Journal of Network and Computer Applications 101 (2018) 55–82

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes

Mohamed Amine Ferrag[a,b,*], Leandros Maglaras[c], Antonios Argyriou[d], Dimitrios Kosmanos[d], Helge Janicke[c]

[a] Department of Computer Science, Guelma University, Algeria
[b] Networks and Systems Laboratory (LRS), Badji Mokhtar-Annaba University, Algeria
[c] School of Computer Science and Informatics, De Montfort University, United Kingdom
[d] Department of Electrical and Computer Engineering, University of Thessaly, Greece

ARTICLE INFO

Keywords:
Security
Privacy
Authentication
5G mobile communication
Cryptography

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 cellular networks. 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.

1. 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 (Mukherjee et al., 2017), car-to-car communications (Sun et al., 2010), smart grid (Ferrag and Ahmim, 2017), smart parking, named data networking, blockchain based services, unmanned aerial vehicle (UAV) etc (Niu et al., 2015b). as shown in Fig. 1. Therefore, telecommunications companies believe that the commercialization of 5G will begin in 2020. In Table 1, we list some of the leading projects for 5G cellular networks by various telecommunications companies.

In a 5G environment, the blend different wireless technologies and service providers that share an IP-based core network, will offer the possibility to the mobile devices of switching between providers and technologies, for maintaining a high level 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 (Zhang et al., 2016a, 2016b). 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 (Panwar et al., 2016; Zhang et al., 2015b, 2015a).

As mobile devices will be connected to the network all the time, through the vertical handover, they will obtain a notion of social nodes.

* Corresponding author at: Department of Computer Science, Guelma University, Algeria.
E-mail addresses: mohamed.amine.ferrag@gmail.com (M.A. Ferrag), Leandros.maglaras@dmu.ac.uk (L. Maglaras), dimitriskosmanos@gmail.com (D. Kosmanos), heljanic@dmu.ac.uk (H. Janicke).

https://doi.org/10.1016/j.jnca.2017.10.017
Received 10 August 2017; Received in revised form 8 October 2017; Accepted 28 October 2017
Available online 10 November 2017

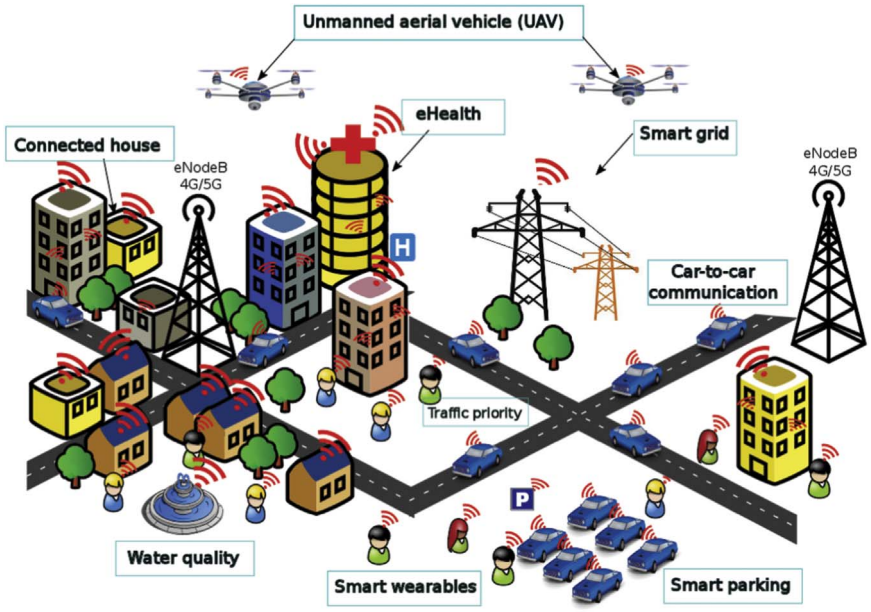

Fig. 1. What will 5G enable?

Table 1
The leading projects for 5G.

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

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 (Ferrag et al., 2017a). 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 (Basaras et al., 2016; Attar et al., 2012; Wang et al., 2012).

For the process of conducting the literature review, we follow the same process conducted by our previous work in Ferrag et al. (2017a). 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.
- 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.

Table 2
Definitions of acronyms and notations.

Acronym	Definition	Acronym	Definition
3GPP	Third Generation Partnership Project	IRS	Intrusion Response System
4G	Fourth-generation mobile network	LTE	Long-Term Evolution
5G	Fifth-generation mobile network	LTE-A	Long-Term Evolution Advanced
AES	Advanced Encryption Standard	M2M	Machine-to-Machine
AIM	Advanced Identity Management	MAC	Message Authentication Code
AKA	Authentication and Key Agreement	MD5	Message Digest 5
AMAC	Aggregate Message Authentication Codes	MIMO	Multiple-Input Multiple-Output
AP	Access point	MITM	Man-in-the-middle
BRPCA	Bayesian Robust Principal Component Analysis	MME	Mobility Management Entity
BS	Base station	MSS	Managed security services
BTS	Base Transceiver Station	MTC	Machine Type Communication
CNN	Controller Area Network	NB	Narrowband
CRC	Cyclic Redundancy Check	NFV	Network Function Virtualization
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

- 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 2 presents the existing surveys for 4G and 5G cellular networks. In Section 3, we provide a classification for the threat models, countermeasures, and various informal and formal security analysis techniques used by the authentication and privacy preserving schemes for 4G and 5G cellular networks. In Section 4, 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 5. Finally, we draw our conclusions in Section 6. Table 2 lists the acronyms and notations used in the paper.

2. 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 cellular networks. These survey articles are categorized as shown in Tables 3 and 4. 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 3. Based on this categorization it is obvious that except from three big categories of articles, one dealing with scheduling and interference mitigation (Kwan and Leung, 2010; Capozzi et al., 2013; Abu-Ali et al., 2014; Yassin et al., 2017; Mehaseb et al., 2016; Panwar et al., 2016), the other with D2D Communication (Liu et al., 2015; Ghavimi and Chen, 2015; Gandotra and Jha, 2016; Noura and Nordin, 2016; Gupta and Jha, 2015; Tehrani et al., 2014) and the third with security and privacy issues (Seddigh et al., 2010; Bikos and Sklavos, 2013; Cao et al., 2014; Lichtman et al., 2016; Panwar et al., 2016; Park and Park, 2007; Aiash et al., 2010), 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, 6G and even 6 G (David, 2016), 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 (Zhioua et al., 2013; Gavrilovska et al., 2016; Andrews et al., 2014), mobile internet applications (Gupta et al., 2013), resource and mobility management (Xenakis et al., 2014; Olwal et al., 2016), energy (Buzzi et al., 2016), MIMO techniques (Olwal et al., 2016; Gupta and Jha, 2015; Elijah et al., 2016), social perspectives (Singh et al., 2017) and so on (See Table 3 for detailed categorization).

Table 3
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; Ar: Architecture.

Ref.	SIM	SP	HD	VN	GCN	STD	MIA	RC	RMM	D2D	DO	HM	SDN	US	ENE	BN	DNMA	MIMO	Soc	CC	mmWave	Ar
Kwan and Leung (2010), Capozzi et al. (2013), Abu-Ali et al. (2014), Yassin et al. (2017), Mehaseb et al. (2016), Panwar et al. (2016)	√																					
Seddigh et al. (2010), Bikos and Sklavos (2013), Cao et al. (2014), Lichtman et al. (2016), Panwar et al. (2016), Park and Park (2007), Aiash et al. (2010)		√																				
Damnjanovic et al. (2011), Liu et al. (2016), Han et al. (2016), Wang et al. (2017)			√																			
Araniti et al. (2013), Seo et al. (2016)				√																		
Wang and Rangapillai (2012), Wu et al. (2015), Zhang et al., (2016c)					√																	
Zhioua et al. (2013), Gavrilovska et al. (2016), Andrews et al. (2014)						√																
Gupta et al. (2013)							√															
Laya et al. (2014), Panwar et al. (2016)								√														
Xenakis et al. (2014), Olwal et al. (2016)									√													
Liu et al. (2015), Ghavimi and Chen (2015), Gandotra and Jha (2016), Noura and Nordin (2016),Gupta and Jha (2015), Tehrani et al. (2014)										√												
Rebecchi et al. (2015)											√											
Gódor et al. (2015)												√										
Nguyen et al. (2016), Le et al. (2016)													√									
Bajracharya et al. (2016)														√								
Buzzi et al. (2016)															√							
Jaber et al. (2016), Saha et al. (2016)																√						
Wei et al., (2016), Islam et al. (2017)																	√					
Agiwal et al. (2016), Gupta and Jha (2015), Elijah et al. (2016)																		√				
Singh et al. (2017)																			√			
Abu-Lebdeh et al. (2016), Chen et al. (2015)																				√		
Niu et al. (2015a)																					√	
Gupta and Jha (2015)																						√

Table 4
Year of publication.

Ref.	Year
Park and Park (2007)	2007
Kwan and Leung (2010), Seddigh et al. (2010), Aiash et al. (2010)	2010
Damnjanovic et al. (2011)	2011
Wang and Rangapillai (2012)	2012
Capozzi et al. (2013), Araniti et al. (2013), Zhioua et al. (2013), Gupta et al. (2013), Bikos and Sklavos (2013)	2013
Laya et al. (2014), Cao et al. (2014), Xenakis et al. (2014), Liu et al. (2015), Abu-Ali et al. (2014), Tehrani et al. (2014), Andrews et al. (2014)	2014
Wu et al. (2015), Ghavimi and Chen (2015), Rebecchi et al. (2015), Gódor et al. (2015), Yassin et al. (2017), Olwal et al. (2016), Niu et al. (2015a), Gupta and Jha (2015), Chen et al. (2015), Elijah et al. (2016)	2015
Nguyen et al. (2016), Lichtman et al. (2016), Mehaseb et al. (2016), Bajracharya et al. (2016), Le et al. (2016), Liu et al. (2016), Gandotra and Jha (2016), Seo et al. (2016), Buzzi et al. (2016), Jaber et al. (2016), Han et al. (2016), Panwar et al. (2016), Wei et al., (2016), Agiwal et al. (2016), Noura and Nordin (2016), Olwal et al. (2016), Gavrilovska et al. (2016), Saha et al. (2016), Zhang et al., (2016c), Abu-Lebdeh et al. (2016)	2016
Yassin et al. (2017), Singh et al. (2017), Wang et al. (2017), Islam et al. (2017)	2017

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 (Seddigh et al., 2010; Bikos and Sklavos, 2013; Cao et al., 2014; Lichtman et al., 2016; Panwar et al., 2016; Park and Park, 2007; Aiash et al., 2010). As it is shown in Table 5 authentication and privacy preservation was only covered partially from Cao et al. (2014) 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.

3. Threat models, countermeasures, and security analysis techniques

3.1. 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) 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. Tables 6–8, present the approaches used in authentication and privacy schemes for detecting and avoiding the replay attack, the Denial of service (DoS) attack, and the forgery attack, respectively.

3.1.1. 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

Table 5
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 and Park (2007)	√	X	X	X	X	- Presented some security threats on 4G networks.
Aiash et al. (2010)	√	X	X	0	X	- Reviewed the X.805 standard for the AKA protocol.
Seddigh et al. (2010)	√	X	X	X	X	- Surveyed the security advances for MAC layer in 4G technologies LTE and WiMAX.
Bikos and Sklavos (2013)	0	√	X	X	X	- Presented the cryptographic algorithms for LTE.
Cao et al. (2014)	X	√	X	0	X	- Presented the security architectures and mechanisms specified by the 3GPP standard.
Lichtman et al. (2016)	X	√	X	X	X	- Surveyed the jamming and spoofing mitigation techniques for LTE.
Panwar et al. (2016)	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.

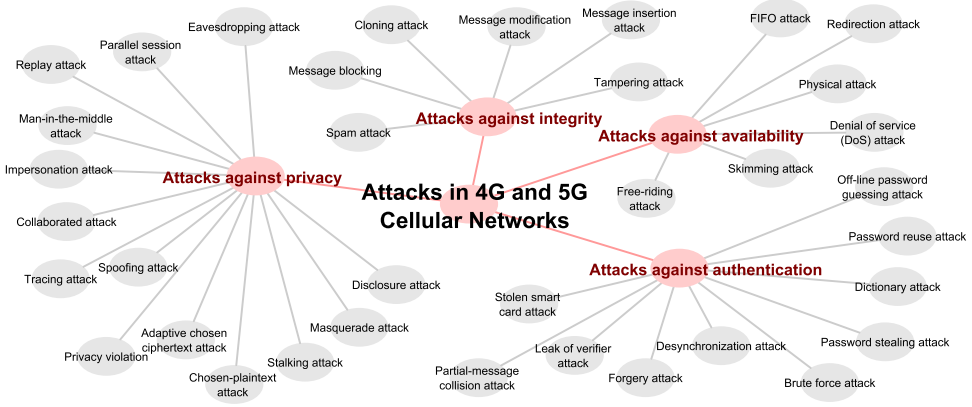

Fig. 2. Classification of attacks in 4G and 5G Cellular Networks.

Table 6
Approaches for detecting and avoiding the replay attack in 4G and 5G cellular networks.

Scheme	Data attacked	Approach
Z. Li et al. (2013); X. Li et al. (2013)	Pretending to be a valid user to login the server by sending messages previously transmitted by a legal user	Hash function with the timestamp
Haddad et al. (2015)	The packets are replayed either by external attacker or LTE-A	The pairing-based message authentication code
Chaudhry et al. (2015)	Replaying the login request	Server signature with the timestamp
Zhang et al. (2015)	Replaying the login request	Authenticated key exchange protocol
Kumari et al. (2014a)	Replaying the blocked login request	The timestamp
Cao et al. (2015)	Replying the messages between the machine type communication devices and the machine type communication server via the 3GPP network domain	The use of the count values (NCC - Next Hop Chaining Counter) and the updating secret values
Fan et al. (2016)	Replaying the login request	Hash function with the timestamp
Cao et al. (2015)	Replying the messages between the machine type communication devices and the machine type communication server	The random numbers
He and Wang (2015)	Personal biometric impression	Hash function with the timestamp

Table 7
Approaches for detecting and avoiding the Denial of service (DoS) attack in 4G and 5G cellular networks.

Scheme	Data attacked	Approach
Kumari et al. (2014a)	The smart card	Checks the correctness of entered identity and password
Chaudhry et al. (2015)	The smart card	Checks the correctness of entered identity and password
Liao and Hsiao (2014)	Jamming the readers with hidden blocker tags	Elliptic curve cryptosystem
Jang et al. (2014)	Requesting the radio network temporary identities	Hash function with the random numbers
Ulltveit-Moe et al. (2011)	Attacking the radio channel, using radio noise or bandwidth consuming attacks.	Intrusion prevention system
Chien and Laih (2009)	Launch a desynchronization attack	Elliptic curve cryptosystem

Table 8
Approaches for detecting and avoiding the forgery attack in 4G and 5G cellular networks.

Scheme	Data attacked	Approach
Z. Li et al. (2013); X. Li et al. (2013)	Forge a valid login request message	Biometrics
Dubrova et al. (2015)	Forge a valid login request message	Cyclic redundancy check
Jiang et al. (2015)	Impersonate as a legitimate user and forges or modifies the authentication messages	Smart-card-based password
Lee et al. (2007)	Forge the valid deniable authentication information	ElGamal signature
Lu et al. (2008)	Forge a valid login request message based on collaborated Attack	Pseudonym-based trust management
Zhou et al. (2010)	Copy or counterfeit a prevailing RFID tag	Two secrets (the secret key and the chip serial number)
Zhang et al. (2015)	Forge a valid login request message	Elliptic curve cryptography
Sood et al. (2011)	Forge a valid login request message	Dynamic identity-based authentication
Chen et al. (2014)	Obtain system secret key and the user password	Smart-card-based password
Liao and Hsiao (2014)	An adversary impersonating a reader or tag is verified as a legitimate object	Elliptic curve cryptography

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. (2016), 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. (2013) proposed an idea that only requires minimum number of human interaction for detecting and avoiding the MITM attack in cellular networks. Mayrhofer et al. (2013) proposed a unified cryptographic authentication protocol framework to use with arbitrary auxiliary channels in order to detect the MITM attack in cellular networks. Based on the combination of learning parity with noise, circulant matrix, and multivariate quadratic, X. Li et al. (2013); Z. Li et al. (2013) 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. (2014) 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. (2015) 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. (2016) 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.

3.1.2. 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.

As discussed by Hasan et al. (2017), the cloning attack is based on a man-in-the-middle rouge BTS with access to the cross-layer information. To conduct the cross-layer attack on the 5G network, the adversary run the following steps: 1) Passive sniffing of downlink and uplink channels, 2) Parsing 5G control messages, 3) Extract cross-layer information, and

4) create attack vectors, such as physical layer Jamming attack or BTS cloning attack. To detecting cloning attack, Dong et al. (2016) proposed a clone detection protocol with fully distributed characteristics, named LSCD. Based on two stages, namely, 1) building witness and 2) clone detection, the LSCD protocol provides strong protection against attacks and a high detection probability. In addition, the LSCD protocol is efficient in terms of energy consumption and detection probability at different distances from the sink, compared to the line-selected multicast protocol in Parno et al. (2005). 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.

3.1.3. 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. (2013) 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. (2016) and Li et al. (2016) proposed the same idea that uses a MAC to maintain the integrity of tracking area identity, while Yao et al. (2016) 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. (2016a, 2016b) can detect the free-riding attack.

3.1.4. 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.

Moreover, Sun et al. (2012) 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.

3.2. Countermeasures

In this subsection, we discuss the countermeasures used by the authentication and privacy preserving schemes for 4G and 5G cellular networks. Table 9 presents all the countermeasures used by the authentication and privacy preserving schemes for 4G and 5G cellular networks. These countermeasures can be classified into three types of categories, including, cryptography methods, humans factors, and intrusion detection methods, as presented in Fig. 3.

3.2.1. Cryptography methods

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

The schemes (He et al., 2008; Deng et al., 2009; Karopoulos et al., 2011; Ma et al., 2014), and (Liao and Hsiao, 2014) use the public key infrastructure (PKI) (Salomaa, 2013) in order to identify the genuine access point (AP) or base station (BS). Both schemes (Mahmoud et al., 2016; Barni et al., 2010) use the Paillier cryptosystem (Paillier, 1999), which is based on three algorithms, namely, *generation of keys*, *encryption*, and *decryption*. The *generation of keys* is based on two large, independent and random prime numbers: p and q. Let m be a message to be encrypted, the *encryption* algorithmcomputes $c = (1+N)^m \cdot r^N \mathrm{mod} N^2$ where $0 \leq m < N$, r is a random integer $0 < r < N$, and the public key $N = p \cdot q$. To find the clear text m, the *decryption* algorithmcomputes $m = \frac{(c \cdot r^{-N} \mathrm{mod}\, N^2) - 1}{N}$. The scheme (Zhu et al., 2009) uses both Blind signature (Chaum, 1983) and Rabin's public key cryptosystem (Rabin, 1979). 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 (Boneh and Shacham, 2004) is used by the scheme (Gisdakis et al., 2015) in order to provide conditional anonymity. Furthermore, Boneh et al. (2004) proposed short group signatures due to group signatures based on Strong-RSA are too long for some applications. The digital signature standard (DSS) (Biryukov, 2011) is used by the PT scheme (Lu et al., 2008) in order to provide confidentiality and integrity to data exchanges after authentication as well as to simplify the key exchange protocol. According to Wang et al. (2015), wireless channel reciprocity based key establishment can be classified into three categories, namely, 1) Quantization, 2) Reconciliation and privacy amplification, and 3) Feasibility and security.

The symmetric encryption is used by four schemes, namely, (Chen et al., 2013; Wang et al., 2014; Saxena et al., 2016; Lu et al., 2009), in order to provide user anonymity. Specifically, Chen et al. (2013) 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. (2016) 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 Wang et al. (2014) 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. (2009) 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 three popular methods, namely, the Message Authentication Code (MAC) (Black, 2000), the Keyed-Hash Message Authentication Code (HMAC) (Krawczyk et al., 1997), and the Aggregate Message Authentication Codes (AMAC) (Katz and Lindell, 2008).

3.2.2. Humans factors

The humans' factors-based countermeasures are proposed to ensure authentication. The research community has proposed three

Table 9
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	Lee et al. (2007),Bersani and Tschofenig (2007),He et al. (2008),Lu et al. (2008),Chen et al. (2008),Liu and Bailey (2009),Lu et al. (2009),Fan and Lin (2009),Zhu et al. (2009),Wu et al. (2009),Abdelkader et al. (2010),Zhou et al. (2010),Terzis et al. (2011),Sood et al. (2011),Lee et al., (2011),Cao et al. (2012b),Fu et al. (2012),Cao et al. (2012),Sharma and Leung (2012),Li et al. (2012),Sun et al. (2012),He (2012),Chen et al. (2013),Liu and Liang (2013),Mayrhofer et al. (2013),Li et al. (2013a, 2013b),Jang et al. (2014),Wang et al. (2014),Chen et al. (2014),Ma et al. (2014),Liao and Hsiao (2014),Kumari et al. (2014a), Li et al. (2013a, 2013b),Haddad et al. (2015),Gisdakis et al. (2015),Chaudhry et al. (2015),Zhang et al. (2015),Cao et al. (2015),Dubrova et al. (2015),He and Wang (2015),Jiang et al. (2015),Fu et al. (2016a),Mahmoud et al. (2016),Ramadan et al. (2016),Zhang et al. (2016a, 2016b)
Index-pseudonym	Zhou et al. (2010)
UMTS-AKA mechanism	Dimitriadis and Polemi (2006),Dimitriadis and Shaikh (2007)
Message Authentication Code (MAC)	Dimitriadis and Shaikh (2007),Lu et al. (2008),Fu et al. (2012),Chen et al. (2013)
Electronic Product Code (EPC)	Chien and Chen (2007),Liu and Bailey (2009)
Intrusion Detection Message Exchange Format (IDMEF) and Intrusion Detection Exchange Protocol (IDXP)	Ulltveit-Moe et al. (2011)
Digital certificate and signature	He et al. (2008),Zhang et al. (2016a, 2016b)
Public Key Infrastructure (PKI)	He et al. (2008),Deng et al. (2009),Karopoulos et al. (2011),Ma et al. (2014),Liao and Hsiao (2014)
Advanced Encryption Standard (AES)	Bersani and Tschofenig (2007)
APFS protocol and Digital signature standard (DSS)	Lu et al. (2008)
Password	Chen et al. (2008),Fan and Lin (2009),Sood et al. (2011),Lee et al., (2011),Li et al. (2012),Sun et al. (2012)
Transport Layer Security (TLS)	Chen et al. (2008); Karopoulos et al. (2011)
Trusted Platform Module (TPM)	Chen et al. (2008)
Keyed-Hash Message Authentication Code (HMAC)	Liu and Bailey (2009),Terzis et al. (2011),Mayrhofer et al. (2013),Saxena et al. (2016),Zhang et al. (2016a, 2016b)
Pseudorandom Number Generator (PRNG)	Sun and Ting (2009),Zhou et al. (2010),Dubrova et al. (2015)
Cyclic Redundancy Code (CRC–16)	Sun and Ting (2009),Dubrova et al. (2015)
Homomorphic Encryption	Mahmoud et al. (2016),Barni et al. (2010)
Paillier cryptosystem	Mahmoud et al. (2016),Barni et al. (2010)
Forward security technique	Lu et al. (2009)
Error Correction Codes (ECC)	Liao and Hsiao (2014),Chien and Laih (2009)
Anonymous ticket	Pereniguez et al. (2011)
Biometrics	Fan and Lin (2009)
Blind signature and Rabin's public key cryptosystem	Zhu et al. (2009)
Elliptic Curve Diffie–Hellman protocol (ECDH)	Zhang et al. (2015),He and Wang (2015),Wu et al. (2009),Cao et al. (2012)
Bootstrapping Pseudonym (BP), Home Fast Pseudonym (HFP), and Visited Fast Pseudonym (VFP)	Pereniguez et al. (2010)
Advanced Identity Management (AIM)	Abdelkader et al. (2010)
Physically Unclonable Function (PUF)	Kulseng et al. (2010)
Linear Feedback Shift Register (LFSR)	Kulseng et al. (2010)
Personal Identification Number (PIN)	Dimitriadis and Polemi (2006)
Semantic secure symmetric encryption	Lu et al. (2009)
Smart cards	Kumari et al. (2014a),Li et al. (2013a, 2013b), Chaudhry et al. (2015),He and Wang (2015), Fan and Lin (2009)
Proxy-signature scheme	Cao et al. (2012b)
Network domain security (NDS)/IP	Cao et al. (2012)
Trusted Node Authentication (TNA)	Sharma and Leung (2012)
Schnorr's signature scheme	He (2012)
Pseudo-Location Swapping (PLS)	Niu et al. (2013)
Symmetric encryption	Chen et al. (2013),Wang et al. (2014),Saxena et al. (2016)
Hierarchical identity-based signature	Liu and Liang (2013)
Mobile vector network protocol	Liu and Liang (2013)
Hamming weight of vector	Li et al. (2013a, 2013b)
International Mobile Subscriber Identity (IMSI)	Jang et al. (2014), Ramadan et al. (2016), Saxena et al. (2016)
Radio Network Temporary Identities (RNTI)	Jang et al. (2014)
Fuzzy extractor	Li et al. (2013a, 2013b); He and Wang (2015)
Certificate revocation	Haddad et al. (2015)
Group signatures with verifier local revocation	Gisdakis et al. (2015)
Group-based access authentication	Cao et al. (2015)
Aggregate Message Authentication Codes AMAC	Cao et al. (2015),Fu et al. (2016a)
Designated verifier proxy signature (DVPS)	Ramadan et al. (2016)

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.

3.2.3. 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 Papadopoulos et al. (2016) authors propose a novel IDS based on Bayesian Robust Principal Component Analysis (BRPCA).

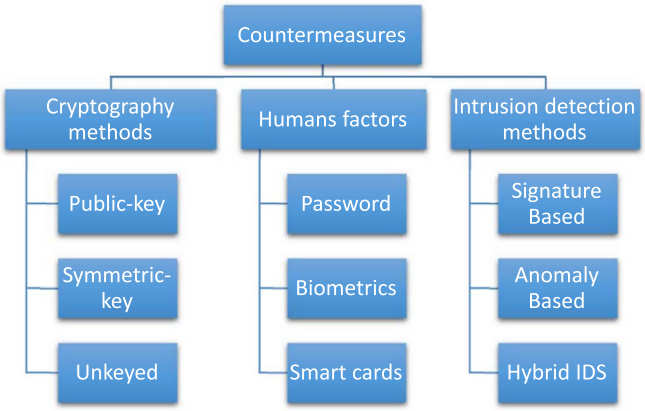

Fig. 3. Classification of countermeasures used by the authentication and privacy preserving schemes for 4G and 5G cellular networks.

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 Santoro et al. (2017) 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 Gupta et al. (2017) 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 Casas et al. (2016) 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 Devi et al. (2017) 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 (Ali-Eldin et al., 2016). Authors evaluated their method against DOS attacks, like the previous methods in Papadopoulos et al. (2016), Santoro et al. (2017), Gupta et al. (2017), Casas et al. (2016) 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 Kang and Kang (2016). Authors in Kang and Kang (2016) 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 Sou and Lin (2017) 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 Kolias et al. (2017) 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 (Kolias et al., 2016). The proposed method achieves both low network footprint and user privacy. Taking in mind privacy along with security, authors in Ulltveit-Moe et al. (2011) 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 Wang et al. (2016) 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 Anwar et al. (2017) 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.

3.3. 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, Table 10. 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 (Goldwasser et al.,

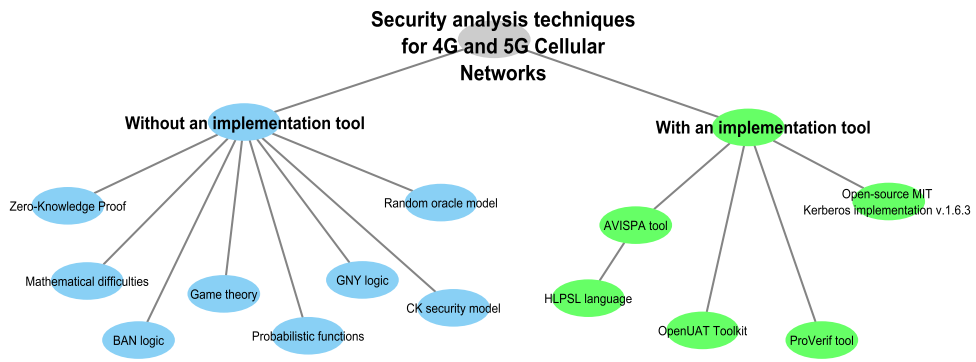

Fig. 4. Classification of security analysis techniques.

Table 10
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.
Dimitriadis and Shaikh (2007)	2007	- Communicating Sequential Processes (CSP) Hoare (1978); - Rank Functions;	- Mutual authentication - Biometric authentication	- Data privacy	- Formalize the authentication and key establishment properties of the IDM3G protocol as trace specifications.	No
Lu et al. (2008)	2008	- Zero-Knowledge Proof Goldwasser et al. (1989)	- User authentication	- Mutual anonymity	- Analyze the anonymity degree of the PT protocol.	No
Deng et al. (2009)	2009	- Strand spaces model Thayer Fábrega et al. (1999)	- Authentication and Key Agreement	- Confidentiality	- Analyze security performance of the authentication and key agreement protocol.	No
Fan and Lin (2009)	2009	- GNY logic Gong et al. (1990)	- Three-factor authentication - Remote user authentication	- Privacy of the biometric data	- Analyze the completeness of a cryptographic protocol.	No
Wu et al. (2009)	2009	- CK security model Canetti and Krawczyk (2001)	- Mutual authentication and key agreement	- N/A	- Prove that the NAKE protocol is probably secure.	No
Pereniguez et al. (2010)	2010	- Network Address Identifier (NAI) format DeKok (2005)	- Fast re-authentication	- Identity privacy	- Test the privacy solution behavior.	No
Abdelkader et al. (2010)	2010	- AVISPA tool Armando et al. (2005); - HLPSL language Armando et al. (2005);	- Mutual authentication	- Identity privacy	- Prove the efficiency of the identity management mechanism.	Yes
Pereniguez et al. (2011)	2011	- Open-source MIT Kerberos implementation v.1.6.3 Kerberos Distribution (2017)	- Cross-realm authentication	- Anonymity; - Service access untraceability;	- Evaluate the performance of the enhanced Kerberos protocol.	Yes
Cao et al. (2012b)	2012	- AVISPA tool Armando et al. (2005); - HLPSL language Armando et al. (2005);	- Handover authentication	- N/A	- Show that the scheme can work correctly to achieve robust security properties.	Yes
Fu et al. (2012)	2012	- AVISPA tool Armando et al. (2005); - HLPSL language Armando et al. (2005);	- Handover authentication	- Identity privacy	- Ensure the security of the handover authentication scheme.	Yes
Sun et al. (2012)	2012	- ProVerif Blanchet (2016b)	- Identity based authentication	- N/A	- Guarantee the necessary security features claimed by the oPass protocol.	Yes
He (2012)	2012	- Random oracle model Canetti et al. (2004)	- 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
Chen et al. (2013)	2013	- Game theory Manshaei et al. (2013)	- 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
Mayrhofer et al. (2013)	2013	- OpenUAT Mayrhofer (2007)	- Multichannel authentication	- N/A	- Implement some intuitive authentication methods in a common library based.	Yes
Li et al. (2013a, (2013b)	2013	- Probabilistic functions Weis et al. (2004)	- RFID authentication	- N/A	- Define formally security models for the LCMQ authentication system.	No
Gisdakis et al. (2015)	2015	- ProVerif Blanchet (2016b)	- Mutual authentication	- Location privacy	- Verify the system in $\pi - Calculus$ with ProVerif.	Yes
Chaudhry et al. (2015)	2015	- ProVerif Blanchet (2016b) - Game theory Manshaei et al. (2013)	- Remote user authentication	- Anonymity	- Verify the resistance against known attacks.	Yes
Zhang et al. (2015)	2015	- Bellare–Rogaway Bellare and Rogaway (1993)	- Roaming authentication	- Anonymity	- Prove the security of scheme under Elliptic Curve Diffie–Hellman (ECDH) assumption.	No
Fan et al. (2016)	2015	- GNY logic Gong et al. (1990)	- RFID mutual authentication	- N/A	- Prove the correctness of the LRMAPC protocol.	No
He and Wang (2015)	2015	- BAN logic Burrows et al. (1990)	- Biometrics-based authentication	- Anonymity	- Demonstrate that the scheme is valid and practical.	No
Fu et al. (2016a)	2016	- ProVerif Blanchet (2016b)	- Group authentication;	- Anonymity; - Unlinkability; - Traceability;	- Verify the secrecy of the real identity.	Yes
Mahmoud et al. (2016)	2016	- Mathematical difficulties	- Anonymous authentication	- Location privacy	- Achieve security and privacy using discrete logarithm and computational Diffie-Hellman problems.	No
Hamandi et al. (2017)	2016	- AVISPA tool Armando et al. (2005)	- Mutual authentication with key agreement	- Location privacy	- Verify the protocol security against insider attacks and outsider attacks.	Yes
Fu et al., (2016b)	2016	- AVISPA tool Armando et al. (2005)	- Handover authentication	- Anonymity; - Unlinkability; - Traceability; - Non-frameability;	- Show that *Nframe* can maintain the security requirements in frequent handover authentication semantics.	Yes

1989), Mathematical difficulties, GNY logic (Gong et al., 1990), CK security model (Canetti and Krawczyk, 2001), Random oracle model (Canetti et al., 2004), Game theory (Manshaei et al., 2013), Probabilistic functions (Weis et al., 2004), and BAN logic (Burrows et al., 1990). To analyze the completeness of a cryptographic protocol, both schemes (Fan et al., 2016) and (Fan and Lin, 2009) use the GNY logic (Gong et al., 1990). The scheme (He, 2012) use random oracle model (Canetti et al., 2004) 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 (He and Wang, 2015) uses the BAN logic (Burrows et al., 1990) to demonstrate that the scheme is valid and practical. The mathematical difficulties is used by the scheme (Mahmoud et al., 2016) to achieve security and privacy using discrete logarithm and computational Diffie-Hellman problems. Furthermore, the game theory (Manshaei et al., 2013) is used by the scheme (Chen et al., 2013) 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. (2013), 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 (Armando et al., 2005), Open-source MIT Kerberos implementation v.1.6.3 (Kerberos Distribution, 2017), OpenUAT (Mayrhofer, 2007), and ProVerif (Blanchet, 2016b). The Open-source MIT Kerberos (Kerberos Distribution, 2017) is used especially for evaluate the performance of the enhanced Kerberos protocol such as the scheme (Pereniguez et al., 2011). The OpenUAT (Mayrhofer, 2007) is used by the scheme (Mayrhofer et al., 2013) 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 (Fu et al., 2016a; Chaudhry et al., 2015; Gisdakis et al., 2015), and (Gisdakis et al., 2015) use the ProVerif (Blanchet, 2016b), 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 Blanchet (2016a). Therefore, five schemes (Hamandi et al., 2017; Fu et al., 2016b; Cao et al., 2012b; Fu et al., 2012), and (Abdelkader et al., 2010) use the AVISPA tool (Armando et al., 2005) based on the HLPSL language (Armando et al., 2005) to verify the security of these schemes against insider attacks and outsider attacks.

4. 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, Tables 11, 12. 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*. Table 14 summarizes the authentication and privacy preserving schemes for 4G and 5G Cellular Networks.

4.1. 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. (2012b), 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 (Cao et al., 2012b) provide several security features, including, perfect forward and backward secrecy. In addition, the scheme (Cao et al., 2012b) is efficient in terms of computational cost and communication overhead compared with the handover scheme in Bohák et al. (2007), but the identity privacy is not considered. Similar to the scheme (Cao et al., 2012b) 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 (Cao et al., 2012) is efficient in terms of computational cost, communication cost, and storage cost. As a matter of fact, these both two schemes (b, 2012) do not consider the identity and location privacy. To solve this problem, the idea of Gao et al. (2013) can be applied with both schemes (Cao et al., 2012b) and (Cao et al., 2012).

IEEE 802.16 m is proposed as an advanced air interface to meet the requirements of the fourth generation (4G) systems. To preserves the identity privacy for IEEE 802.16 m network, Fu et al. (2012) proposed a privacy-preserving fast handover authentication scheme based on the pseudonym. Based on the 3-way handshake procedure, the scheme (Fu et al., 2012) can achieve the following research objectives, including, 1) Fast handover, 2) Mutual authentication and key agreement, and 3) Privacy preservation. In addition, the scheme (Fu et al., 2012) is efficient in terms of computation and communication overhead compared with Fu et al. scheme (Fu et al., 2010). The scheme (Fu et al., 2012) 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. (2013) 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 (Niu et al., 2013).

To provide the security key derivation and anonymity for all of the mobility scenarios in LTE-A networks, Cao et al. (2015) 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 (Lai et al., 2014). Using software-defined networking, Duan and Wang (2015) proposed an authentication handover scheme with privacy protection in 5G heterogeneous network communications. Recently, Fu et al. (2016a) proposed a novel group authentication protocol with privacy-preserving to provide unlinkability and traceability in 4G/5 communications. The scheme (Fu et al., 2016a) is efficient in terms of the signaling overhead and computation overhead compared to two schemes, including, Cao's scheme (Cao et al., 2012) and SE-AKA (Lai et al., 2013). To fit in with all of the mobility scenarios in the LTA/LTA-A networks, Fu et al. (2016b) 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

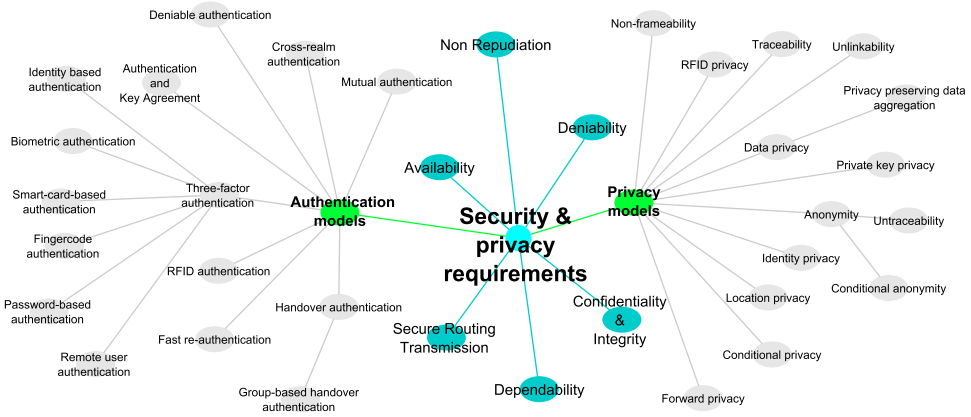

Fig. 5. Categorization of authentication and privacy models.

communication overhead compared to three schemes, namely, HALP scheme (Jing et al., 2012), Pair-Hand scheme (He et al., 2012), and UHAEN scheme (Cao et al., 2012a), but the perfect forward and backward secrecy are not considered compared to the scheme (Cao et al., 2012b). 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 et al. (2016).

4.2. 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) 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 (Cantor, 2003; Kormann and Rubin, 2000), but the location privacy is not considered. Similar to the IDM3G protocol, Dimitriadis and Shaikh (2007) 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 (Dimitriadis and Polemi, 2006). He et al. (2008) proposed three categories of authentication scenarios for the 4G system. The main idea of He et al. (2008) is the use of *Self-Certified Public-Key*, which need not be accompanied by a separate digital certificate. The advantage of the protocol (He et al., 2008) 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. (2009), 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 ideas in Shen et al. (2016), Ferrag et al. (2016a), and Zhou et al. (2015a) 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 Ferrag et al. (2017a, 2016b). To the best of our knowledge, Lu et al. (2009) 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 (Lu et al., 2009) is efficient in terms of the packet delay time and the total packet time cost compared with the protocol (Armknecht et al., 2007). On the other hand, mutual authentication with identity privacy can also be preserved using the identity management mechanism proposed by Abdelkader et al. (2010). 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. (2016), the EPS-AKA protocol of the LTE network does not support Internet of Things (IoT) (Ferrag et al., 2017b). 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. (2011), 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. (2014) proposed an authentication protocol to safely transmit identification parameters in different cases of the initial attach under 4G mobile communications.

According to Madueno et al. (2016), 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. (2015) proposed a privacy-preserving scheme to secure the communications of an automatic metering infrastructure via LTE-A networks. To share keys, the scheme (Haddad et al., 2015) uses a key agreement protocol between the smart meters, the utility company, and the LTE network. The scheme (Haddad et al., 2015) 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. (2016) 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 (Gisdakis et al., 2015). Gisdakis et al. (2015) 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 Manolopoulos et al. (2011). 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 (Gisdakis et al., 2015) can provide the anonymity and the report unlinkability.

Table 11
Authentication models achieved by security schemes for 4G and 5G cellular networks.

Schemes	Authentication models										
	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.**
Dimitriadis and Polemi (2006), Dimitriadis and Shaikh (2007), Bersani and Tschofenig (2007), He et al. (2008), Lu et al. (2009), Zhu et al. (2009), Wu et al. (2009), Abdelkader et al. (2010), Terzis et al. (2011),Niu et al. (2013), Jang et al. (2014),Chen et al. (2014),Ma et al. (2014), Kumari et al. (2014a), Haddad et al. (2015), Gisdakis et al. (2015), Ramadan et al. (2016), Saxena et al. (2016), Hashem Eiza et al. (2016), Hamandi et al. (2017)	X										
Dimitriadis and Shaikh (2007), Fan and Lin (2009), He and Wang (2015)										X	
Chien (2007), Chien and Chen (2007),Liu and Bailey (2009), Sun and Ting (2009), Chien and Laih (2009), Kulseng et al. (2010), Zhou et al. (2010),Li et al. (2013a, 2013b), Liao and Hsiao (2014), Fan et al. (2016)					X						
Lee et al. (2007), Chen et al. (2008)									X		
Deng et al. (2009), Zhu et al. (2009), Wu et al. (2009), Fu et al. (2012), Cao et al. (2012), Li et al. (2012),He (2012), Chen et al. (2013), Chen et al. (2014), Kumari et al. (2014a), Haddad et al. (2015), Cao et al. (2015), Ramadan et al. (2016),Hamandi et al. (2017)				X							
Fan and Lin (2009), Li et al. (2013a, 2013b)							X				
Fan and Lin (2009), Lee et al., (2011), Li et al. (2013a, 2013b), Chaudhry et al. (2015)			X								
Pereniguez et al. (2010)						X					
Sood et al. (2011), Wang et al. (2014), Jiang et al. (2015)								X			
Cao et al. (2012b), Fu et al. (2012), Cao et al. (2012), Cao et al. (2015), Cao et al. (2015), Fu et al. (2016b)											X
Li et al. (2012), Sun et al. (2012), Liu and Liang (2013)		X									

Table 12
Privacy models achieved by security schemes for 4G and 5G cellular networks.

Schemes	Privacy models									
	Identity privacy	**Location privacy**	**Anonymity**	**RFID privacy**	**Untraceability**	**Non-frameability**	**Traceability**	**Conditional privacy**	**Forward privacy**	**Privacy preserving data aggregation**
Fu et al. (2016a, 2016b)							X			
Zhang et al. (2016a, 2016b), Hashem Eiza et al. (2016)								X		
Dimitriadis and Polemi (2006), He et al. (2008), Pereniguez et al. (2010), Abdelkader et al. (2010),Barni et al. (2010), Karopoulos et al. (2011), Fu et al. (2012), Ramadan et al. (2016), Sood et al. (2011)	X									
Fu et al., (2016b)						X				
Chien and Chen (2007), Chien (2007), Zhou et al. (2010), Wang et al. (2014), Liao and Hsiao (2014), Gisdakis et al. (2015), Chaudhry et al. (2015), Zhang et al. (2015), Cao et al. (2015), He and Wang (2015), Fu et al. (2016a), Saxena et al. (2016), Hashem Eiza et al. (2016), Fu et al., (2016b),Pereniguez et al. (2011)			X							
Liu and Bailey (2009),Sun and Ting (2009), Chien and Laih (2009)				X						
Lu et al. (2009), Zhou et al. (2010), Terzis et al. (2011), Gao et al. (2013), Niu et al. (2013), Liao and Hsiao (2014), Gisdakis et al. (2015), Mahmoud et al. (2016), Hamandi et al. (2017)		X								
Pereniguez et al. (2010), Pereniguez et al. (2011), Zhang et al. (2015), Saxena et al. (2016)					X					
Saxena et al. (2016)									X	
Haddad et al. (2015)										X

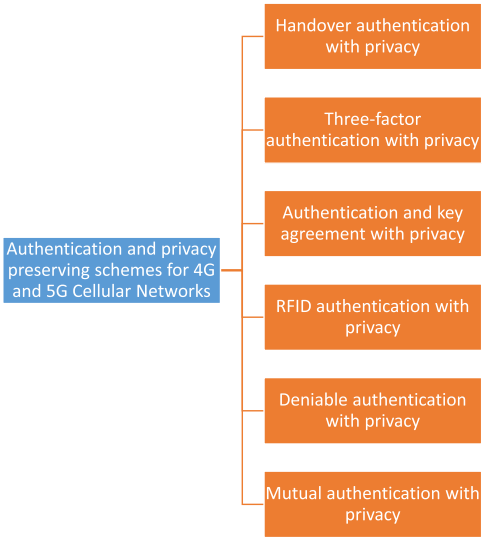

Fig. 6. Classification of authentication and privacy preserving schemes for 4G and 5G cellular networks.

Table 13
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

4.3. 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 (2009), 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 (Weis, 2003). As presented in Fig. 8, RFID authentication protocols with RFID privac1) Generation-2 Protocol, e.g., the Gen2 protocol in Duc et al. (2006), 2) CRC-Based Protocol, e.g., the SASI protocol in Chien (2007), 3) Minimalist Cryptography, e.g., the protocol in Juels (2005), 4) Protocol with Substring Function, e.g., the protocols in Li et al. (2006) and Chien and Huang (2007), and 5) ECC-Based Protocol, e.g., the protocol in Chien (2007). Similar to Sun and Ting (2009); Dubrova et al. (2015) proposed a message authentication scheme based on Cyclic Redundancy Check (CRC) codes for 5G Mobile Technology.

Chien (2007) 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 (2007) addressed the weaknesses of two schemes (Karthikeyan and Nesterenko, 2005; Duc et al., 2006) and proposed a mutual authentication scheme for GEN-2 RFID. The scheme (Chien and Chen, 2007) can preserve the privacy and resist against DOS attack compared to both schemes (Karthikeyan and Nesterenko, 2005; Duc et al., 2006). Liu and Bailey proposed an another interesting protocol that can achieve both privacy and authentication in Liu and Bailey (2009). 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 (2009), 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 (Chien, 2007; Duc et al., 2006), and (Li et al., 2006).

To achieve RFID authentication with anonymity/untraceability, and even availability, Chien and Laih (2009) proposed a RFID authentication protocol based on Error Correction Codes (ECC) (Costello et al., 1998). The protocol (Chien and Laih, 2009) 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 (Chien and Laih, 2009) is efficient in term of computation complexity compared to the protocol LMAP (Peris-Lopez et al., 2006). According to Kulseng et al. (2010), the lightweight solution such as LMAP (Peris-Lopez et al., 2006) has been either broken or weakened. In fact, the authors in Kulseng et al. (2010) 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. (2013a, 2013b) 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. (2010) 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 (Zhou et al., 2010) 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 (Zhou et al., 2010) is in desynchronization resistance compared to the protocol (Kulseng et al., 2010). By using a modified EAP-AKA protocol (Al Shidhani and Leung, 2009) for authentication with the access network, Sharma and Leung (2012) proposed a robust one-pass IMS authentication mechanism in LTE-fem to cell heterogeneous networks. The mechanism is 50% improvement over the existing multi-pass authentication scheme published before 2012. Liao and Hsiao (2014) 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 and Batina (2006).

To preserve the authentication for IoT in 5G. Fan et al. (2016) 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. (2016) 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 (Zhuang et al., 2016) and RCIA (Mujahid et al., 2015), Luo et al. (2016) proposed

Table 14
Summary of authentication and privacy preserving schemes for 4G and 5G cellular networks. See Table 13 for the notations used.

Scheme	Network model	Auth. model	Privacy model	Performances (+) and limitations (-)	Complexity	Destined for
Saxena et al. (2016)	- 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 Sun and Ting (2009); He et al. (2008), and Lu et al. (2008).	Bandwidth consumption: - Between UE and MME=697 bits; - Between MME and HSS=886 bits;	4G
Wang et al. (2014)	- 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. (2013); Isawa and Morii (2012); He et al. (2011); Zhou and Xu (2011), and Xu et al. (2011); - The proposed scheme needs to be evaluated in term of communication overhead; - The handover delays are not measured;	- Computation cost on user side: $1T_{SE} + 4T_H + 1T_S$	5G
Cao et al. (2015)	- 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: $3en + 4 + \eta$	4G
He and Wang (2015)	- 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: $3T_M + 7T_H$	5G
Fu et al. (2016a)	- 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: $n + 6\,m$	4G
Mahmoud et al. (2016)	- 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	4G
Ramadan et al. (2016)	- 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 X. Li et al. (2013); Z. Li et al. (2013);	- Computation cost on user side: $4T_{ECC} + 2T_H + 2T_P + T_M$	4G

(continued on next page)

Table 14 *(continued)*

Scheme	Network model	Auth. model	Privacy model	Performances (+) and limitations (-)	Complexity	Destined for
Hashem Eiza et al. (2016)	-Multi-tier 5G enabled vehicular network	- 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: $6T_H + 2T_S$; - $T_{COM} = 13.3$ s	5G
Hamandi et al. (2017)	- 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;	4G
Li et al. (2016)	- 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 Li et al. (2013a, 2013b).	- Computation cost: $(T_L + T_H + 2T_M)n$	4G
Zhang et al. (2015)	- 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: $4T_M + 4\,T_H + 10T_S$	5G
Fu et al., (2016b)	- 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 Jing et al. (2012), Pair-Hand scheme He et al. (2012), and UHAEN scheme Cao et al. (2012a); - The perfect forward and backward secrecy are not considered compared to the scheme Cao et al. (2012b).	- Computation cost on user side: $5T_M$	4G

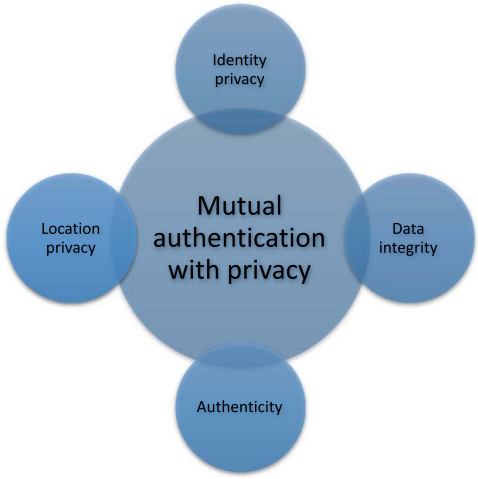

Fig. 7. Classification of mutual authentication with privacy schemes.

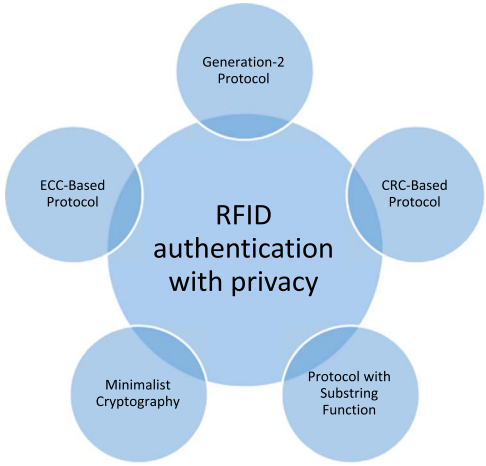

Fig. 8. Classification of RFID authentication protocols with RFID privacy.

recently a new ultra-lightweight mutual authentication protocol, which doesn't use any unbalanced operations like *OR* and *AND*.

4.4. Deniable authentication with privacy

The deniable authentication differs from traditional authentication in a way that the Receiver cannot convince a third party (Di Raimondo et al., 2005). Therefore, Lee et al. (2007) 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 (Harn and Xu, 1994), the protocol (Lee et al., 2007) does not only consider the security issues proposed in Shao (2004), 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) (Black, 2000) between two parties in cellular networks can achieving the deniable authentication.

To providing a lower degree of scalability and security, Bersani and Tschofenig (2007) 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 (Aboba et al., 2004), RFC 2284 (Blunk, 1998), and was updated by RFC 5247 (Aboba et al., 2008). As detailed in Fig. 9, there are many EAP authentication framework-based methods, which published as RFCs (IETF, 2017) as Internet Standards. However, Chen et al. (2008) proposed two strong devices and user authentication schemes for Wi-Fi and WiMAX inter-networked wireless cities. The idea of (Chen et al., 2008) is based on the modified Transport Layer Security (TLS) protocol (Dierks, 2008), which leverage Trusted Platform Module (TPM) technologies (Perez et al., 2006). The work (Chen et al., 2008) 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. (2010), if the authentication mechanism does not have an adequate level of privacy, the identity and location can be revealed. Pereniguez et al. (2010) 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. (2017) proposed a caching

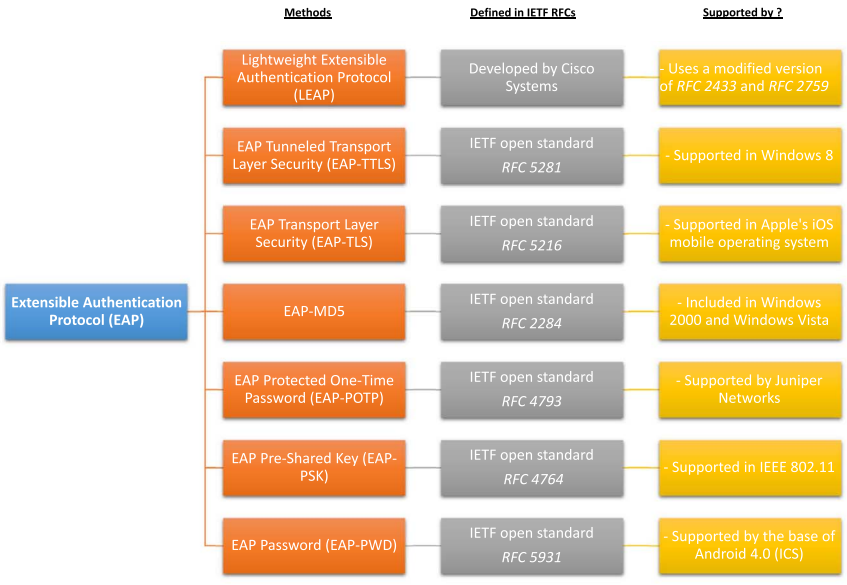

Fig. 9. Classification of methods based on EAP authentication framework.

mechanism, called UPP-KC, where the keys are cached only along a predicted path for broadband wireless networks.

4.5. 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 Ferrag et al. (2017a). Lu et al. (2008) 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.

Focusing on solving 5G network security issues, Yan et al. (2016) proposed a security and trust framework to securely deploy various trustworthy security services over the virtualized networks using cloud computing. Based on the modified model of population dynamics Zhou et al. (2015b) proposed a novel threshold credit-based incentive mechanism, named TCBI, for Cloud-based vehicular DTNs. To achieving the privacy preserving context transfer for 4G networks, Terzis et al. (2011) proposed four privacy preserving schemes for Context transfer protocol (CXTP) (Loughney et al., 2005). 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 (Neuman et al., 2005), 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. (2011), the Kerberos protocol suffers from two issues, namely, user anonymity and service access untraceability. The authors proposed a two-level privacy architecture, named PrivaKERB, to preserves the privacy of the user during activity with Kerberos. Based on two different levels of privacy: level 1, which provides user anonymity through pseudonyms, and level 2 where, apart from user anonymity, service access untraceability is assured. In addition, PrivaKERB is efficient in terms of service times, resource and network utilization compared to the standard Kerberos protocol (Neuman et al., 2005).

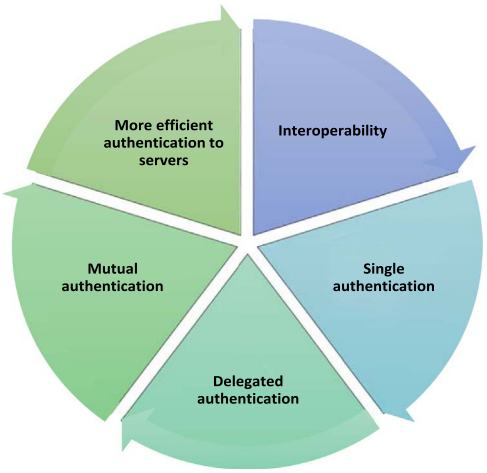

Fig. 10. Different models offered by the Kerberos protocol.

According to Wang and Yan (2017), implementing D2D communications introduce new security threats comparing with traditional cellular communication systems. Recently, Zhang et al. (2016a, 2016b) proposed a secure data sharing strategy for 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 two ideas proposed by Hashem Eiza et al. (2016) and Lin et al. (2008) can be applied for cloud-assisted video reporting service in 5G enabled vehicular networks.

4.6. 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 (Pedrycz and Vasilakos, 2000). Therefore, Deng et al. (2009) proposed an improved authentication and key agreement protocol based on public key cryptosystem. The protocol (Deng et al., 2009) 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. (2017) 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. (2016) 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 (Li et al., 2013a, 2013b). To avoid the signal congestion in 3GPP networks, Yao et al. (2016) proposed a group-based authentication for machine-to-machine (M2M), which is efficient in term of bandwidth consumption.

According to Zhu et al. (2009), the AKA protocol can easily be extended to provide revocable privacy by adopting the fair blind signature technique (Chaum, 1983). Specifically, Zhu et al. (2009) 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 (Zhu et al., 2009). Besides, PPAB is efficient in term of energy consumption compared to the scheme (Rabin, 1979), but the deniability and completeness are not considered. To the best of our knowledge, the work of Zhu et al. (2009) 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. (2015) 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. (2009), the SIP protocol does not include any specific security mechanisms. Specifically, Wu et al. (2009) 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 (Zhu et al., 2009). To provide the location and identity privacy, Karopoulos et al. (2011) 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 (Wu and Tseng, 2010) and Yoon et al.'s scheme (Yoon and Yoo, 2010), He (2012) proposed a new user authentication and key agreement protocol using bilinear pairings for mobile client–server environment. The idea of He (2012) is based on the bilinear pairing under the computational Diffie–Hellman (CDH) and collision attack assumption and in the random oracle model. The scheme (He, 2012) 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 (Fu et al., 2012). However, using a temporary confidential channel, Chen et al. (2013) designed three type of authentication, including, 1) Bipartite authentication protocol, 2) Tripartite authentication protocol, and 3) Multipartite transitive authentication.

Based on three main categories of auxiliary channels, including, *input*, *transfer*, and *verification*, Mayrhofer et al. (2013) 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) (Mayrhofer, 2007). 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. (2016) proposed a user-to-user mutual authentication and key agreement scheme, which is more compatible with the LTE security architecture. The scheme (Ramadan et al., 2016) 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.

4.7. 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 (2009), 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 (Fan and Lin, 2009) is efficient in term of low computation for smart cards compared to three-factor authentication schemes in Lee et al. (2002) and Lin and Lai (2004). Therefore, according to Blasco et al. (2016), the biometric systems can mainly be classified into three categories: 1) Traditional Biometric Systems (e.g., Windows Hello (Rathgeb and Uhl, 2011)), 2) Wearable biometric systems (e.g., Using a smartphone), and 3) Hybrid

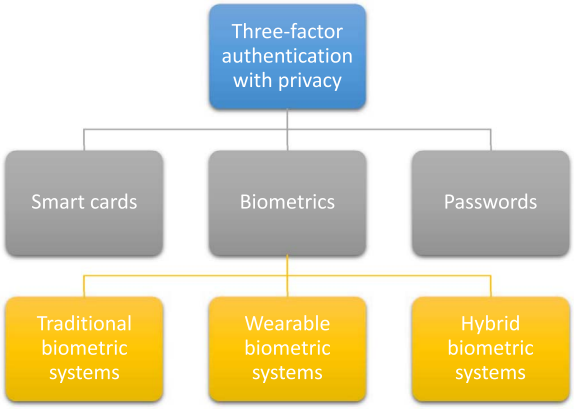

Fig. 11. Classification of three-factor authentication schemes with privacy.

biometric systems (e.g., Hybrid systems arises in telecare services (Camara et al., 2015b)). 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 (Blasco et al., 2016) and (Camara et al., 2015a).

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. (2010), 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 Jain et al. (2000), the identification protocol (Barni et al., 2010) is efficient in term of bandwidth usage compared to both schemes Erkin et al. (2009) and Sadeghi et al. (2010). Especially for multiserver environment, He and Wang (2015) proposed a biometrics-based authentication scheme, which is overcome the weaknesses in Yoon and Yoo's (2013) scheme and Kim et al.'s (2012) scheme.

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. (2011) presented a cryptanalysis of the Hsiang and Shih protocol (Hsiang and Shih, 2009) in order to propose a secure dynamic identity-based authentication protocol for multi-server architecture. The protocol (Sood et al., 2011) is efficient in term of computation complexity compared to related smart card based multi-server authentication protocols (Hsiang and Shih, 2009; Liao and Wang, 2009). Similar to Sood et al. (2011); Lee et al., (2011) presented a cryptanalysis of Hsiang et al. scheme (Hsiang and Shih, 2009) 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 (Lee et al., 2011) proposed a scheme to solve these weaknesses. In addition, Lee et al. scheme (Lee et al., 2011) is efficient in term of communication cost of the login and verification phase compared to three schemes, namely, Hsiang et al. scheme (Hsiang and Shih, 2009), Liao-Wang scheme (Liao and Wang, 2009), and Chang-Lee scheme (Chang and Lee, 2004). Li et al. (2012) out that the protocol (Sood et al., 2011) is still not secure. Based on the cryptanalysis of the protocol (Sood et al., 2011), the authors (Lee et al., 2011) proposed a security dynamic identity-based authentication protocol for multi-server architecture. The protocol (Li et al., 2012) provide the user's anonymity, proper mutual authentication, and session key agreement. In addition, the protocol (Li et al., 2012) is efficient in terms of computational complexity compared with some related dynamic ID based multi-server authentication protocols, including, Sood et al. (2011); Hsiang and Shih (2009), and Liao and Wang (2009). Similar to Chen et al. (2013); Liu and Liang (2013) 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 (Liu and Liang, 2013)

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 (Liu and Liang, 2013) is efficient in term of handover delays compared with the protocol in Dang et al. (2010).

Previous works in this area, i.e., password-based-authentication, have come short of providing solutions to detecting password reuse attacks. To provide privacy-preserving and secure roaming service for 4G and 5G cellular networks, Wang et al. (2014) revisited the privacy-preserving two-factor authentication scheme presented by Li et al. in Li et al. (2013), which they showed that the scheme (Scarlata et al., 2001) suffers from offline password guessing attack. The study of Wang et al. (2014) can withstand offline password guessing attack even if the victim's smart card is lost. As an additional benefit, the Wang et al. scheme (Wang et al., 2014) is efficient in term of computation cost on user side compared to fives schemes Li et al. (2013); Isawa and Morii (2012); He et al. (2011); Zhou and Xu (2011), and Xu et al. (2011). To overcome the weaknesses of Das scheme (Das, 2011), Li et al. (2013a, 2013b) a three-factor remote user authentication and key agreement scheme using biometrics. Based on discrete logarithm problem (Bruce, 1995), the Li et al. scheme (Li et al., 2013a, 2013b) can ensure the known-key secrecy and provide the perfect forward secrecy.

Similar to Wang et al. (2014); Chen et al. (2014) proposed an improved smart-card-based password authentication and key agreement scheme. Based on the review of the Xu et al. (2009) scheme and Sood et al. (2010) scheme, the scheme (Chen et al., 2014) can achieve mutual authentication and guarantees forward secrecy. In addition, the scheme (Chen et al., 2014) is efficient in term of computation cost on server side compared to three schemes Xu et al. (2009); Sood et al. (2010), and Song (2010). Therefore, if the authentication stored in the memory device is exposed, Jiang et al. pointed out that the scheme (Chen et al., 2014) suffers from offline password guessing attacks.

Based on the cryptanalysis of two schemes of Sood et al. (2011) and Wen and Li (2012); Ma et al. (2014) proposed three general principles that are vital for designing secure smart-card-based password authentication schemes in the future, which can be applied for 4G and 5G cellular networks. To overcome the weaknesses of Chang et al.'s scheme (Chang et al., 2013), Kumari et al. (2014a) proposed an improved user authentication scheme with session key agreement facility. Compared to the Chang et al.'s scheme (Chang et al., 2013), the Kumari et al.' scheme (Kumari et al., 2014a) cannot only provide forward secrecy, but the user is anonymous and untraceable. To overcome the weaknesses of Kumari et al.'s scheme (Kumari et al., 2014b), Chaudhry et al. (2015) proposed an enhanced remote user authentication scheme, which can ensures privacy and anonymity.

5. Open issues and future directions

As shown in Fig. 12, authentication and privacy-preserving schemes for 4G and 5G cellular networks focus on four 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, we outline both open issues and future directions that could improve the capabilities and effectiveness of authentication and privacy-preserving schemes for 4G and 5G cellular networks, summarized in the following recommendations:

- With the emergence of new communication models in 5G heterogeneous communication environment, such as, vehicular crowdsensing, Unmanned Aerial Vehicle (UAV) systems, Software Defined Networking (SDN), Network Function Virtualization (NFV), smart grids, and fog computing, the new authentication and privacy-preserving schemes for 4G and 5G cellular networks require novel designs for highly parallel low-cost architectures.
- The need for better privacy is an open issue for 4G and 5G cellular networks, which will require new privacy models. Appropriate and novel designs based on the combination of privacy metrics promises significant privacy improvements.
- The ever increasing speed of network links requires rigorous investigation of other kinds of attacks. There are some attacks that are not dealt sufficiently in the surveyed authentication and privacy-preserving schemes for 4G and 5G cellular networks, such as, packet tracing attacks, sybil attacks, forgery attacks, black hole attacks, and wormhole attacks. These attacks can pose a lot of privacy problems in cellular networks.

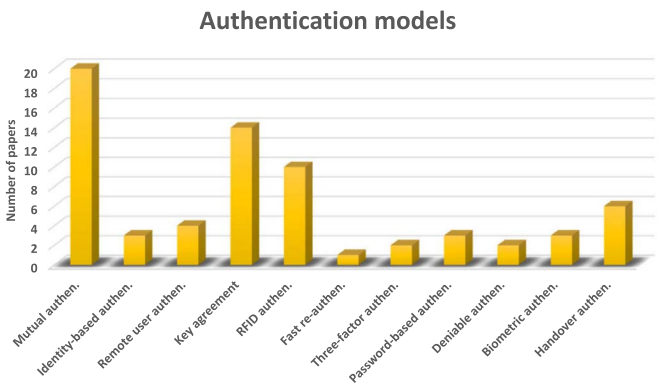

Fig. 12. Number of papers vs. Authentication models.

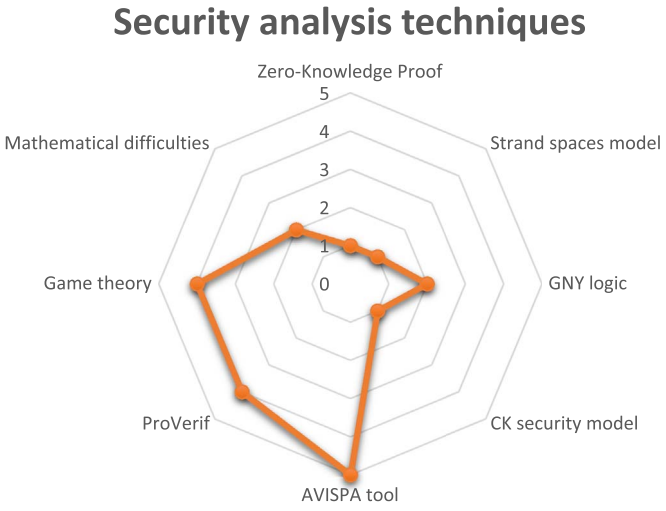

Fig. 13. Number of papers vs. Security analysis techniques.

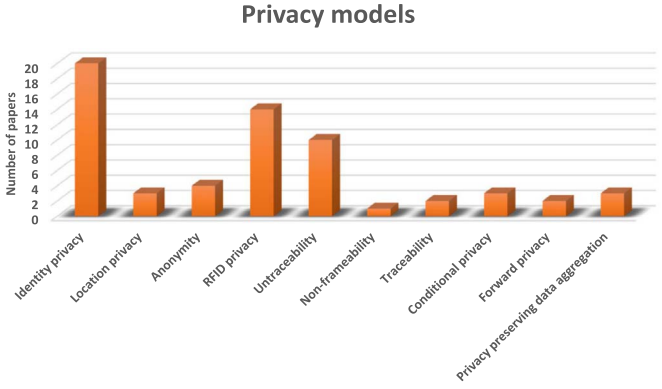

Fig. 14. Number of papers vs. Privacy models.

- Since IDSs can threaten users' privacy in 4G and 5G cellular networks, raises the need for deployment of adaptive multilateral secure IDSs. Combining the basic techniques of data avoidance and data reduction among others novel multilateral IDSs that can continuously monitor a system while allowing all involved parties to protect their own interests and that can adapt to varying the conditions of the system are of great need.
- In order to help the research community to come up with novel, efficient authentication and privacy-preserving schemes without interfering with the operation of a live system, the research community is of great need of open access big datasets, which include a wide variety of intrusions that are simulated or conducted in 4G or 5G environments.

5.1. 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. (2017) 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.

5.2. 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. (2017) 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.

5.3. 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 (Brunstrom et al., 2017). 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.

5.4. Dataset for intrusion detection in 5G scenarios

As we have seen in subSection Section 3.2, 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 (Buczak and Guven, 2016). Buczak and Guven (2016) 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 Section 3.1 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.

5.5. 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. (2017) 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.

5.6. 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. (2017) 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.

6. 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

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H., 2004. Extensible authentication protocol (EAP). Tech. rep.

Aboba, B., Levkowetz, H., Simon, D., Eronen, P, 2008. Extensible authentication protocol (EAP) key management framework, RFC 5247.

Abu-Ali, N., Taha, A.-E.M., Salah, M., Hassanein, H., 2014. Uplink scheduling in LTE and LTE-advanced: tutorial, survey and evaluation framework. IEEE Commun. Surv. Tutor. 16 (3), 1239–1265. http://dx.doi.org/10.1109/SURV.2013.1127.00161.

Abu-Lebdeh, M., Sahoo, J., Glitho, R., Tchouati, C.W., 2016. Cloudifying the 3GPP IP multimedia subsystem for 4G and beyond: a survey. IEEE Commun. Mag. 54 (1), 91–97. http://dx.doi.org/10.1109/MCOM.2016.7378432.

Agiwal, M., Roy, A., Saxena, N., 2016. Next generation 5G wireless networks: a comprehensive survey. IEEE Commun. Surv. Tutor. 18 (3), 1617–1655. http://dx.doi.org/10.1109/COMST.2016.2532458.

Aiash, M., Mapp, G., Lasebae, A., Phan, R., 2010. Providing Security in 4G Systems: Unveiling the Challenges. In: Proceedings of Sixth Advanced International Conference Telecommunication, IEEE, pp. 439–444. http://dx.doi.org/10.1109/AICT.2010.24.

Al Shidhani, A., Leung, V., 2009. Pre-Authentication Schemes for UMTS-WLAN Interworking. EURASIP J. Wirel. Commun. Netw. 2009 (1), 806563. http://dx.doi.org/10.1155/2009/806563.

Ali-Eldin, A., van den Berg, J., Ali, H.A., 2016. A risk evaluation approach for authorization decisions in social pervasive applications. Comput. Electr. Eng. 55, 59–72. http://dx.doi.org/10.1016/j.compeleceng.2016.01.022.

Andrews, J.G., Buzzi, S., Choi, W., Hanly, S.V., Lozano, A., Soong, A.C.K., Zhang, J.C., 2014. What Will 5G Be? IEEE J. Sel. Areas Commun. 32 (6), 1065–1082. http://dx.doi.org/10.1109/JSAC.2014.2328098.

Anwar, S., Mohamad Zain, J., Zolkipli, M.F., Inayat, Z., Khan, S., Anthony, B., Chang, V., 2017. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms 10 (2), 39. http://dx.doi.org/10.3390/a10020039.

Araniti, G., Campolo, C., Condoluci, M., Iera, A., Molinaro, A., 2013. LTE for vehicular networking: a survey. IEEE Commun. Mag. 51 (5), 148–157. http://dx.doi.org/10.1109/MCOM.2013.6515060.

Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuellar, J., Drielsma, P. H., Heám, P.C., Kouchnarenko, O., Mantovani, J., Mödersheim, S., von Oheimb, D., Rusinowitch, M., Santiago, J., Turuani, M., Viganò, L., Vigneron, L., 2005. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In: Proceedings of International Conference on Computer Aided Verification, pp. 281–285. http://dx.doi.org/10.1007/11513988_27.

Armknecht, F., Girao, J., Matos, A., Aguiar, R.L., 2007. Who Said That? Privacy at Link Layer. In: Proceedings of the 26th IEEE International Conference on Computer Communication, IEEE INFOCOM 2007, pp. 2521–2525. http://dx.doi.org/10.1109/INFCOM.2007.313.

Arul, R., Raja, G., Kottursamy, K., Sathiyanarayanan, P., Venkatraman, S., 2017. User path prediction based key caching and authentication mechanism for broadband wireless networks. Wirel. Pers. Commun. 94 (4), 2645–2664. http://dx.doi.org/10.1007/s11277-016-3877-5.

AT & T Newsroom, 2017. URL ⟨http://about.att.com/story/att_launches_lte_m_network_a_step_forward_to_5g.html⟩.

Attar, A., Tang, H., Vasilakos, A.V., Yu, F.R., Leung, V.C., 2012. A survey of security challenges in cognitive radio networks: solutions and future research directions. Proc. IEEE 100 (12), 3172–3186.

B. Parno, A. Perrig, V. Gligor, Distributed detection of node replication attacks in sensor networks. In: Proceedings of IEEE Symposium on Security and Privacy, IEEE, 2005, pp. 49–63.

Bajracharya, R., Shrestha, R., Zikria, Y.B., Kim, S.W., 2016. LTE in the Unlicensed Spectrum: a survey. IETE Tech. Rev., 1–13. http://dx.doi.org/10.1080/02564602.2016.1251344.

Barni, M., Scotti, F., Piva, A., Bianchi, T., Catalano, D., Di Raimondo, M., Donida Labati, R., Failla, P., Fiore, D., Lazzeretti, R., Piuri, V., Privacy-preserving fingercode authentication. In: Proceedings The 12th ACM Workshop on Multimedia and Security - MM & Sec '10, ACM Press, New York, New York, USA, p. 231. http://dx.doi.org/10.1145/1854229.1854270.

Basaras, P., Belikaidis, I., Maglaras, L., Katsaros, D., 2016. Blocking epidemic propagation in vehicular networks. In: Proceedings of the 12th Annual Conference on Wireless On-demand Network Systems and Services (WONS), 2016 , IEEE, pp. 1–8.

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

Bellare, M., Rogaway, P., 1993. Entity Authentication and Key Distribution. In: Adv. Cryptol. CRYPTO' 93, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 232–249. http://dx.doi.org/10.1007/3-540-48329-2_21.

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

Bikos, A.N., Sklavos, N., 2013. LTE/SAE security issues on 4G wireless networks. IEEE Secur. Priv. 11 (2), 55–62. http://dx.doi.org/10.1109/MSP.2012.136.

Biryukov, A., 2011. Digital Signature Standard. In: Encycl. Cryptogr. Secur., Springer US, Boston, MA, pp. 347–347. doi:10.1007/978-1-4419-5906-5_145.

Black, J.R., 2000. Message Authentication Codes. University of California, Davis.

Blanchet, B., 2016. Modeling and verifying security protocols with the applied pi calculus and ProVerif. Found. Trends {®} Priv. Secur. 1 (1–2), 1–135.

Blanchet, B, 2016b. ProVerif: Cryptographic Protocol Verifier Formal Model. URL ⟨http://www.proverif.ens.fr/⟩.

Blasco, J., Chen, T.M., Tapiador, J., Peris-Lopez, P., 2016. A survey of wearable biometric recognition systems. ACM Comput. Surv. 49 (3), 1–35. http://dx.doi.org/10.1145/2968215.

Blunk, L.J, 1998. PPP extensible authentication protocol (EAP), RFC 2284.

Bohák. A., Buttyán, L., Dóra, L., 2007. An authentication scheme for fast handover between WiFi access points. In: Proceedings ACM Wirel. Internet Conference.

Boneh, D., Boyen, X., Shacham, H., 2004. Short Group Signatures. In: Proceedings of Annual International Cryptol. Conference, pp. 41–55. http://dx.doi.org/10.1007/978-3-540-28628-8_3.

Boneh, D., Shacham, H., 2004. Group signatures with verifier-local revocation. In: Proceedings of the 11th ACM Conference Computer Communication and Security - CCS '04, ACM Press, New York, New York, USA, p. 168. http://dx.doi.org/10.1145/1030083.1030106.

Bruce, S, 1995. Applied cryptography: protocols, algorithms, and source code in C, New York Wiley.

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

Buczak, A.L., Guven, E., 2016. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutor. 18 (2), 1153–1176.

Burrows, M., Abadi, M., Needham, R., 1990. A logic of authentication. ACM Trans. Comput. Syst. 8 (1), 18–36. http://dx.doi.org/10.1145/77648.77649.

Buzzi, S., Chih-Lin, I., Klein, T.E., Poor, H.V., Yang, C., Zappone, A., 2016. A survey of energy-efficient techniques for 5G networks and challenges ahead. IEEE J. Sel. Areas Commun. 34 (4). http://dx.doi.org/10.1109/JSAC.2016.2550338.

Camara, C., Peris-Lopez, P., Tapiador, J.E., 2015a. Security and privacy issues in implantable medical devices: A comprehensive survey. J. Biomed. Inform. 55, 272–289. http://dx.doi.org/10.1016/j.jbi.2015.04.007.

Camara, C., Peris-Lopez, P., Tapiador, J.E., 2015b. Human identification using compressed ECG signals. J. Med. Syst. 39 (11), 148. http://dx.doi.org/10.1007/s10916-015-0323-2.

Canetti, R., Goldreich, O., Halevi, S., 2004. The random oracle methodology, revisited. J. ACM 51 (4), 557–594. http://dx.doi.org/10.1145/1008731.1008734.

Canetti, R., Krawczyk, H., 2001. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In: Proceedings ofInternational Conference on Theory and Applications of Cryptographic Techniques, pp. 453–474. http://dx.doi.org/10.1007/3-540-44987-6_28.

Cantor, S., 2003. ID-FF protocols and schema specification. Version 183, 1–2.

Cao, J., Ma, M., Li, H., 2012a. An uniform handover authentication between E-UTRAN and non-3GPP access networks. IEEE Trans. Wirel. Commun. 11 (10), 3644–3650. http://dx.doi.org/10.1109/TWC.2012.081612.112070.

Cao, J., Li, H., Ma, M., Zhang, Y., Lai, C., 2012b. A simple and robust handover authentication between HeNB and eNB in LTE networks. Comput. Netw. 56 (8), 2119–2131. http://dx.doi.org/10.1016/j.comnet.2012.02.012.

Cao, J., Ma, M., Li, H., Zhang, Y., Luo, Z., 2014. A survey on security aspects for LTE and LTE-A networks. IEEE Commun. Surv. Tutor. 16 (1), 283–302. http://dx.doi.org/10.1109/SURV.2013.041513.00174.

Cao, J., Li, H., Ma, M., 2015. GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks. In: Proceedings of International Conference Communication, IEEE, pp. 3020–3025. http://dx.doi.org/10.1109/ICC.2015.7248787.

Cao, J., Li, H., Ma, M., Li, F., 2015. UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks. In: Proceedings of International Conference on Communication, IEEE, pp. 7246–7251. http://dx.doi.

org/10.1109/ICC.2015.7249483.
Cao, Jin, Ma, Maode, Li, Hui, 2012. A group-based authentication and key agreement for MTC in LTE networks. In: Proceedings of Global Communication Conference, IEEE, pp. 1017–1022. http://dx.doi.org/10.1109/GLOCOM.2012.6503246.
Cao, Jin, Ma, Maode, Li, Hui, 2012. Unified handover authentication between heterogeneous access systems in LTE networks. In: Proceedings of Global Communiction Conference, IEEE, pp. 5308–5313. http://dx.doi.org/10.1109/GLOCOM.2012.6503964.
Capozzi, F., Piro, G., Grieco, L., Boggia, G., Camarda, P., 2013. Downlink packet scheduling in LTE cellular networks: key design issues and a survey. IEEE Commun. Surv. Tutor. 15 (2), 678–700. http://dx.doi.org/10.1109/SURV.2012.060912.00100.
Casas, P., D'Alconzo, A., Fiadino, P., Callegari, C., 2016. Detecting and diagnosing anomalies in cellular networks using Random Neural Networks. In: Proceedings of International Wireless Communication and Mobile Computing Conference, IEEE, pp. 351–356. http://dx.doi.org/10.1109/IWCMC.2016.7577083.
Chang, Y.-F., Tai, W.-L., Chang, H.-C., 2013. Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update. Int. J. Commun. Syst. http://dx.doi.org/10.1002/dac.2552, (n/a-n/a).
Chang, Chin-Chen, Lee, Jung-San, An Efficient and Secure Multi-Server Password Authentication Scheme using Smart Cards. In: Proceedings of International Conference Cyberworlds, IEEE, pp. 417–422. http://dx.doi.org/10.1109/CW.2004.17.
Chaudhry, S.A., Farash, M.S., Naqvi, H., Kumari, S., Khan, M.K., 2015. An enhanced privacy preserving remote user authentication scheme with provable security. Secur. Commun. Netw. 8 (18), 3782–3795. http://dx.doi.org/10.1002/sec.1299.
Chaum D., 1983. Blind Signatures for Untraceable Payments. In: Adv. Cryptol., Springer US, Boston, MA, pp. 199–203. doi:10.1007/978-1-4757-0602-4_18.
Chen, B.-L., Kuo, W.-C., Wuu, L.-C., 2014. Robust smart-card-based remote user password authentication scheme. Int. J. Commun. Syst. 27 (2), 377–389. http://dx.doi.org/10.1002/dac.2368.
Chen, Chien-Ming, Wang, King-Hang, Wu, Tsu-Yang, Pan, Jeng-Shyang, Sun, Hung-Min, 2013. A scalable transitive human-verifiable authentication protocol for mobile devices. IEEE Trans. Inf. Forensics Secur. 8 (8), 1318–1330. http://dx.doi.org/10.1109/TIFS.2013.2270106.
Chen, M., Zhang, Y., Hu, L., Taleb, T., Sheng, Z., 2015. Cloud-based wireless network: virtualized, reconfigurable, smart wireless network to enable 5G technologies. Mob. Netw. Appl. 20 (6), 704–712. http://dx.doi.org/10.1007/s11036-015-0590-7.
Chen, Y.-T., Studer, A., Perrig, A., 2008. Combining TLS and TPMs to Achieve Device and User Authentication for Wi-Fi and WiMAX Citywide Networks. In: Proceedings of Wireless Communication Networks Conference, IEEE, pp. 2804–2809. http://dx.doi.org/10.1109/WCNC.2008.491.
Chien, H.-Y., Chen, C.-H., 2007. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. Comput. Stand. Interfaces 29 (2), 254–259. http://dx.doi.org/10.1016/j.csi.2006.04.004.
Chien, H.-Y., Laih, C.-S., 2009. ECC-based lightweight authentication protocol with untraceability for low-cost RFID. J. Parallel Distrib. Comput. 69 (10), 848–853. http://dx.doi.org/10.1016/j.jpdc.2009.07.007.
Chien, Hung-Yu, 2007. SASI: a new ultralightweight rfid authentication protocol providing strong authentication and strong integrity. IEEE Trans. Dependable Secur. Comput. 4 (4), 337–340. http://dx.doi.org/10.1109/TDSC.2007.70226.
Chien, H.-Y., Huang, C.-W., 2007. A Lightweight RFID Protocol Using Substring. In: Embed. Ubiquitous Comput., Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 422–431. http://dx.doi.org/10.1007/978-3-540-77092-3_37.
Conti, M., Dragoni, N., Lesyk, V., 2016. A survey of man in the middle attacks. IEEE Commun. Surv. Tutor. 18 (3), 2027–2051. http://dx.doi.org/10.1109/COMST.2016.2548426.
Costello, D., Hagenauer, J., Imai, H., Wicker, S., 1998. Applications of error-control coding. IEEE Trans. Inf. Theory 44 (6), 2531–2560. http://dx.doi.org/10.1109/18.720548.
Damnjanovic, A., Montojo, J., Wei, Y., Ji, T., Luo, T., Vajapeyam, M., Yoo, T., Song, O., Malladi, D., 2011. A survey on 3GPP heterogeneous networks. IEEE Wirel. Commun. 18 (3), 10–21. http://dx.doi.org/10.1109/MWC.2011.5876496.
Dang, L., Kou, W., Li, H., Zhang, J., Cao, X., Zhao, B., Fan, K., 2010. Efficient ID-based registration protocol featured with user anonymity in mobile IP networks. IEEE Trans. Wirel. Commun. 9 (2), 594–604. http://dx.doi.org/10.1109/TWC.2010.02.060445.
Das, A., 2011. Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. IET Inf. Secur. 5 (3), 145. http://dx.doi.org/10.1049/iet-ifs.2010.0125.
David, K., 2016. Beyond fifth generation:let's start talking sixth generation [From the Editor]. IEEE Veh. Technol. Mag. 11 (4), 3–4. http://dx.doi.org/10.1109/MVT.2016.2613379.
DeKok, A., 2005. The network access identifier, RFC 7542.
Deng, Yaping, Fu, Hong, Xie, Xianzhong, Zhou, Jihua, Zhang, Yucheng, Shi, Jinling, 2009. A novel 3GPP SAE authentication and key agreement protocol. In: Proceedings of International Conference Networks Infrastructure and Digital Content, IEEE, pp. 557–561. http://dx.doi.org/10.1109/ICNIDC.2009.5360865.
Devi, R., Jha, R.K., Gupta, A., Jain, S., Kumar, P., 2017. Implementation of Intrusion Detection System using Adaptive Neuro-Fuzzy Inference System for 5G wireless communication network. AEU - Int. J. Electron. Commun. 74, 94–106. http://dx.doi.org/10.1016/j.aeue.2017.01.025.
Di Raimondo, M., Gennaro, R., 2005. New approaches for deniable authentication. In: Proceedings of the 12th ACM Conference Computer Communication and Security - CCS '05, ACM Press, New York, New York, USA, p. 112. http://dx.doi.org/10.1145/1102120.1102137.
Dierks, T., 2008. The transport layer security (TLS) protocol version 1.2, RFC 5246.
Dimitriadis, C.K., Polemi, D., 2006. An identity management protocol for Internet applications over 3G mobile networks. Comput. Secur 25 (1), 45–51. http://dx.doi.org/10.1016/j.cose.2005.11.001.
Dimitriadis, C.K., Shaikh, S.A., 2007. A biometric authentication protocol for 3G mobile systems: modelled and validated using CSP and rank functions. IJ Netw. Secur 5 (1), 99–111.
Dong, M., Ota, K., Yang, L.T., Liu, A., Guo, M., 2016. Lscd: a low-storage clone detection protocol for cyber-physical systems. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 35 (5), 712–723.
Duan, X., Wang, X., 2015. Authentication handover and privacy protection in 5G hetnets using software-defined networking. IEEE Commun. Mag. 53 (4), 28–35. http://dx.doi.org/10.1109/MCOM.2015.7081072.
Dubrova, E., Naslund, M., Selander, G., 2015. CRC-based message authentication for 5G mobile technology. 2015 IEEE Trust., IEEE, 1186–1191. http://dx.doi.org/10.1109/Trustcom.2015.503.
Duc, D.N., Lee, H., Kim, K, 2006. Enhancing security of EPCglobal Gen-2 RFID against traceability and cloning, Auto-ID Labs Inf. Commun. Univ. White Pap.
Elijah, O., Leow, C.Y., Rahman, T.A., Nunoo, S., Iliya, S.Z., 2016. A comprehensive survey of pilot contamination in massive MIMO5G system. IEEE Commun. Surv. Tutor. 18 (2), 905–923. http://dx.doi.org/10.1109/COMST.2015.2504379.
Ericsson Press Releases, 2017. URL ⟨https://www.ericsson.com/en/press-releases/2017/3/softbank-and-ericsson-to-demonstrate-5g-28ghz⟩.
Ericsson press, 2014. URL ⟨https://www.ericsson.com/en/press-releases/2014/7/ericsson-5g-delivers-5-gbps-speeds⟩.
Erkin, Z., Franz, M., Guajardo, J., Katzenbeisser, S., Lagendijk, I., Toft, T., 2009. Privacy-Preserving Face Recognition. In: International Symp. Priv. Enhancing Technol. Symp., pp. 235–253. http://dx.doi.org/10.1007/978-3-642-03168-7_14.
Fan, Chun-I., Lin, Yi-Hui, 2009. Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. IEEE Trans. Inf. Forensics Secur. 4 (4), 933–945. http://dx.doi.org/10.1109/TIFS.2009.2031942.
Fan, K., Gong, Y., Liang, C., Li, H., Yang, Y., 2016. Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. Secur. Commun. Netw. 9 (16), 3095–3104. http://dx.doi.org/10.1002/sec.1314.
Ferrag, M.A., Nafa, M., Ghanemi, S., 2016. EPSA: an efficient and privacy-preserving scheme against wormhole attack on reactive routing for mobile ad hoc social networks. Int. J. Secur. Netw. 11 (3), 107. http://dx.doi.org/10.1504/IJSN.2016.078390.
Ferrag, M.A., Maglaras, L., Ahmim, A., 2017. Privacy-preserving schemes for ad hoc social networks: a survey. IEEE Commun. Surv. Tutor., 1. http://dx.doi.org/10.1109/COMST.2017.2718178.
Ferrag, M.A., Ahmim, A., (Eds.), 2017. Security Solutions and Applied Cryptography in Smart Grid Communications, Advances in Information Security, Privacy, and Ethics, IGI Global. doi:10.4018/978-1-5225-1829-7.
Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang J., 2016b. A Survey on Privacy-preserving Schemes for Smart Grid Communications URL http://arxiv.org/abs/1611.07722arXiv:1611.07722.
Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., Shu, L., 2017b. Authentication protocols for internet of things: A comprehensive survey, Security and Communication Networks.
Fu, A., Zhang, Y., Zhu, Z., Liu, X., Fast, A., 2010. Handover authentication mechanism based on ticket for IEEE 802.16 m. IEEE Commun. Lett. 14 (12), 1134–1136. http://dx.doi.org/10.1109/LCOMM.2010.12.100818.
Fu, A., Zhang, Y., Zhu, Z., Jing, Q., Feng, J., 2012. An efficient handover authentication scheme with privacy preservation for IEEE 802.16 m network. Comput. Secur 31 (6), 741–749. http://dx.doi.org/10.1016/j.cose.2012.06.008.
Fu, A., Song, J., Li, S., Zhang, G., Zhang, Y., 2016. A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks. Secur. Commun. Netw. 15. http://dx.doi.org/10.1002/sec.1455, (n/a-n/a).
Fu, A., Qin, N., Wang, Y., Li, Q., Zhang, G, 2016b. Nframe: A privacy-preserving with non-frameability handover authentication protocol based on (t, n) secret sharing for LTE/LTE-A networks, Wirel. NetworksURL http://dx.doi.org/10.1007/s11276-016-1277-0.
Gandotra, P., Jha, R.K., 2016. Device-to-device communication in cellular networks: a survey. J. Netw. Comput. Appl. 71, 99–117. http://dx.doi.org/10.1016/j.jnca.2016.06.004.
Gao, S., Ma, J., Shi, W., Zhan, G., Sun, C., 2013. TrPF: a trajectory privacy-preserving framework for participatory sensing. IEEE Trans. Inf. Forensics Secur 8 (6), 874–887. http://dx.doi.org/10.1109/TIFS.2013.2252618.
Gavrilovska, L., Rakovic, V., Atanasovski, V., 2016. Visions towards 5G: technical requirements and potential enablers. Wirel. Pers. Commun. 87 (3), 731–757. http://dx.doi.org/10.1007/s11277-015-2632-7.
Ghavimi, F., Chen, H.-H., 2015. M2M communications in 3GPP LTE/LTE-A networks: architectures, service requirements, challenges, and applications. IEEE Commun. Surv. Tutor. 17 (2), 525–549. http://dx.doi.org/10.1109/COMST.2014.2361626.
Gisdakis, S., Manolopoulos, V., Tao, S., Rusu, A., Papadimitratos, P., 2015. Secure and privacy-preserving smartphone-based traffic information systems. IEEE Trans. Intell. Transp. Syst. 16 (3), 1428–1438. http://dx.doi.org/10.1109/TITS.2014.2369574.
Gódor, G., Jakó, Z., Knapp, A., Imre, S., 2015. A survey of handover management in LTE-based multi-tier femtocell networks: requirements, challenges and solutions. Comput. Netw. 76, 17–41. http://dx.doi.org/10.1016/j.comnet.2014.10.016.
Goldwasser, S., Micali, S., Rackoff, C., 1989. The knowledge complexity of interactive proof systems. SIAM J. Comput. 18 (1), 186–208. http://dx.doi.org/10.1137/0218012.

Gong, L., Needham, R., Yahalom, R., 1990. Reasoning about belief in cryptographic protocols. In: Proceedings of Computer Society Symposium on Research in Security and Privacy, IEEE, pp. 234–248. http://dx.doi.org/10.1109/RISP.1990.63854.
Gupta, A., Jha, R.K., 2015. A survey of 5G network: architecture and emerging technologies. IEEE Access 3, 1206–1232. http://dx.doi.org/10.1109/ACCESS.2015.2461602.
Gupta, A., Jha, R.K., Jain, S., 2017. Attack modeling and intrusion detection system for 5G wireless communication network. Int. J. Commun. Syst. 30 (10), e3237. http://dx.doi.org/10.1002/dac.3237.
Gupta, M., Jha, S.C., Koc, A.T., Vannithamby, R., 2013. Energy impact of emerging mobile internet applications on LTE networks: issues and solutions. IEEE Commun. Mag. 51 (2), 90–97. http://dx.doi.org/10.1109/MCOM.2013.6461191.
Haddad, Z., Mahmoud, M., Taha, S., Saroit, I.A., 2015. Secure and privacy-preserving AMI-utility communications via LTE-A networks. In: Proceedings of the 11th International Conference on Wireless and Mobile Computing Networks Communication, IEEE, pp. 748–755. http://dx.doi.org/10.1109/WiMOB.2015.7348037.
Hamandi, K., Bou Abdo, J., Elhajj, I.H., Kayssi, A., Chehab, A., 2017. A privacy-enhanced computationally-efficient and comprehensive LTE-AKA. Comput. Commun. 98, 20–30. http://dx.doi.org/10.1016/j.comcom.2016.09.009.
Han, F., Zhao, S., Zhang, L., Wu, J., 2016. Survey of strategies for switching off base stations in heterogeneous networks for greener 5G systems. IEEE Access 4, 4959–4973. http://dx.doi.org/10.1109/ACCESS.2016.2598813.
Harn, L., Xu, Y., 1994. Design of generalised ElGamal type digital signature schemes based on discrete logarithm. Electron. Lett. 30 (24), 2025–2026.
Hasan, K., Shetty, S., Oyedare, T., 2017. Cross layer attacks on gsm mobile networks using software defined radios. In: Proceedings of 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, pp. 357–360.
Hashem Eiza, M., Ni, Q., Shi, Q., 2016. Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks. IEEE Trans. Veh. Technol. 65 (10), 7868–7881. http://dx.doi.org/10.1109/TVT.2016.2541862.
He, D., 2012. An efficient remote user authentication and key agreement protocol for mobile client and server environment from pairings. Ad Hoc Netw. 10 (6), 1009–1016. http://dx.doi.org/10.1016/j.adhoc.2012.01.002.
He, D., Wang, D., 2015. Robust biometrics-based authentication scheme for multiserver environment. IEEE Syst. J. 9 (3), 816–823. http://dx.doi.org/10.1109/JSYST.2014.2301517.
He, D., Ma, M., Zhang, Y., Chen, C., Bu, J., 2011. A strong user authentication scheme with smart cards for wireless communications. Comput. Commun. 34 (3), 367–374. http://dx.doi.org/10.1016/j.comcom.2010.02.031.
He, D., Chen, C., Chan, S., Bu, J., 2012. Secure and efficient handover authentication based on bilinear pairing functions. IEEE Trans. Wirel. Commun. 11 (1), 48–53. http://dx.doi.org/10.1109/TWC.2011.110811.111240.
He, D., Chan, S., Guizani, M., 2017. Drone-assisted public safety networks: The security aspect. IEEE Communications Magazine.
He, D., Zeadally, S., Wu, L., Wang, H., 2016. Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography, Comput. Networks. URL http://dx.doi.org/10.1016/j.comnet.2016.12.013.
He, Dake, Wang, Jianbo, Zheng, Yu, 2008. User authentication scheme based on self-certified public-key for next generation wireless network. In: Proceedings of International Symposium on Biometrics Security and Technology, IEEE, pp. 1–8. http://dx.doi.org/10.1109/ISBAST.2008.4547638.
Hoare, C.A.R., Communicating Sequential Processes. In: Orig. Concurr. Program., Springer New York, New York, NY, 1978, pp. 413–443. doi:10.1007/978-1-4757-3472-0_16.
Hsiang, H.-C., Shih, W.-K., 2009. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Comput. Stand. Interfaces 31 (6), 1118–1123. http://dx.doi.org/10.1016/j.csi.2008.11.002.
Huawei News, 2017 . URL ⟨http://www.huawei.com/en/events/mwc/2017/⟩.
IETF, 2017. URL ⟨https://www.ietf.org/rfc.html⟩.
Isawa, R., Morii, M., 2012. Anonymous authentication scheme without verification table for wireless environments. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 95 (12), 2488–2492.
Islam, S.M.R., Avazov, N., Dobre, O.A., Kwak, K.-s., 2017. Power-domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges. IEEE Commun. Surv. Tutor. 19 (2), 721–742. http://dx.doi.org/10.1109/COMST.2016.2621116.
Jaber, M., Imran, M.A., Tafazolli, R., Tukmanov, A., 2016. 5G backhaul challenges and emerging research directions: a survey. IEEE Access 4, 1743–1766. http://dx.doi.org/10.1109/ACCESS.2016.2556011.
Jain, A., Prabhakar, S., Hong, L., Pankanti, S., 2000. Filterbank-based fingerprint matching. IEEE Trans. Image Process 9 (5), 846–859. http://dx.doi.org/10.1109/83.841531.
Jang, U., Lim, H., Kim, H., 2014. Privacy-enhancing security protocol in LTE initial attack. Symmetry (Basel) 6 (4), 1011–1025. http://dx.doi.org/10.3390/sym6041011.
Jiang, Q., Ma, J., Li, G., Li, X., 2015. Improvement of robust smart-card-based password authentication scheme. Int. J. Commun. Syst. 28 (2), 383–393. http://dx.doi.org/10.1002/dac.2644.
Jing, Q., Zhang, Y., Liu, X., Fu, A., 2012. An efficient handover authentication scheme with location privacy preserving for EAP-based wireless networks. In: Proceedings of International Conference on Communication, IEEE, pp. 857–862. http://dx.doi.org/10.1109/ICC.2012.6363795.
Juels, A., 2005. Minimalist Cryptography for Low-Cost RFID Tags (Extended Abstract), In: Proceedings of International Conference on Security Communication and Networks, pp. 149–164. http://dx.doi.org/10.1007/978-3-540-30598-9_11.
Kang, M.-J., Kang, J.-W., 2016. Intrusion detection system using deep neural network for in-vehicle network security. PLoS One 11 (6), e0155781.
Karopoulos, G., Kambourakis, G., Gritzalis, S., 2011. PrivaSIP: ad-hoc identity privacy in SIP. Comput. Stand. Interfaces 33 (3), 301–314. http://dx.doi.org/10.1016/j.csi.2010.07.002.
Karthikeyan, S., Nesterenko, M., 2005. RFID security without extensive cryptography. In: Proceedings of the 3rd ACM Workshop on Security ad hoc Sensor networks - SASN '05, ACM Press, New York, New York, USA, p. 63. http://dx.doi.org/10.1145/1102219.1102229.
Katz, J., Lindell, A.Y., 2008. Aggregate Message Authentication Codes. In: Top. Cryptol. CT-RSA 2008, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 155–169. http://dx.doi.org/10.1007/978-3-540-79263-5_10.
Kim, H., Jeon, W., Lee, K., Lee, Y., Won, D., 2012. Cryptanalysis and Improvement of a Biometrics-Based Multi-server Authentication with Key Agreement Scheme. In: Proceedings of International Conference on Computer Science and Its Applications, pp. 391–406. http://dx.doi.org/10.1007/978-3-642-31137-6_30.
Kolias, C., Kambourakis, G., Stavrou, A., Gritzalis, S., 2016. Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. IEEE Commun. Surv. Tutor. 18 (1), 184–208. http://dx.doi.org/10.1109/COMST.2015.2402161.
Kolias, C., Kolias, V., Kambourakis, G., 2017. TermID: a distributed swarm intelligence-based approach for wireless intrusion detection. Int. J. Inf. Secur. 16 (4), 401–416. http://dx.doi.org/10.1007/s10207-016-0335-z.
Kormann, D.P., Rubin, A.D., 2000. Risks of the passport single signon protocol. Comput. Netw. 33 (1–6), 51–58. http://dx.doi.org/10.1016/S1389-1286(00)00048-7.
Krawczyk, H., Bellare, M., Canetti, R., 1997. RFC2104 - HMAC: Keyed-hashing for message authentication, Tech. rep. arXiv:arXiv:1011.1669v3arXiv:1011.1669v3, http://dx.doi.org/10.17487/rfc2104.
Ku, Y.-J., Lin, D.-Y., Lee, C.-F., Hsieh, P.-J., Wei, H.-Y., Chou, C.-T., Pang, A.-C., 2017. 5g radio access network design with the fog paradigm: confluence of communications and computing. IEEE Commun. Mag. 55 (4), 46–52.
Kulseng, L., Yu, Z., Wei, Y., Guan, Y., 2010. Lightweight Mutual Authentication and Ownership Transfer for RFID Systems. In: Proceedings of IEEE INFOCOM, IEEE, pp. 1–5. http://dx.doi.org/10.1109/INFCOM.2010.5462233.
Kumari, S., Khan, M.K., Li, X., 2014a. An improved remote user authentication scheme with key agreement. Comput. Electr. Eng. 40 (6), 1997–2012. http://dx.doi.org/10.1016/j.compeleceng.2014.05.007.
Kumari, S., Gupta, M.K., Khan, M.K., Li, X., 2014b. An improved timestamp-based password authentication scheme: comments, cryptanalysis, and improvement. Secur. Commun. Netw. 7 (11), 1921–1932. http://dx.doi.org/10.1002/sec.906.
Kwan, R., Leung, C., 2010. A survey of scheduling and interference mitigation in LTE. J. Electr. Comput. Eng. 2010, 1–10. http://dx.doi.org/10.1155/2010/273486.
Lai, C., Li, H., Lu, R., Shen, X.S., 2013. SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks. Comput. Netw. 57 (17), 3492–3510. http://dx.doi.org/10.1016/j.comnet.2013.08.003.
Lai, C., Li, H., Lu, R., Jiang, R., Shen, X., 2014. SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks. In: Proceedings of International Conference Communication, IEEE, pp. 1011–1016. http://dx.doi.org/10.1109/ICC.2014.6883452.
Laya, A., Alonso, L., Alonso-Zarate, J., 2014. Is the random access channel of LTE and LTE-A suitable for M2M communications? A survey of alternatives. IEEE Commun. Surv. Tutor. 16 (1), 4–16. http://dx.doi.org/10.1109/SURV.2013.111313.00244.
Le, N.T., Hossain, M.A., Islam, A., Kim, D.-y., Choi, Y.-J., Jang, Y.M., 2016. Survey of promising technologies for 5G networks. Netw., Mob. Inf. Syst. 2016, 1–25. http://dx.doi.org/10.1155/2016/2676589.
Lee, J., Ryu, S., Yoo, K., 2002. Fingerprint-based remote user authentication scheme using smart cards. Electron. Lett. 38 (12), 554. http://dx.doi.org/10.1049/el:20020380.
Lee, W.-B., Wu, C.-C., Tsaur, W.-J., 2007. A novel deniable authentication protocol using generalized ElGamal signature scheme. Inf. Sci. (Ny.) 177 (6), 1376–1381. http://dx.doi.org/10.1016/j.ins.2006.09.020.
Lee, C.-C., Lin, T.-H., Chang, R.-X, 2011. A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards, Expert Syst. Appl. URL http://dx.doi.org/10.1016/j.eswa.2011.04.190.
Li, J., Wen, M., Zhang, T., 2016. Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks. IEEE Internet Things J. 3 (3), 408–417. http://dx.doi.org/10.1109/JIOT.2015.2495321.
Li, X., Xiong, Y., Ma, J., Wang, W., 2012. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. J. Netw. Comput. Appl. 35 (2), 763–769. http://dx.doi.org/10.1016/j.jnca.2011.11.009.
Li, X., Niu, J., Wang, Z., Chen, C., 2013. Applying biometrics to design three-factor remote user authentication scheme with key agreement. Secur. Commun. Netw. http://dx.doi.org/10.1002/sec.767, (n/a-n/a).
Li, Z., Gong, G., Qin, Z., 2013. Secure and efficient LCMQ entity authentication protocol. IEEE Trans. Inf. Theory 59 (6), 4042–4054. http://dx.doi.org/10.1109/TIT.2013.2253892.
Li, Huixian, Yang, Yafang, Pang, Liaojun, 2013b. An efficient authentication protocol with user anonymity for mobile networks. In: Proceedings of IEEE Wireless Communication and Network Conference, IEEE, pp. 1842–1847. http://dx.doi.org/10.1109/WCNC.2013.6554844.
Li, Y.-z., Cho, Y.-b., Um, N.-k., Lee, S.-h., Security and Privacy on Authentication Protocol for Low-cost RFID. In: Proceedings of International Conference on Computer Intelligence and Security, IEEE, 2006, pp. 1101–1104. http://dx.doi.org/10.1109/ICCIAS.2006.295432.
Liao, Y.-P., Hsiao, C.-M., 2014. A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Ad Hoc Netw. 18, 133–146. http://dx.doi.org/10.1016/j.adhoc.2013.02.004.

Liao, Y.-P., Wang, S.-S., 2009. A secure dynamic ID based remote user authentication scheme for multi-server environment. Comput. Stand. Interfaces 31 (1), 24–29. http://dx.doi.org/10.1016/j.csi.2007.10.007.
Lichtman, M., Jover, R.P., Labib, M., Rao, R., Marojevic, V., Reed, J.H., 2016. LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation. IEEE Commun. Mag. 54 (4), 54–61. http://dx.doi.org/10.1109/MCOM.2016.7452266.
Lin, C.-H., Lai, Y.-Y., 2004. A flexible biometrics remote user authentication scheme. Comput. Stand. Interfaces 27 (1), 19–23. http://dx.doi.org/10.1016/j.csi.2004.03.003.
Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P.-H., Shen, X., 2008. Security in vehicular ad hoc networks, IEEE communications magazine 46 (4).
Liu, A.X., Bailey, L.A., 2009. PAP: a privacy and authentication protocol for passive RFID tags. Comput. Commun. 32 (7–10), 1194–1199. http://dx.doi.org/10.1016/j.comcom.2009.03.006.
Liu, D., Wang, L., Chen, Y., Elkashlan, M., Wong, K.-K., Schober, R., Hanzo, L., 2016. User sssociation in 5G networks: a survey and an outlook. IEEE Commun. Surv. Tutor. 18 (2), 1018–1044. http://dx.doi.org/10.1109/COMST.2016.2516538.
Liu, H., Liang, M., 2013. Efficient identity-based hierarchical access authentication protocol for mobile network. Secur. Commun. Netw. 6 (12), 1509–1521. http://dx.doi.org/10.1002/sec.412.
Liu, J., Kato, N., Ma, J., Kadowaki, N., 2015. Device-to-device communication in LTE-advanced networks: a survey. IEEE Commun. Surv. Tutor. 17 (4), 1923–1940. http://dx.doi.org/10.1109/COMST.2014.2375934.
Loughney, J., Nakhjiri, M., Perkins, C., Koodli, R., 2005. Context transfer protocol (CXTP), Tech. rep.
Lu, Li, Han, Jinsong, Liu, Yunhao, Hu, Lei, Huai, Jin-Peng, Ni, Jian, Ma, L., 2008. Pseudo trust: zero-knowledge authentication in anonymous P2Ps. IEEE Trans. Parallel Distrib. Syst. 19 (10), 1325–1337. http://dx.doi.org/10.1109/TPDS.2008.15.
Lu, Rongxing, Lin, Xiaodong, Zhu, Haojin, Ho, Pin-Han, Shen, Xuemin, 2009. Novel anonymous mutual authentication protocol with provable link-layer location privacy. IEEE Trans. Veh. Technol. 58 (3), 1454–1466. http://dx.doi.org/10.1109/TVT.2008.925304.
Luo, H., Wen, G., Su, J., Huang, Z, 2016. SLAP: Succinct and Lightweight Authentication Protocol for low-cost RFID system, Wirel. Networks URL http://dx.doi.org/10.1007/s11276-016-1323-y.
M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, V. Kumar, Security and Privacy in Fog Computing: Challenges, IEEE Access (2017) doi: 10.1109/GLOCOMW.2010.5700310.
Ma, C.-G., Wang, D., Zhao, S.-D., 2014. Security flaws in two improved remote user authentication schemes using smart cards. Int. J. Commun. Syst. 27 (10), 2215–2227. http://dx.doi.org/10.1002/dac.2468.
Madueno, G.C., Nielsen, J.J., Kim, D.M., Pratas, N.K., Stefanovic, C., Popovski, P., 2016. Assessment of LTE wireless access for monitoring of energy distribution in the smart grid. IEEE J. Sel. Areas Commun. 34 (3), 675–688. http://dx.doi.org/10.1109/JSAC.2016.2525639.
Mahmoud, M., Saputro, N., Akula, P., Akkaya, K., 2016. Privacy-preserving power injection over a hybrid AMI/LTE smart grid network. IEEE Internet Things J., 1. http://dx.doi.org/10.1109/JIOT.2016.2593453.
Manolopoulos, V., Papadimitratos, P., Tao, S., Rusu, A., 2011. Securing smartphone based ITS. In: Proceedings of the 11th International Conference on ITS Telecommunication, IEEE, pp. 201–206. http://dx.doi.org/10.1109/ITST.2011.6060053.
Manshaei, M.H., Zhu, Q., Alpcan, T., Bacşar, T., Hubaux, J.-P., 2013. Game theory meets network security and privacy. ACM Comput. Surv. 45 (3), 1–39. http://dx.doi.org/10.1145/2480741.2480742.
Mayrhofer, R., Fub, Ion, I., 2013. UACAP: a unified auxiliary channel authentication protocol. IEEE Trans. Mob. Comput. 12 (4), 710–721. http://dx.doi.org/10.1109/TMC.2012.43.
Mayrhofer, R., 2007. Towards an Open Source Toolkit for Ubiquitous Device Authentication. In: Proceedings of Fifth Annual IEEE International Conference on Pervasive Computer Communication Workshop, IEEE, pp. 247–254. http://dx.doi.org/10.1109/PERCOMW.2007.118.
Mehaseb, M.A., Gadallah, Y., Elhamy, A., Elhennawy, H., 2016. Classification of LTE uplink scheduling techniques: an M2M perspective. IEEE Commun. Surv. Tutor. 18 (2), 1310–1335. http://dx.doi.org/10.1109/COMST.2015.2504182.
MIT Kerberos Distribution, 2017. URL ⟨https://web.mit.edu/kerberos/⟩.
Mujahid, U., Najam-ul Islam, M., Shami, M.A., 2015. RCIA: a new ultralightweight RFID authentication protocol using recursive hash. Int. J. Distrib. Sens. Netw. 11 (1), 642180. http://dx.doi.org/10.1155/2015/642180.
Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M.A., Choudhury, N., Kumar, V., 2017. Security and privacy in fog computing: challenges. IEEE Access, 1. http://dx.doi.org/10.1109/ACCESS.2017.2749422.
Neuman, C., Hartman, S., Yu, T., Raeburn, K, 2005. The Kerberos network authentication service (V5), IETF RFC 4120.
Nguyen, V.-G., Do, T.-X., Kim, Y., 2016. SDN and virtualization-Based LTE mobile network architectures: a comprehensive survey. Wirel. Pers. Commun. 86 (3), 1401–1438. http://dx.doi.org/10.1007/s11277-015-2997-7.
Niu, Y., Li, Y., Jin, D., Su, L., Vasilakos, A.V., 2015a. A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges. Wirel. Netw. 21 (8), 2657–2676. http://dx.doi.org/10.1007/s11276-015-0942-z.
Niu, Y., Gao, C., Li, Y., Su, L., Jin, D., Vasilakos, A.V., 2015b. Exploiting device-to-device communications in joint scheduling of access and backhaul for mmwave small cells. IEEE J. Sel. Areas Commun. 33 (10), 2052–2069.
Niu, Ben, Zhu, Xiaoyan, Chi, Haotian, Li, Hui, 3PLUS: Privacy-preserving pseudo-location updating system in location-based services. In: Proceedings of IEEE Wireless Communication Networks Conference, IEEE, 2013, pp. 4564–4569. http://dx.doi.org/10.1109/WCNC.2013.6555314.
Noura, M., Nordin, R., 2016. A survey on interference management for Device-to-Device (D2D) communication and its challenges in 5G networks. J. Netw. Comput. Appl. 71, 130–150. http://dx.doi.org/10.1016/j.jnca.2016.04.021.
NTT Press Releases, 2017. URL ⟨http://www.ntt.co.jp/news2017/1703e/170327a.html⟩.
Olwal, T.O., Djouani, K., Kurien, A.M., 2016. A survey of resource management toward 5G radio access networks. IEEE Commun. Surv. Tutor. 18 (3), 1656–1686. http://dx.doi.org/10.1109/COMST.2016.2550765.
Paillier, P., 1999. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In: Adv. Cryptol. EUROCRYPT '99, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 223–238. http://dx.doi.org/10.1007/3-540-48910-X_16.
Panwar, N., Sharma, S., Singh, A.K., 2016. A survey on 5G: The next generation of mobile communication. Phys. Commun. 18, 64–84. http://dx.doi.org/10.1016/j.phycom.2015.10.006.
Papadopoulos, S., Drosou, A., Dimitriou, N., Abdelrahman, O.H., Gorbil, G., Tzovaras, D., 2016. A BRPCA based approach for anomaly detection in mobile networks. Inf. Sci. Syst., 115–125. http://dx.doi.org/10.1007/978-3-319-22635-4_10.
Pedrycz, W., Vasilakos, A., 2000. Computational Intelligence in Telecommunications Networks. CRC Press.
Pereniguez, F., Kambourakis, G., Marin-Lopez, R., Gritzalis, S., Gomez, A., 2010. Privacy-enhanced fast re-authentication for EAP-based next generation network. Comput. Commun. 33 (14), 1682–1694. http://dx.doi.org/10.1016/j.comcom.2010.02.021.
Pereniguez, F., Marin-Lopez, R., Kambourakis, G., Gritzalis, S., Gomez, A., 2011. PrivaKERB: a user privacy framework for Kerberos. Comput. Secur. 30 (6–7), 446–463. http://dx.doi.org/10.1016/j.cose.2011.04.001.
Perez, R., Sailer, R., van Doorn, L., 2006. Others, vTPM: virtualizing the trusted platform module. In: Proceedings of the 15th Conference on USENIX Security Symposium, pp. 305–320.
Peris-Lopez, P., Hernandez-Castro, J.C., Estévez-Tapiador, J.M., Ribagorda, A., 2006. LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. In: Proceedings 2nd Workshop on RFID Security, p. 6.
Rabin, M.O., Digitalized signatures and public-key functions as intractable as factorization, Tech. rep., Massachusetts Institute of Technology (MIT) (1979).
Ramadan, M., Li, F., Xu, C., Mohamed, A., Abdalla, H., Ali, A.A., 2016. User-to-user mutual authentication and key agreement scheme for LTE Cellular System. IJ Netw. Secur 18 (4), 769–781.
Rathgeb, C., Uhl, A., 2011. A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur. 2011 (1), 3. http://dx.doi.org/10.1186/1687-417X-2011-3.
Rebecchi, F., Dias de Amorim, M., Conan, V., Passarella, A., Bruno, R., Conti, M., 2015. Data offloading techniques in cellular networks: a survey. IEEE Commun. Surv. Tutor. 17 (2), 580–603. http://dx.doi.org/10.1109/COMST.2014.2369742.
Reuters News, 2017. URL ⟨http://www.reuters.com/article/us-verizon-5g-idUSKBN1611S9⟩.
Sadeghi, A.-R., Schneider, T., Wehrenberg, I., 2010. Efficient Privacy-Preserving Face Recognition. In: International Conference Inf. Secur. Cryptol., pp. 229–244. http://dx.doi.org/10.1007/978-3-642-14423-3_16.
Saha, R.K., Saengudomlert, P., Aswakul, C., 2016. Evolution toward 5G mobile networks - a survey on enabling technologies. Eng. J. 20 (1), 87–119. http://dx.doi.org/10.4186/ej.2016.20.1.87.
Salomaa, A., 2013. Public-Key Cryptography. Springer Science & Business Media.
Santoro, D., Escudero-Andreu, G., Kyriakopoulos, K.G., Aparicio-Navarro, F.J., Parish, D.J., Vadursi, M., 2017. A hybrid intrusion detection system for virtual jamming attacks on wireless networks. Measurement 109, 79–87.
Saxena, N., Grijalva, S., Chaudhari, N.S., 2016. Authentication Protocol for an IoT-Enabled LTE Network. ACM Trans. Internet Technol. 16 (4), 1–20. http://dx.doi.org/10.1145/2981547.
Saxena, N., Roy, A., Kim, H., 2017. Efficient 5g small cell planning with embms for optimal demand response in smart grids. IEEE Trans. Ind. Inform. 13 (3), 1471–1481.
Scarlata, V., Levine, B., Shields, C., 2001. Responder anonymity and anonymous peer-to-peer file sharing. In: Proceedings of the Ninth International Conference Netw. Protoc. ICNP IEEE Comput. Soc, pp. 272–280. http://dx.doi.org/10.1109/ICNP.2001.992907.
Seddigh, N., Nandy, B., Makkar, R., Beaumont, J., 2010. Security advances and challenges in 4G wireless networks. In: 2010 Proceedings of the Eighth International Conference Privacy, Secur. Trust, IEEE, pp. 62–71. http://dx.doi.org/10.1109/PST.2010.5593244.
Seo, H., Lee, K.-D., Yasukawa, S., Peng, Y., Sartori, P., 2016. LTE evolution for vehicle-to-everything services. IEEE Commun. Mag. 54 (6), 22–28. http://dx.doi.org/10.1109/MCOM.2016.7497762.
Shao, Z., 2004. Efficient deniable authentication protocol based on generalized ElGamal signature scheme. Comput. Stand. Interfaces 26 (5), 449–454. http://dx.doi.org/10.1016/j.csi.2003.11.001.
Sharma, M.J., Leung, V.C., 2012. IP Multimedia subsystem authentication protocol in LTE-heterogeneous networks. Human.-Centr. Comput. Inf. Sci. 2 (1), 16. http://dx.doi.org/10.1186/2192-1962-2-16.
Shen, N., Yang, J., Yuan, K., Fu, C., Jia, C., 2016. An efficient and privacy-preserving location sharing mechanism. Comput. Stand. Interfaces 44, 102–109. http://dx.doi.org/10.1016/j.csi.2015.06.001.
Singh, S., Saxena, N., Roy, A., Kim, H., 2017. A survey on 5G network technologies from social perspective. IETE Tech. Rev. 34 (1), 30–39. http://dx.doi.org/10.1080/02564602.2016.1141077.

Song, R., 2010. Advanced smart card based password authentication protocol. Comput. Stand. Interfaces 32 (5–6), 321–325. http://dx.doi.org/10.1016/j.csi.2010.03.008.
Sood, S.K., Sarje, A.K., Singh, K., 2011. A secure dynamic identity based authentication protocol for multi-server architecture. J. Netw. Comput. Appl. 34 (2), 609–618. http://dx.doi.org/10.1016/j.jnca.2010.11.011.
Sood, S.K., Sarje, A.K., Singh, K., An improvement of Xu et al.'s authentication scheme using smart cards. In: Proceedings of the Third Annual ACM Bangalore Conference - Comput. '10, ACM Press, New York, New York, USA, 2010, pp. 1–5. http://dx.doi.org/10.1145/1754288.1754303.
Sou, S.-I., Lin, C.-S., 2017. Random packet inspection scheme for network intrusion prevention in LTE core networks. IEEE Trans. Veh. Technol., 1. http://dx.doi.org/10.1109/TVT.2017.2675454.
Sun, H.-M., Chen, Y.-H., Lin, Y.-H., 2012. oPass: a user authentication protocol resistant to password stealing and password reuse attacks. IEEE Trans. Inf. Forensics Secur 7 (2), 651–663. http://dx.doi.org/10.1109/TIFS.2011.2169958.
Sun, Hung-Min, Ting, Wei-Chih, 2009. A Gen2-based RFID authentication protocol for security and privacy. IEEE Trans. Mob. Comput. 8 (8), 1052–1062. http://dx.doi.org/10.1109/TMC.2008.175.
Sun, J., Zhang, C., Zhang, Y., Fang, Y., 2010. An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Trans. Parallel Distrib. Syst. 21 (9), 1227–1239.
Sun, J., Zhang, R., Jin, X., Zhang, Y., 2016. SecureFind: secure and privacy-preserving object finding via mobile crowdsourcing. IEEE Trans. Wirel. Commun. 15 (3), 1716–1728. http://dx.doi.org/10.1109/TWC.2015.2495291.
Tehrani, M.N., Uysal, M., Yanikomeroglu, H., 2014. Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions. IEEE Commun. Mag. 52 (5), 86–92. http://dx.doi.org/10.1109/MCOM.2014.6815897.
Terzis, I., Kambourakis, G., Karopoulos, G., Lambrinoudakis, C., 2011. Privacy preserving context transfer schemes for 4G networks. Wirel. Commun. Mob. Comput. 11 (2), 289–302. http://dx.doi.org/10.1002/wcm.1019.
Thayer Fábrega, F.J., Herzog, J.C., Guttman, J.D., 1999. Strand spaces: proving security protocols correct. J. Comput. Secur. 7 (2–3), 191–230. http://dx.doi.org/10.3233/JCS-1999-72-304.
Tuyls, P., Batina, L., 2006. RFID-Tags for Anti-counterfeiting. In: Cryptogr. Track RSA Conference, pp. 115–131. http://dx.doi.org/10.1007/11605805_8.
Ulltveit-Moe, N., Oleshchuk, V.A., Køien, G.M., 2011. Location-aware mobile intrusion detection with enhanced privacy in a 5G context. Wirel. Pers. Commun. 57 (3), 317–338. http://dx.doi.org/10.1007/s11277-010-0069-6.
Vodafone News, 2016. URL ⟨http://www.vodafone.com/content/index/what/technology-blog/5g-high-frequency.html⟩.
Wang, M., Yan, Z., 2017. A survey on security in d2d communications. Mob. Netw. Appl. 22 (2), 195–208.
Wang, M., Chen, J., Aryafar, E., Chiang, M., 2017. A survey of client-controlled hetnets for 5G. IEEE Access 5, 2842–2854. http://dx.doi.org/10.1109/ACCESS.2016.2624755.
Wang, T., Liu, Y., Vasilakos, A.V., 2015. Survey on channel reciprocity based key establishment techniques for wireless systems. Wirel. Netw. 21 (6), 1835–1846.
Wang, X., Vasilakos, A.V., Chen, M., Liu, Y., Kwon, T.T., 2012. A survey of green mobile networks: opportunities and challenges. Mob. Netw. Appl. 17 (1), 4–20.
Wang, Y., Chu, W., Fields, S., Heinemann, C., Reiter, Z., 2016. Detection of intelligent intruders in wireless sensor networks. Futur Internet 8 (1), 2. http://dx.doi.org/10.3390/fi8010002.
Wang, D., Wang, P., Liu, J., 2014. Improved privacy-preserving authentication scheme for roaming service in mobile networks. In: Proceedings of IEEE Wireless Communication Networks Conference, IEEE, pp. 3136–3141. http://dx.doi.org/10.1109/WCNC.2014.6953015.
Wang, L.-C., Rangapillai, S., 2012. A survey on green 5G cellular networks. In: Proceedings of International Conference on Signal Processing and Communication, IEEE, pp. 1–5. http://dx.doi.org/10.1109/SPCOM.2012.6290252.
Wei, Z., Yuan, J., Ng, D.W.K., Elkashlan, M., Ding, Z, 2016. A Survey of Downlink Non-orthogonal Multiple Access for 5G Wireless Communication Networks URL http://arxiv.org/abs/1609.01856arXiv:1609.01856.
Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W., 2004. Security and privacy aspects of low-cost radio frequency identification systems. Secur. pervasive Comput., 201–212. http://dx.doi.org/10.1007/978-3-540-39881-3_18.
Weis, S.A., 2003. Security and privacy in radio-frequency identification devices, Weis, S. A., 2003. Security and privacy in radio-frequency identification devices, Ph.D. Thesis, Massachusetts Institute of Technology.
Wen, F., Li, X., 2012. An improved dynamic ID-based remote user authentication with key agreement scheme. Comput. Electr. Eng. 38 (2), 381–387. http://dx.doi.org/10.1016/j.compeleceng.2011.11.010.
Wu, J., Zhang, Y., Zukerman, M., Yung, E.K.-N., 2015. Energy-efficient base-stations sleep-mode techniques in green cellular networks: a survey. IEEE Commun. Surv. Tutor. 17 (2), 803–826. http://dx.doi.org/10.1109/COMST.2015.2403395.
Wu, L., Zhang, Y., Wang, F., 2009. A new provably secure authentication and key agreement protocol for SIP using ECC. Comput. Stand. Interfaces 31 (2), 286–291. http://dx.doi.org/10.1016/j.csi.2008.01.002.
Wu, T.-Y., Tseng, Y.-M., 2010. An efficient user authentication and key exchange protocol for mobile client-server environment. Comput. Netw. 54 (9), 1520–1530. http://dx.doi.org/10.1016/j.comnet.2009.12.008.
Xenakis, D., Passas, N., Merakos, L., Verikoukis, C., 2014. Mobility management for femtocells in LTE-advanced: key aspects and survey of handover decision algorithms. IEEE Commun. Surv. Tutor. 16 (1), 64–91. http://dx.doi.org/10.1109/SURV.2013.060313.00152.
Xu, J., Zhu, W.-T., Feng, D.-G., 2009. An improved smart card based password authentication scheme with provable security. Comput. Stand. Interfaces 31 (4), 723–728. http://dx.doi.org/10.1016/j.csi.2008.09.006.
Xu, J., Zhu, W.-T., Feng, D.-G., 2011. An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. Comput. Commun. 34 (3), 319–325. http://dx.doi.org/10.1016/j.comcom.2010.04.041.
Y. Park, T. Park, A Survey of Security Threats on 4G Networks, in: 2007 IEEE Globecom Work., IEEE, 2007 1 6 doi: 10.1109/GLOCOMW.2007.4437813.
Yan, Z., Zhang, P., Vasilakos, A.V., 2016. A security and trust framework for virtualized networks and software-defined networking. Secur. Commun. Netw. 9 (16), 3059–3069.
Yao, J., Wang, T., Chen, M., Wang, L., Chen, G., 2016. GBS-AKA: Group-Based Secure Authentication and Key Agreement for M2M in 4G Network. In: proceedings of International Conference Cloud Computing and Research Innovation, IEEE, pp. 42–48. http://dx.doi.org/10.1109/ICCCRI.2016.15.
Yassin, M., AboulHassan, M.A., Lahoud, S., Ibrahim, M., Mezher, D., Cousin, B., Sourour, E.A., 2017. Survey of ICIC techniques in LTE networks under various mobile environment parameters. Wirel. Netw. 23 (2), 403–418. http://dx.doi.org/10.1007/s11276-015-1165-z.
Yoon, E.-J., Yoo, K.-Y., 2013. Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. J. Supercomput. 63 (1), 235–255. http://dx.doi.org/10.1007/s11227-010-0512-1.
Yoon, E.-J., Yoo, K.-Y., 2010. A new efficient id-based user authentication and key exchange protocol for mobile client-server environment. In: Proceedings of International Conference on Wireless Information Technology System, IEEE, pp. 1–4. http://dx.doi.org/10.1109/ICWITS.2010.5611903.
Zhang, A., Chen, J., Hu, R.Q., Qian, Y., 2016. SeDS: secure data sharing strategy for D2D communication in LTE-advanced networks. IEEE Trans. Veh. Technol. 65 (4), 2659–2672. http://dx.doi.org/10.1109/TVT.2015.2416002.
Zhang, G., Fan, D., Zhang, Y., Li, X., Liu, X., 2015. A privacy preserving authentication scheme for roaming services in global mobility networks. Secur. Commun. Netw. 8 (16), 2850–2859. http://dx.doi.org/10.1002/sec.1209.
Zhang, Z., Chai, X., Long, K., Vasilakos, A.V., Hanzo, L., 2015a. Full duplex techniques for 5G networks: self-interference cancellation, protocol design, and relay selection. IEEE Commun. Mag. 53 (5), 128–137.
Zhang, Z., Wang, X., Long, K., Vasilakos, A.V., Hanzo, L., 2015b. Large-scale mimo-based wireless backhaul in 5G networks. IEEE Wirel. Commun. 22 (5), 58–66.
Zhang, Z., Long, K., Vasilakos, A.V., Hanzo, L., 2016. Full-duplex wireless communications: challenges, solutions, and future research directions. Proc. IEEE 104 (7), 1369–1409.
Zhang S., Wu, Q., Xu, S., Li, G.Y., 2016c. Fundamental Green Tradeoffs: Progresses, Challenges, and Impacts on 5G Networks http://arxiv.org/abs/1604.07918arXiv:1604.07918, http://dx.doi.org/10.1109/COMST.2016.2594120.
Zhioua, G.E.M., Labiod, H., Tabbane, N., Tabbane, S., 2013. LTE advanced relaying standard: a survey. Wirel. Pers. Commun. 72 (4), 2445–2463. http://dx.doi.org/10.1007/s11277-013-1157-1.
Zhou, J., Cao, Z., Dong, X., Xiong, N., Vasilakos, A.V., 2015a. 4s: a secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Inf. Sci. 314, 255–276.
Zhou, J., Dong, X., Cao, Z., Vasilakos, A.V., 2015b. Secure and privacy preserving protocol for cloud-based vehicular. IEEE Trans. Inf. Forensics Secur. 10 (6), 1299–1314.
Zhou, S., Zhang, Z., Luo, Z., Wong, E.C., 2010. A lightweight anti-desynchronization RFID authentication protocol. Inform. Syst. Front. 12 (5), 521–528. http://dx.doi.org/10.1007/s10796-009-9216-6.
Zhou, T., Xu, J., 2011. Provable secure authentication protocol with anonymity for roaming service in global mobility networks. Comput. Netw. 55 (1), 205–213. http://dx.doi.org/10.1016/j.comnet.2010.08.008.
Zhu, Haojin, Lin, Xiaodong, Shi, Minghui, Ho, Pin-Han, Shen, Xuemin, 2009. PPAB: a privacy-preserving authentication and billing architecture for metropolitan area sharing networks. IEEE Trans. Veh. Technol. 58 (5), 2529–2543. http://dx.doi.org/10.1109/TVT.2008.2007983.
Zhuang, X., Zhu, Y., Chang, C.-C, 2016. A New Ultralightweight RFID Protocol for Low-Cost, Wirel. Pers. Commun. (3) 1787–1802. http://dx.doi.org/10.1007/s11277-014-1958-x.

Dr. Mohamed Amine Ferrag received the bachelor's, master's, and Ph.D. degrees from Badji Mokhtar Annaba University, Algeria, in 2008, 2010, and 2014, respectively, all in computer science. Since 2014, he has been an Assistant Professor with the Department of Computer Science, Guelma University, Algeria. Since 2010, he has also been a Researcher Member of the Networks and Systems Laboratory, Badji Mokhtar University, Annaba. He has edited the book Security Solutions and Applied Cryptography in Smart Grid Communications (IGI Global). His research interests include wireless network security, network coding security, and applied cryptography. He is currently serving in various editorial positions, such as Editorial Board Member of Computer Security Journals, such as the International Journal of Information Security and Privacy (IGI Global), the International Journal of Internet Technology and Secured Transactions (Inderscience Publishers), and the EAI Endorsed Transactions on Security and Safety. He has served as an organizing committee member (the Track Chair, the Co-Chair, the Publicity Chair, the Proceedings Editor, and the Web Chair) in numerous international conferences.

Dr. Leandros A. Maglaras is a Lecturer in the School of Computer Science and Informatics of De Montfort University conducting research in the Cyber Security Centre & Software Technology Research Laboratory. He obtained the B.Sc. (M.Sc. equivalent) in Electrical and Computer Engineering from Aristotle University of Thessaloniki, Greece in 1998, M.Sc. in Industrial Production and Management from University of Thessaly in 2004 and M.Sc. and PhD degrees in Electrical & Computer Engineering from University of Thessaly, in 2008 and 2014 respectively. During 2014 he was a Research Fellow at University of Surrey, Department of Computing, on the FP7 CockpitCI project. He served on the Editorial Board of several International peer-reviewed journals such as Wiley Journal on Security & Communication Networks. He is a Senior Member of the Institute of Electrical & Electronic Engineers (IEEE).

Dr. Antonios Argyriou received the Diploma degree in electrical and computer engineering from Democritus University of Thrace, Xanthi, Greece, and the M.S. and Ph.D. degrees in electrical and computer engineering (as a Fulbright Scholar) from Georgia Institute of Technology, Atlanta, GA, USA, in 2001, 2003, and 2005, respectively. Currently, he is an Assistant Professor with the Department of Electrical and Computer Engineering, University of Thessaly, Volos, Greece. From 2007–2010, he was a Senior Research Scientist with Philips Research, Eindhoven, The Netherlands. From 2004–2005, he was a Senior Engineer with Soft. Networks, Atlanta, GA, USA. He currently serves on the Editorial Board of the Journal of Communications. His research interests include wireless communication systems and networks, and video delivery. He has also served as Guest Editor for the IEEE TRANSACTIONS ON MULTIMEDIA Special Issue on Quality-Driven Cross-Layer Design, and he was also a Lead Guest Editor for the Journal of Communications, Special Issue on Network Coding and Applications. He serves on the TPCs of several international conferences and workshops in the area of communications, networking, and statistical signal processing.

Dimitrios Kosmanos is a PhD student at the Department of Electrical & Computer Engineering, University of Thessaly, Greece since 2014. He received a MSc degree at the same University. Before his current position, he was collaborating as fellow researcher with the CERTH department of Volos. He was interested in optimized video transmission techniques in wireless cooperative networks. His current research interests were techniques for improved detection and suppressing jamming threats in 802.11p WIFI protocol for Vehicular Ad Hoc Networks and specifically for autonomous vehicles.

Prof. Helge Janicke obtained his first degree in “practical informatics” from the University of Applied Sciences, Emden (Germany). During his doctoral studies he was funded by the Data and Information Fusion Defence Technology Centre (DIF-DTC), a research consortium of high-tech companies and universities which formed a key plank of the UK Government's future vision for defence technology development. He was awarded his PhD in 2007 from De Montfort University (DMU) and subsequently worked for the DIF-DTC consortium as a Research Fellow, funded jointly by QinetiQ and the Ministry of Defence. In 2008, Janicke worked for the University of Leicester as a Teaching Fellow leading several modules on software engineering, quality assurance and measurement theory.