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing based road surface condition monitoring system using fog computing," *IEEE Internet of Things Journal*, 2017.