IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 8, 2016, accepted July 24, 2016, date of publication August 18, 2016, date of current version September 16, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2601009

Survey on Threats and Attacks on Mobile Networks

SILVÈRE MAVOUNGOU[1], GEORGES KADDOUM[1], (Member, IEEE), MOSTAFA TAHA[2], (Member, IEEE), AND GEORGES MATAR[1]

[1]Laboratory of Communications and Integrated Microelectronics, École de Technologie Supérieure, Montreal, QC H3C 1K3, Canada
[2]Electrical Engineering Department, Assiut University, Asyut 71515, Egypt

Corresponding author: S. Mavoungou (smavoungou@hotmail.com)

This work was supported by the ETS' Research Chair of Physical Layer Security in Wireless Networks.

ABSTRACT Since the 1G of mobile technology, mobile wireless communication systems have continued to evolve, bringing into the network architecture new interfaces and protocols, as well as unified services, high data capacity of data transmission, and packet-based transmission (4G). This evolution has also introduced new vulnerabilities and threats, which can be used to launch attacks on different network components, such as the access network and the core network. These drawbacks stand as a major concern for the security and the performance of mobile networks, since various types of attacks can take down the whole network and cause a denial of service, or perform malicious activities. In this survey, we review the main security issues in the access and core network (vulnerabilities and threats) and provide a classification and categorization of attacks in mobile network. In addition, we analyze major attacks on 4G mobile networks and corresponding countermeasures and current mitigation solutions, discuss limits of current solutions, and highlight open research areas.

INDEX TERMS Mobile network security, availability attacks, confidentiality attacks, integrity attacks, authentication attacks, impersonation attacks, trusted Computing, Intrusion Detection, signaling attacks, spoofing attacks, flooding attacks.

NOMENCLATURE

1G	First Generation of Mobile Networks
2G	Second Generation of Mobile Networks
3G	Third Generation of Mobile Networks
3GPP	Third Generation Partnership Project
4G	Fourth Generation of mobile networks
AAA	Authentication Authorization and Accounting
ACK	Acknowledgment
AKA	Authentication and Key Agreement
AS	Access Stratum
AuC	Authentication Center
AWGN	Additive White Gaussian Noise
AUTN	Authentication Token Number
AV	Authentication Vectors
BER	Bit Error Rate
BS	Base Station
BSC	Base Station Controller
BSS	Base Station Subsystem
BW	Bandwidth
CA	Content-Aware
CIDS	Cooperative Intrusion Detection System
CDMA	Code Division Multiple Access
CFI	Control Format Indicator
CM	Connection Management
CMC	Cipher Mode Command
CN	Core Network
C-plane	Control Plane
C-RNTI	Cell Radio Network Temporary Identifier
CQI	Channel Quality Indicator
CS-RS	Cell-Specific Reference Signal
CS	Circuit Switched
CSI	Channel State Information
CTS	Clear To Send
CUSUM	Cumulative Sums
DoS	Denial of Service
DDoS	Distributed Denial of Service
DMSI	Dynamic Mobile Subscriber Identity
DPI	Deep Packet Inspection
EAP	Extensible Authentication Protocol
ECN	Explicit Congestion Notification
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway

EPS	Evolved Packet System
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
eNB	Evolved Node B
GBR	Guaranteed Bit Rate
GGSN	GPRS Gateway Support Node
Gi	GGSN interconnection interface with external PDN
GMM	GPRS Mobility Management
GPRS	General Packet Radio Service
GSM	Global Service Mobile system
GTP	GPRS Tunneling Protocol
GUTI	Globally Unique Temporary Identifier
HARQ	Hybrid Automatic Repeat Request
HeNB	Home Evolved Node B
HLR	Home Location Register
HN	Home Network
HSS	Home Subscriber Server
HSPA	High Speed Packet Access
ICMP	Internet Message Control Protocol
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPS	Intrusion Protection System
ITU	International Telecommunications Union
Kc	Ciphering key
LAI	Location Area Identity
LAN	Local Area Network
LTE	Long Term Evolution
LTE-A	Long Term Evolution-Advanced
M2M	Machine to Machine
MAC	Medium Access Control
MCS	Modulation Coding Scheme
ME	Mobile Equipment
MIB	Master Information Block
MIMO	Multiple Input Multiple Output
MITM	Man-In-The-Middle
MM	Mobility Management
MNO	Mobile Network Operators
MME	Mobility Management Entity
MS	Mobile Station
MSI	Modulation Scheme Indicator
MSC	Mobile Switching Center
MTC	Mobile Trust Computed
NACK	Non acknowledgment
NAS	Non-Access Stratum
OFDM	Orthogonal Frequency Division Multiplexing
PBCH	Physical Broadcast Channel
PCFICH	Physical Control Format Indicator Channel
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDSCH	Physical Downlink Shared Channel
PDU	Packet Data Unit
P-GW	Packet Data Network Gateway
PHICH	Physical Hybrid-ARQ Indicator Channel
PLMN	Public Land Mobile Network
PRACH	Physical Random Access Channel
PRB	Physical Resource Block
PS	Packet Switched
PSS	Primary and Secondary Synchronization Signals
PUCCH	Physical Uplink Control Channel
PUSCH	Physical Uplink Shared Channel
QoS	Quality of Service
QoE	Quality of Experience
RAB	Radio Access Bearer
RAN	Radio Access Network
RAND	Random Number
RAT	Radio Access Technology
RCS	Rich Communication Services
RID	Random Identity
RES	Signed Response
RLC	Radio Link Control
RNC	Radio Node Controller
RRC	Radio Resource Control
RTS	Ready To Send
S1	Radio interface between evolved node B, MME and S-GW
S1-C	Control plane interface between evolved node B and MME or S1-MME
S1-U	user plane interface between evolved node B and S-GW
S11	control plane interface for EPS management between MME and S-GW
SAE	System Architecture Evolution
SCTP	Stream Control Transmission Protocol
SDR	Software Defined Radio
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SGi	interconnection interface to external PDN
SIB	System Information Block
SIP	Session Initiation Protocol
SM	Session Management
SN	Serving Network
SNID	Service Network Identity
SNR	Signal-to-Noise Ratio
SQN	Sequence Number
SS7	Signaling System Number 7
SYN	Synchronization
TAU	Tracking Area Update
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TA	Tracking Area
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Telecommunication Mobile System
U-plane	User Plane
USIM	User Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register
VoLTE	Voice over LTE
VPN	Virtual Private Network

WCDMA	WideBand Code Division Multiple Access
WiFi	Ethernet 802.11 wireless technologies
WLAN	Wireless Local Area Network
WiMAX	Worldwide Interoperability for Microwave Access
X2AP	X2 Application protocol
X2	Interface between eNBs
X2-C	Control plane interface between eNBs
X2-U	User plane interface between eNBs

I. INTRODUCTION

In the last recent decades, the mobile experience has been expanding everywhere, and almost 25 billion of devices are expected to be interconnected by 2020 due to the always-available connectivity, enabling a fast, reliable, longer, real-time and on-the-go connection [1]–[3]. This great mobile experience is powered by evolving mobile technologies. In fact, four generations of technologies have shaped the mobile network evolution, starting from the First Generation of Mobile Networks (1G) in the early 1980s. The 1G technology consists of analog-based systems, which have established seamless mobile connectivity introducing mobile voice services (speech transmission). Subsequently, the Second Generation of Mobile Networks (2G) has emerged, whose implementation started by the end of 1980s. 2G is a digital wireless system using multiple access technologies such as Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA), making it more efficient in terms of data services, mobility management and spectrum efficiency. It has also increased voice capacity delivering mobile to the masses, enabled low bit rate data services, and was supported by several standards, such as the Global Service Mobile system (GSM) based on TDMA, and IS95 based on CDMA. A tremendous achievement in GSM was the introduction of distinct platforms of services such as the Voice Mail Service (VMS) and the Short Message Service Center (SMSC).

After 2G, the Third Generation of Mobile Networks (3G) brought the "*mobile broadband experience*" by enabling a high speed data transmission. Similarly to the 2G, two competing standards have played key roles in the evolution of the 3G [1]: 1) CDMA2000/TD-SCDMA and 2) WideBand Code Division Multiple Access (WCDMA)/Universal Telecommunication Mobile System (UMTS). The 3G continued its evolution towards a better connectivity, carrier aggregation, higher data rates, and enhanced mobile broadband experiences. This evolution has recently become a reality with the emerging and deployment of the Fourth Generation of mobile networks (4G), giving access to a wide range of applications and services based on the Internet Protocol (IP).

In fact, 4G provides mobile networks with the ability to deliver more capacity for faster and better mobile broadband experiences, and keeps continuously evolving to provide more data capacity, as well as fast and real-time connections. A major evolution in 4G resides in the air interface which has introduced a simplified All-IP network architecture. This constitutes the fundamental advantage over the 3G, as the Radio Node Controller (RNC) and Base Station Controller (BSC) functionalists have been distributed among Evolved Node B (eNB)s, servers and gateways.

In the meantime, the explosion of the mobile subscribers combined with the multiplicity of wireless devices have revealed an urgent need to build an efficient mobile network, which can be achieved by the 4G mobile networks architecture. However, as the 4G architecture allows inter-operation between different wireless technologies, the impact of services on network efficiency and security has become more critical. In fact, many mobile network architectural designs are still being developed by taking into account compatibility and interoperability requirements with previous existing technologies (2G, and 3G). This coexistence and seamless interoperability between various network technologies in 4G raise security issues [4]–[7]. Contrarily to the 1G and 2G, 3G and 4G have introduced the most significant impact in the network architecture. As a result, it became paramount to consider aspects such as network interoperability, availability and security when designing a mobile network solution [8]. Moreover, because of the evolution in the mobile technology, many new challenges have surfaced. First, the new standard introduced complexity in the network architecture, as well as security issues in relation with confidentiality, integrity and authenticity [9]. Second, the emergence of mobile computing has opened a large scale of applications and services for mobile devices bringing many security issues facing the mobile device itself as well as the entire network. In fact, mobile networks vulnerabilities against various types of threats such as interface flooding, network element crashing, traffic eavesdropping, unauthorized data access, traffic modification, data modification on a network element, compromising of a network element, malicious insider, theft of service, etc. have been reported by several research papers [10]–[19]. Typical threats in 4G include attacks at the inter-networking with GSM and UMTS, signaling Denial of Service (DoS) attacks, network impersonation attacks, cryptographic attacks, IP-based attacks (including GTP-based and diameter-based attacks), jamming-based DoS attacks, spoofing attacks, Man-In-The-Middle (MITM) attacks, etc.

Although there has been a continuously growing interest in this domain, few surveys have been committed to investigate threats and attacks in 4G mobile networks. The Long Term Evolution (LTE) security and privacy threats in the radio link, as well as the security issues related to the integration of the Wireless Local Area Network (WLAN) with LTE networks have been analyzed in [20]–[26]. In [22], authors review requirements for the design of key features for session and bearer control in LTE. In [21] and [24], authors particularly review the security architectures and vulnerabilities in 4G mobile networks such as traffic redirection and resynchronisation attacks from the mobile terminal to the home network in LTE. Physical layer security has been reviewed in [24] and [27]. In particular, authors in [24] investigate

security threats on the physical layer of Worldwide Interoperability for Microwave Access (WiMAX) and LTE, and also propose Radio Resource Control (RRC) ciphering and user plane protection. Vulnerabilities related to RRC signaling have been examined in [26].

In [17] and [28], IP threats related to GPRS Tunneling Protocol (GTP) and diameter protocol vulnerabilities have been analyzed. As a countermeasure, the solution proposed is based on intrusion detection and prevention system capable of capturing 4G network control and data traffic on control plane interface for EPS management between MME and S-GW (S11) and user plane interface between evolved node B and S-GW (S1-U). Moreover, this solution also includes proactive and reactive approaches to detect and mitigate diameter related attacks using anomaly and a signature-based detection.

In [6], [8], [10], [11] and [29]–[33], vulnerabilities related to the authentication and key agreement in LTE are examined. Different Authentication and Key Agreement (AKA) schemes have been proposed.

The mobility management in LTE, and the handover authentication procedure in heterogeneous networks (LTE and non-Third Generation Partnership Project (3GPP) access network) have been discussed in [13] and [34]–[38]. Different schemes have been proposed including a uniform handover authentication scheme to provide mutual authentication, key agreement, protection against MITM, replay attacks, user anonymity, and perfect forward secrecy. They also proposed an algorithm for the selection of an optimal key update interval to mitigate the effects of a desynchronization attack and handover key compromise.

In [18], [19] and [39]–[41], authors have reviewed the physical layer security threats. Typical threats such as eavesdropping and jamming the LTE air interface are deeply analyzed. Different countermeasures and open research issues including information-theoretic security, artificial noise aided security, security-oriented beamforming techniques, diversity-assisted security approaches, and physical-layer secret key generation are also presented. In [42] and [43], authors have carried out a review of threats and attacks on mobile devices, which includes attacks methodologies and goals. They have also identified five sensitive areas in the General Packet Radio Service (GPRS) architecture that can constitute threat entry points to perform attacks both on mobile devices and mobile networks. Typical entry points highlighted in this paper include the mobile station (Mobile Station (MS)), the SIM-card, an interface between the MS and Serving GPRS Support Node (SGSN), the GPRS backbone network (IP and Signaling System Number 7 (SS7)), and the interconnection between different Packet Data Network (PDN)s (particularly the Gp/S8 interface connecting the Mobile Network Operators (MNO) to roaming partners networks, giving them access to internal packet core services and data). In addition, the internet access over the GGSN interconnection interface with external PDN (Gi) and interconnection interface to external PDN (SGi) interfaces, which are used to connect various user devices to the internet and other non-trusted networks, can be exploited to expose the GPRS network elements and the mobile subscribers to a large broad of threats from the internet. Typical threats may include bandwidth saturation, data flooding, spoofing or cache poisoning, and hijacking of a legitimate user's IP address.

In this paper, we are motivated to provide an overview of threats and attacks in mobile networks as well as current solutions and countermeasures, and discuss possible future threats in the next generation of mobile networks. The main contribution of our paper is to draw an inventory of attacks in 4G networks, and to provide an attack categorization and classification (attack reference map) with the corresponding mitigation solution. We specially focus on IP-based attacks, signaling attacks and jamming based attacks.

The remainder of this paper is organized as follows. Section II reviews some background about the current security architecture, including the inter-operation architecture between previous and other existing technologies. In Section III we provide an overview of vulnerabilities, threats, and attacks landscape in mobile networks. Section IV focuses on the threats and attacks as well as current countermeasures and mitigation solutions in 4G. Section V discusses open research problems. The paper is concluded in Section VI.

II. BACKGROUND OF 4G ARCHITECTURE EVOLUTION

In this section, we present the 4G network architecture by focusing on the security architecture and interface protocol. The 4G technology is the first global standard for mobile broadband issued by the International Telecommunications Union (ITU) in order to provide more data capacity, as well as a migration path for 2G and other standards such as GSM and CDMA by facilitating the convergence of wireless technology.

It has been built based on the requirement to migrate to an All-IP architecture in order to achieve a standardization of all existing technologies platform. A major evolution in 4G resides in the air interface, also referred to as LTE, which has introduced a simplified All-IP network architecture. This constitutes the fundamental difference with the 3G, due to the fact that in 4G the Radio Network Controller (RNC) and BSC functionalities are distributed among Evolved Node B (eNBs), servers and gateways. In comparison with 2G and 3G, the radio access network in 4G, which is known as the UMTS Terrestrial Radio Access Network (UTRAN), is fully All-IP. 4G offers many advantages such as backward compatibility with 2G and 3G systems and the capability to encompass systems from various networks technologies. Its primary goal is to improve spectral efficiency, bandwidth and throughput through deployment of cost effective network elements based on open standards with improved data and application services for the end users. The 4G has been designed to support low latency, high level of security, and different Quality of Service (QoS) [22], [44], [45].

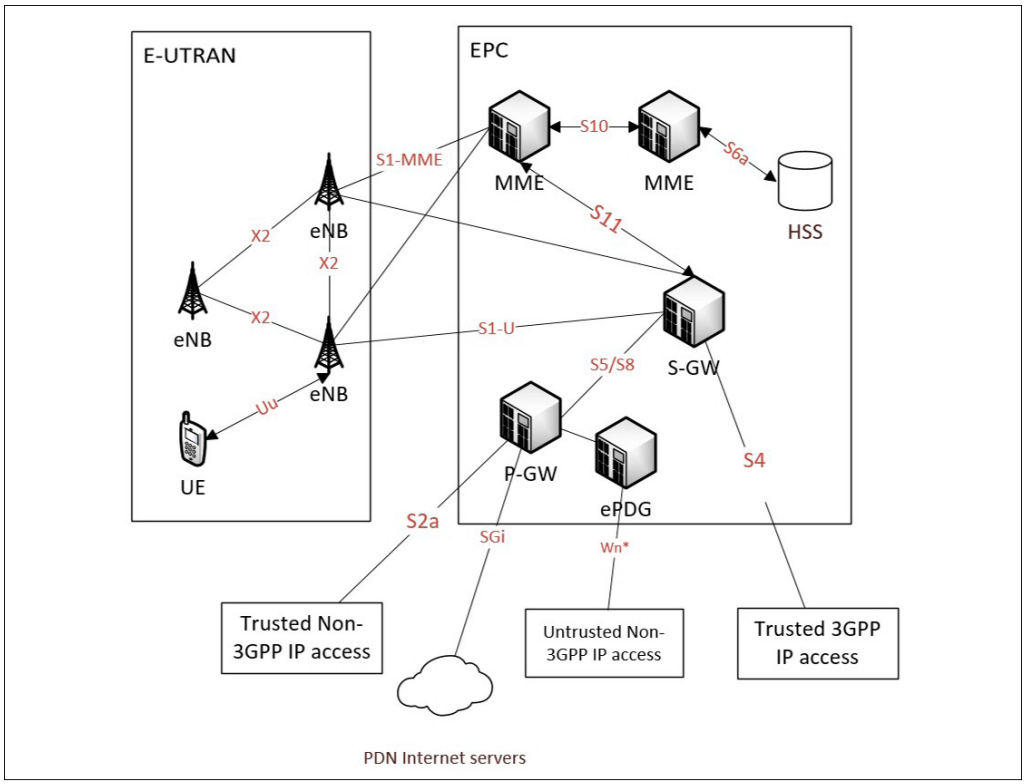

FIGURE 1. LTE Architecture overview.

A. 4G NETWORK COMPONENTS

The architecture of 4G mobile network as specified in the System Architecture Evolution (SAE) and Evolved Packet System (EPS) by the 3GPP is described in [46]. As shown in Fig. 1, the evolution towards 4G has introduced two major changes in the mobile network architecture.

The first change is related to the replacement of the Packet Switched (PS) domain inherited from 2G/3G by the Evolved Packet Core (EPC). The second change consists of the replacement of the UTRAN by the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).

The EPC is responsible for the overall control of the User Equipment (UE) and the establishment of bearers and communication with external PDN, private corporate networks and IP Multimedia Subsystem (IMS). The main functions of logical nodes of the EPC can be summarized as follows:

- Home Subscriber Server (HSS): consists of a data base containing users subscription information such as QoS profile and other data related to access restrictions to roaming, dynamic identity of the MME to which the user is registered. The Authentication Center (AuC), which generates the authentication vectors and security keys, can be integrated in the HSS.
- Packet Data Network Gateway (P-GW): serves as the contact point with external networks through the SGi, and is responsible for allocating the IP address to the UE. It is also responsible of filtering of downlink users IP packets into different QoS-based bearers.
- Serving Gateway (S-GW): acts as router between the E-UTRAN and the P-GW, and also serves as the local mobility anchor for the data bearers during inter-eNB handover, and inter-operation with other 3GPP technologies (GPRS and UMTS). It is responsible of transferring all the IP traffic from users, gathering information for charging in the visited network, and lawful interception.
- Mobility Management Entity (MME): is the entity in charge of controlling the high-level operation of Mobile Equipment (ME) and other elements of the network, by processing the signaling between the UE and the Core Network (CN). The processing of the signaling messages is achieved using the Non-Access Stratum (NAS) protocols between UE and the CN illustrated in Fig. 2 and Fig. 3.
  The MME functions in the NAS protocol can be classified in two main groups. In the first group, the session management layer is in charge of handling bearers management including the establishment, maintenance and release of the bearers. In the second group, the connection management or mobility management layer is responsible of the connection management.

The E-UTRAN is the access network of LTE, and consists of eNBs as illustrated in Fig. 1. The E-UTRAN

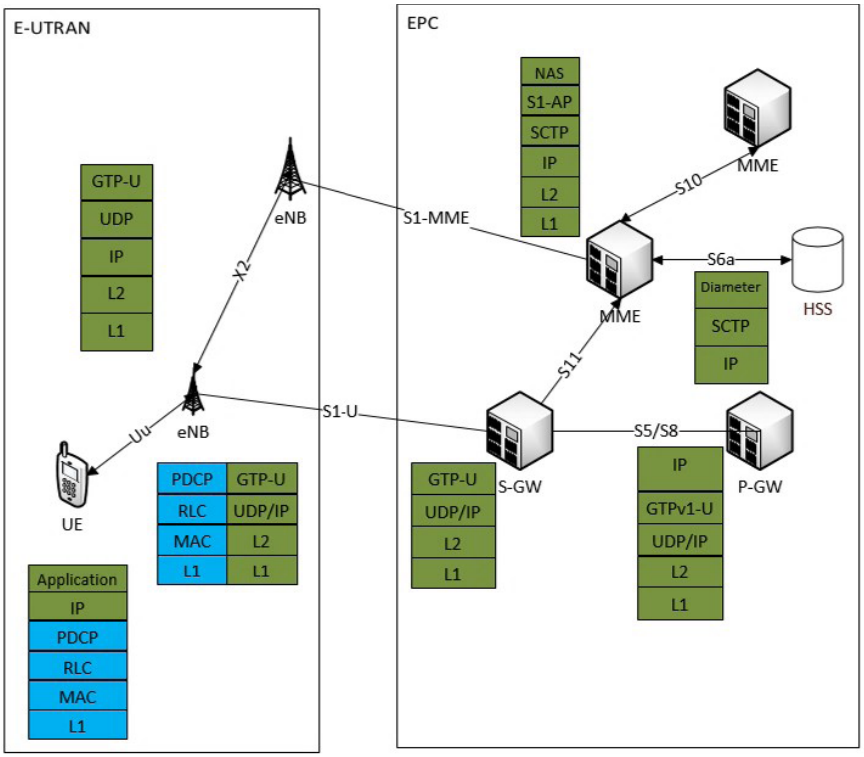

FIGURE 2. LTE User plane protocol stack overview.

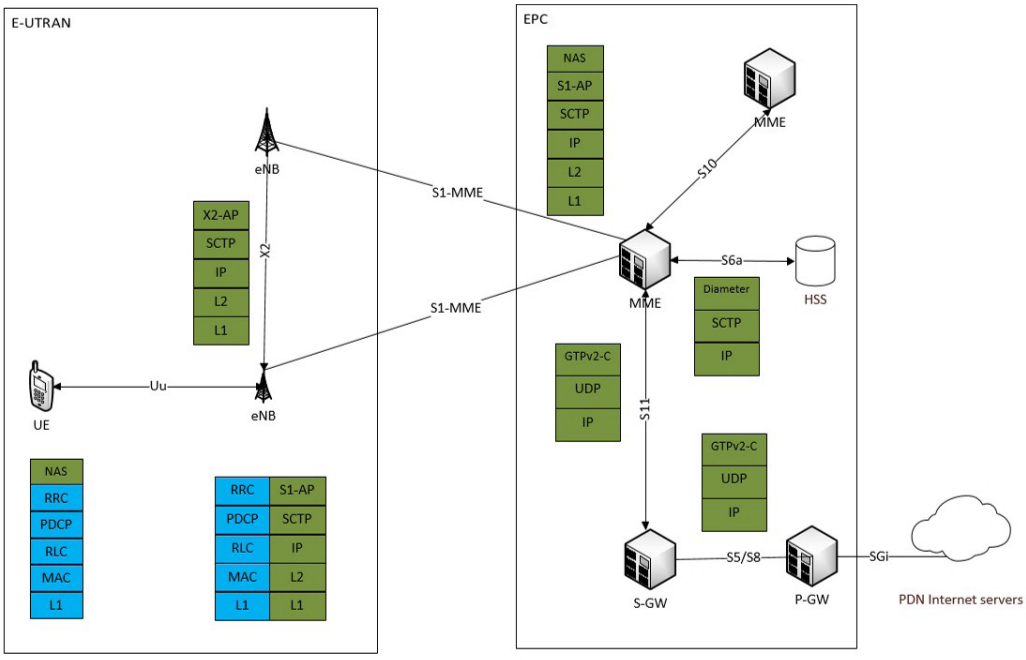

FIGURE 3. LTE Control plane protocol stack overview.

functions consist of radio resource management, compression of IP packet headers, encryption of data sent over the radio interface, and the connectivity with the EPC.

The E-UTRAN provides the E-UTRAN's User Plane (U-plane) and Control Plane (C-plane) protocol terminations towards the UEs, MME, and SAE gateways. It is also in charge of managing radio communications between the

mobile and the EPC. At the heart of the E-UTRAN architecture, eNBs are in charge of controlling MSs inside radio cells. In comparison with the access network of the 3G, the E-UTRAN does not support soft handover state, which causes a limitation of mobile to communicate only with one base station, and one cell in the same time. In addition, each eNB also handles the emission of radio transmissions to all its mobiles on the downlink, and the reception of transmissions from mobiles on the uplink, through the LTE air interface. The eNB is also responsible of the low-level operation control of all its connected mobiles by sending signaling messages such as handover commands related to radio transmissions.

The radio protocol architecture of E-UTRAN comprises a U-plane and a C-plane.

In the U-plane, an IP packet for a UE is encapsulated in an EPC-specific protocol and tunneled between the P-GW and the eNB for transmission to the UE. Different tunneling protocols are used across different interfaces as shown in the E-UTRAN user plane protocol stack in Fig. 2. The U-plane protocols consist of Packet Data Convergence Protocol (PDCP), Radio Link Control (RLC) and Medium Access Control (MAC) sublayers that are terminated in the eNB on the network side.

In the C-plane protocol stack shown in Fig. 3, the low layers protocol stack performs the same functions. In particular, the RRC (known as *Layer 3*) in the Access Stratum (AS) protocol stack is the main controlling function responsible of establishing the radio bearers and configuring all the lower layers using RRC signaling between the eNB and the UE. The difference between the C-plane and U-plane protocol stacks resides in the lack of header compression function for the C-plane.

As illustrated in Fig. 2 and Fig. 3, the green regions show the protocols used in NAS, whereas the blue regions present the AS protocols. Both NAS and AS constitute the two types of security in LTE based on the network location. The AS security is concentrated on the radio link between the UE and eNBs, whereas the NAS security is between the UE and the MME.

To achieve the interconnection between network components inside E-UTRAN and EPC, NAS and AS protocols messages are carried over standardized interfaces illustrated in Fig. 1 [47].

- Radio interface between evolved node B, MME and S-GW (S1): consists of a separation and linking interface between the E-UTRAN and the CN. It comprises two sub-interfaces, one for the C-plane and the other one for the U-plane. In the C-plane, the S1 sub-interface is called Control plane interface between evolved node B and MME (S1-C) or S1-MME and interconnects eNBs with MME. The S1-C protocol is based on the Stream Control Transmission Protocol (SCTP)/IP stack, and carries signaling messages between eNBs with MME. It is also in charge of EPS bearer setup and release procedures, signaling information during handover, and NAS signaling transport. In the U-plane, the S1 sub-interface is called S1-U and uses the GTP/UDP5/IP stack, which has the advantage of facilitating intra-3GPP mobility. S1-U is used for the interconnection between eNB and S-GW. It carries the user traffic by providing non guaranteed data delivery.
- Interface between eNBs (X2): is used to interconnect eNBs inside E-UTRAN. Like S1 interface, this interface is also divided into C-plane and U-plane sub-interfaces, which are respectively referred as the Control plane interface between eNBs (X2-C), and the User plane interface between eNBs (X2-U). Based on the X2 Application protocol (X2AP) and the SCTP, the X2-C is in charge of the mobility functions (intra-LTE mobility and handovers), Multi-cell SGSN function, and the management and error handling function of X2 interface. The X2-U supports the tunneling of end user packets between the eNBs through the GTP-U and takes in charge the indication of the SAE Access Bearer in the target node to which the packet belongs to as well as mechanisms to minimize packet losses related to mobility. The X2-U interface is also used during the inter-eNBs handover for temporary user downlink data forwarding.
- Uu interface: represents the Air interface between the mobile and the eNB, which comprises the Physical layer and the Data Link layer. In particular, the Data link layer is composed of the MAC protocol, RLC protocol, and the PDCP [46]. The Uu interface carries the signaling messages destined to eNB, NAS messages for the MME, and the transfer of user traffic to S-GW. In the C-plane, the Uu interface carries the RRC signaling which in turn carry MME NAS messages used for registration, bearer setup and mobility management. RRC is responsible for the establishment of security related functions over the air, configuring PDCP profile for each type of bearer, determining the RLC mode for the packets, priority establishment of each channel, and setting Hybrid Automatic Repeat Request (HARQ) parameters for the physical layer [47].
- S10 interface: is used for the interconnection between MME.
- S11 interface: is used as an interconnection between MME and S-GW, and contains additional functions for paging and mobility.
- S3 interface: allows information exchange related to the user and its corresponding bearer for inter 3GPP access network mobility between MME and SGSN. In the interoperation scenario in which a UE moves from 4G LTE to 3G coverage, the context information request from SGSN to MME is carried over the S3 interface.
- S4 interface: interconnects SGSN and S-GW. Since LTE APNs are configured in the P-GW, SGSN gets the information about the APN from P-GW using this interface. As a result, for example during a UE handover from LTE to 3G network, SGSN requests S-GW to establish a session over S4 interface.

- S5/S8 interface: consists of two interfaces interconnecting S-GW and P-GW. These interfaces are used when a connection to non-collocated P-GW for the IP network connectivity is required by S-GW. The difference between S5 and S8 interfaces resides in the fact that the S5 interface is used when the UE is not roaming, whereas the S8 interface is used when the UE is roaming between different mobile networks.
- S6a interface: interconnects MME to HSS. It is used for authentication and authorization. Location information, subscriber information, and authentication data that are required for authenticating and granting user access to the network are carried over this interface.

B. SECURITY ARCHITECTURE

As specified by 3GPP in [48], the LTE security architecture specifications aim at enhancing the security requirements of the 3G mobile networks [49]. The 3G security architecture defines five security features in order to meet security objectives [48]:

- The Network Access Security: provides users with security features for a secure access to services, and prevents against attacks on the (radio) access link. These security features include the user identity confidentiality, the authentication of user and network entity, the confidentiality of user and signaling data based on ciphering algorithm, the data integrity, and the mobile equipment identification.
- The Network domain security: provides security features to enable a secure signaling data exchange between nodes, and protects against attacks on the fixed wired network,
- The User Domain Security: provides a secure access to MS,
- The Application Domain Security: comprises the set of security features that enable application in the user and in the provider domain for a secure message exchange between entities,
- The Visibility and Configurability of Security: comprises the set of security features providing the user with the ability to inform himself whether a security feature is in operation or not, and whether the use and provision of services should depend on the security feature.

The goals of security features presented above can be summarized as follows:

- Ensure user-to-network security: by providing user identity and device confidentiality, as well as entity authentication, which can be achieved using temporary identification and ciphering. As an authentication protocol, the EPS AKA procedure is used in LTE networks for mutual authentication between users and networks [11], [29], [33], [36], [50], [51].
- Ensure user data and signaling data confidentiality: by providing encryption algorithm, and ciphering to RRC-signaling in order to prevent UE tracking,
- Ensure user data and signaling data integrity: by providing integrity protection of the origin authentication of signaling data, and the authentication of the network by the UE.

Compared to 3G, the key separation of the AS and NAS in LTE security architecture is achieved through a hierarchical key architecture. The use of compulsory key-based data encryption, signaling encryption and integrity protection in LTE is a major enhancement to the security of the 4G mobile network system. However, some vulnerabilities related to the LTE security features and mechanisms such as the security of handover procedures, the security in IMS, the security at eNB, and the security in Mobile Trust Computed (MTC), etc. still exist [14], [37], [45], [50], [52].

III. OVERVIEW OF ATTACKS IN MOBILE NETWORKS

In this section, we focus on providing an overview of attacks in mobile networks, including a categorization and classification of different attacks.

A. VULNERABILITIES, THREATS, AND ATTACK ENTRY POINTS

Due to the introduction of new radio access technologies and the migration towards IP-based architecture, new vulnerabilities have been brought into the network architecture, which exposes mobile networks to different threats targeting protocol stacks, security features, and network interfaces [24]. A vulnerability in mobile network can be understood as a weakness inherent to network architecture and components, which can be exploited by a threat to perform an attack. Therefore, a threat is determined by the ability to intentionally attempt to 1) unauthorized access to information, 2) manipulate information and 3) render a system unreliable or unusable.

According to [53], the transition to the flat IP-based architecture has introduced a shift in mobile wireless threat entry points. In fact, 2G and 3G mobile core networks were hardly targeted by threats due to the use of SS7, which was hardly penetrable compared to diameter signaling used in all IP and beyond 4G mobile technologies, where devices and core networks appear to be more vulnerable to various attacks. This can be explained by the evolution in mobile devices, which are turning to more powerful data-centric directly visible from the internet, and the replacement of SS7 signaling protocol by diameter protocol, as well as the use of various and flexible access technologies in the Radio Access Network (RAN) such as Femto cells, and Ethernet 802.11 wireless technologies (WiFi) hotspots. Although diameter is an important protocol for signaling of billing data, traffic and subscriber management, subscriber authentication, roaming, and mobility management in LTE, it is vulnerable to signaling attacks.

There are various entry points in 4G mobile networks such as compromised smart mobile devices, the access network, the backhaul and core network, and other external or 3rd party networks.

1) COMPROMISED MOBILE DEVICES

Compromised mobile devices can be used to launch attacks on mobile networks. In fact, mobile devices are crucial elements in mobile networks security, since they can constitute targets and also be used as enabler for launching attacks towards the mobile networks. In [53], authors particularly point out the possibility to spread malwares in mobile devices and compromise them through application download, which tends to be the most commonly used method for such purpose [54]. Attack vectors for mobile malwares can range from Mobile network services, internet access, to Bluetooth. These vectors can be used to launch attacks on mobile devices in order to collect private data, utilize computing resources, or perform harmful actions. Various types of malware attacks can be performed on mobile devices such as mobile botnets, which is considered as the next major large scale threat targeting mobile network due to the integration of internet with mobile networks [55]. In fact, a botnet is a set of compromised devices which can be controlled and coordinated remotely. Using mobile malware like Trojan horse, a mobile device can be turn into a botclient, thus enabling it to receive commands from a remote command and control server. In fact, in [4], authors have also demonstrated the possibility to launch Distributed Denial of Service (DDoS) attacks on mobile networks by using malwares residing on different user equipment at WLAN. Such attacks can be effective by using mobile botnets to launch signaling DDoS attacks, and target a specific Home Location Register (HLR) with a large volume of traffic, thus preventing legitimate users of cellular networks from accessing and using the service, [2], [26], [43], [56]–[61].

Other spreading techniques used to compromise a mobile device include granting of permissions from malicious applications. In addition to malwares, mobile devices can also be targeted by a large broad of threats including threats from the internet, phishing and MITM [62].

2) THE ACCESS NETWORK

In the access network, the S1 interface constitutes the main entry point as it is used to connect and authenticate eNBs to the mobile network. Typical vulnerabilities affecting this interface relate to the possibility to use an eNB cell station to access and attack the MME (and consequently take down the entire core service), as well as the possibility to inject false traffic into applications [62]. Other vulnerabilities in the access domain security, which can be exploited to threaten the operation of mobile networks are discussed in [63]–[65] in relation with the lack of data and signaling encryption.

In fact, during the initial authentication procedure, messages exchanged before the security mode command setup are not encrypted nor integrity protected. These messages transfer data such as Authentication Token Number (AUTN), Random Number (RAND), Signed Response (RES) and International Mobile Subscriber Identity (IMSI) used to authenticate a UE. Typically, an attacker can exploit the lack of protection of the RRC connection reject message to launch a DoS attack in mobile networks. In addition, the lack of authentication between the Serving Network (SN) and the Home Network (HN), as well as the lack of cryptosystem in the wireless network and protection of Location Area Identity (LAI) in UMTS-AKA also constitute vulnerabilities that may be exploited to launch attacks in mobile networks. In particular, redirection attacks can lead to the alteration of the LAI. For example, the lack of integrity protection of some UMTS signaling messages that are exchanged between the MS and the RNC can expose the network to a modification of RRC messages as they are unprotected [66].

Another vulnerability in the access network is related to the authentication protocol during seamless interoperation between different access technologies such as GSM, UMTS and LTE as reported and examined in [5], [65] and [67]–[69].

In fact, the GSM AKA protocol suffers a weakness related to the inter-operation of the 2G/3G access network, which can be explained by several reasons. First, the lack of mutual authentication between the subscribers and the network is a major threat as it can cause the user identity to be revealed through an IMSI catcher. This vulnerability can be exploited to launch active attacks against a GSM-compatible network by the means of Software Defined Radio (SDR) for example [70]. Second, the lack of integrity protection of signaling data can be used to force the mobile or network to engage in a plain data (voice or text) transmission after removing or modifying the security options. Finally, the storage of authentication triplets in the Visitor Location Register (VLR) can lead to the exposure of the symmetric key of a targeted mobile station. Thus, some security issues may occur during the integration of the GSM device into the UMTS network involving the following scenarios. For example, during the roaming of the GSM device in the UMTS network, an attacker can eavesdrop the communication provided that it has already got access to the Ciphering key (Kc) while the device was in a fully GSM network. Moreover, it is possible for a Mobile Switching Center (MSC) to use a compromised ciphering key (Kc) to authenticate between the mobile and the GSM base station during roaming of a UMTS device in a GSM Base Station Subsystem (BSS). A variant of this scenario involves the encryption of the communication with GSM ciphering key (Kc) during the roaming of a UMTS mobile device in a GSM mobile network (BSS and MSC). In addition, the lack of payloads encryption between the MS and the SGSN during connection to a GSM BSS, can lead to eavesdrop the communication [65].

Finally, other weaknesses in the access network are related to the signaling overload, the limited wireless link bandwidth, the high signaling overhead, and the heavy control processing of signaling messages in the RRC procedure for the Radio Access Bearer (RAB) establishment/release, which can be used to launch attacks in the CN, such as the HLR flooding attack [15], [26], [66], [71]–[73].

3) THE BACKHAUL AND CORE NETWORK

Like the access network, there are also some vulnerabilities that have been reported in the 4G backhaul and CN [37], [74]. The backhaul network consists of the physical connections and networks used to carry data between the RAN and the CN, whereas the CN is comprised of network logic that handles the creation and maintenance of connections between mobile devices and external service networks, and handles transferring of user and control data, as well as authentication of users and devices. Despite the fact that getting access to the CN can be particularly challenging, some security vulnerabilities still exist. According to the authors in [74], the backhaul can provide an attacker with access to all the control and data traffic sent between mobile devices inside a radio coverage area. Since the technological evolution has enabled the integration of different access technologies such as femtocells, and non-3GPP WiFi(s) owned by the MNOs, new potential entry points have been brought in the CN for attackers. Particularly, in the case of LTE, new threat entry points result from the introduction of new interfaces such as the X2 interface, the use of diameter signaling protocols whose traffic increases signaling overload, and the transition to IP [54]. In fact, there are several severe threat factors against the EPC CN including the flat IP-based architecture, and the existing Base Station (BS) with direct connection to the ALL-IP network. In addition, the lack of privacy protection in the EPS-AKA scheme in the access procedure, and the lack of prevention to DoS attacks are other severe threats targeting EPC CN. The lack of backward security in the handover procedure, the lack of protection against desynchronization and replay attacks, as well as the vulnerability in the MTC security architecture and Security Mechanism in IMS and Home Evolved Node B (HeNB) constitute also, moreover, major security threats against the backhaul network [37].

Another weakness that is related to the lack of security schemes in the GTP protocol used in in the EPC NAS, can expose the network to threats like abnormal packet threats consisting of modified or damaged Packet Data Unit (PDU) packet, or PDUs not complying with the protocol, traffic analysis, and traffic modification [75].

Finally, one of the emerging threats in the CN is related to the virtualization and software-defined network, which is reshaping the network architecture resulting in new vulnerabilities entry points as both the user and control-plane traffic become more distributed across network elements and have to cross non-trusted networks [53].

4) THE EXTERNAL OR 3RD PARTY NETWORK

The last entry point for threats targeting mobile networks is formed by the external or 3rd party network. In fact, as reported in [74], different user services are provided through external and third party networks, including internet browsing services, interconnection to corporate networks, roaming partners networks, other connected Public Land Mobile Network (PLMN)s, shared RAN, external transport networks, and non-3GPP access networks.

In the particular case of non-3GPP access networks, the inter-working with WLAN, which can be used for example when accessing 3G HN over WLAN architecture, or during 3G roaming over WLAN architecture, presents several security issues such as disclosure of user's confidential information (this relates to credential during authentication over WLAN), user permanent identity tracking that may occur when accessing 3G services, network impersonation in order to get user personal information, and legitimate user impersonation allowing to get free services access to perform deceitful activities that will be charged to the user [4], [6], [76]. Another weakness is related to the possibility of by-pass access control and authentication process in addition to getting services at free cost, the possibility of interference with the charging process in order to get uncharged services, and the possibility to prevent user from accessing 3G services by the mean of rogue services like propaganda.

In addition to the weaknesses mentioned above, the use of different technologies in converged networks such as WiMAX also constitutes another threat entry point, since WiMAX still presents weak spots in the physical layer and the MAC layer (confidentiality and authentication) in relation with spoofing, MITM and eavesdropping attacks [60].

B. CATEGORIZATION OF ATTACKS IN MOBILE NETWORKS

In this section, we provide a categorization of different attacks in mobile networks. In fact, several papers have proposed different attacks categories depending on criteria such as the difficulty of the attack implementation, the necessity to require the network access, the potential impact of the attack, the origination of the attack, the target of the threat, and the likelihood and risk of the attack [20], [23], [40], [43], [54], [77]–[79]. In [80], four groups of attacks are presented depending on attack origination.

In [81], authors particularly examined attacks against Cooperative Intrusion Detection System (CIDS). In the case of external attacks, they can be classified into disclosure attacks and evasion attacks, since their goal is to detect presence of CIDS in order to evade and decrease the detection accuracy.

The Table 1 provides a summary of threats categories, attacks groups, origin, mode, and target. It can be observed that each attack can be launched inside the network domain (internal attacks) or from the outside (external), using a passive or active adversarial mode. Passive attack aims at gathering data exchanged in the network without disrupting the operation of the communications, whereas an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of the mobile network [20] and [82].

The first group, which consists of threats from internet, PDN, GPRS roaming exchange or other PLMN, can be classified as *External attacks via network*. The second group is called *External with physical access to network entities* and comprises attacks on radio interface, tampering attacks,

TABLE 1. Summary of threats and attacks categorization in mobile networks.

Threat Groups	Attack Categories	Attack Origin	Attack Mode
Interface Flooding	Loss of availability	External / Internal	Active
Network element crashing	Loss of availability	External / Internal	Active
Traffic eavesdropping	Loss of confidentiality	External / Internal	Passive
Unauthorized data access	Loss of confidentiality	External / Internal	Active
Traffic modification	Loss of integrity	External / Internal	Active
Data modification	Loss of integrity	External / Internal	Active
Compromised network element	Loss of control	External / Internal	Active
Malicious insider	Loss of control	Internal	Active
Theft of service	Theft of service	External / Internal	Active

and unauthorized access to networks ports. The third group includes the *Mobile device based attacks* and comprises attacks against other mobile devices and mobile networks. Finally, the last group of attacks can be called as *Insider attacks*, which is usually be performed by malicious MNO staff abusing of administrator rights.

These four groups of attacks can result from five categories of threats exploiting mobile network vulnerabilities. The first category of threat is the *Loss Of Availability*, which can lead to *Availability Attacks* aimed at causing a loss of network availability or DoS. Typical attacks consist in flooding an interface, crashing a network element via a protocol or application implementation flaw, destruction of information and/or network resources, etc. In the physical layer, this can be achieved by jamming the radio channel. It is also possible that many attackers may be coordinated to launch large scale attacks which can lead to a DDoS. The second group relates to the *Loss Of Confidentiality*, which aims at gaining access to user confidential data and can be performed by analyzing encrypted traffic, eavesdropping, and unauthorized access to sensitive data on a network element via information leakage.

Another category is the *Loss Of Integrity* that can be achieved through traffic and data modifications on network elements by carrying out MITM attacks. In fact, MITM refers to the capability of an intruder to put himself between the target user and a genuine network and thus being able to eavesdrop, modify, delete, re-order, replay, and spoof user data and signaling. It can be used to gather information, gain access to private network resources by hijacking ongoing sessions, derive information about a network and its users through traffic analysis, corruption of transmitted data, and injection of new information into network sessions. The Loss of integrity can also be achieved through compromised authentication vectors in the network, consisting of an intruder getting access to authentication vectors after compromising network nodes or by intercepting signaling messages on network links. These compromised authentication vectors may include challenge/response pairs, cipher keys and integrity keys.

The *Loss Of Control* refers to the threat category aimed at gaining control of a network element by compromising it via protocol or application implementation flaw, management interface, and malicious insider.

Finally, the fifth category is related to the *Theft Of Service*, which can be achieved using flaw in authentication and authorization mechanism.

These groups of attacks can target the AS and NAS of the E-UTRAN and the EPC. In the AS, different features and procedures can be targeted based on the protocol layer (Physical, MAC/RLC, and RRC layers). For example, in the RRC layer, procedures such as paging, connection Setup/Release, handover and security key management, UE measurements related to inter-system (inter-RAT) mobility, and QoS constitute the main targets.

Compared to the AS which is IP-based, threats in the NAS target both the PS domain and the Circuit Switched (CS) domain. For example, in the CS domain, threats can be focused on the Connection Management (CM), and Mobility Management (MM), contrarily to the PS domain, where threats may target the Session Management (SM) and GPRS Mobility Management (GMM) features.

Depending on the threats target and objective, main threats categories in mobile networks environment related to the five groups of attacks presented above can be summarized as follows [23] and [80]:

- Interface Flooding: can target different interfaces in the mobile network including radio interfaces and backhaul interfaces.
- Crashing a network element: exploits protocol or application flaws in order to disrupt the function of the targeted network component.
- Traffic eavesdropping: can target different interfaces including radio interface, backhaul, control plane, and user plane. It consists in listening into a communication, spying, or snooping the network in order to gather, or steal information. An intruder can identify sensitive personal information, and steal data during transmission over the internal or external network, or from networked devices by gaining unauthorized access. The information gathered through eavesdropping can be used to perform other attacks targeting mobile networks. Eavesdropping also refers to the ability of an intruder to eavesdrop signaling and data connections associated with other users by modification of the required equipment such as an MS.
- Unauthorized data access: targets sensitive data on a

network element and can be achieved via data leakage.
- Traffic modification: targets different types of data traffic in the radio interface, backhaul, C-plane, and U-plane.
- Data modification on a network element: can be performed by exploiting protocol or application implementation flaw.
- Compromising a network element: can be achieved either via a protocol or application implementation flaw, or via management interface. Using a compromised network element such as a MS, an intruder can perform *User impersonation* by sending signaling and user data to the network, in an attempt to make the network believe that they originate from the target user. Similarly, using a modified BS, an intruder can perform *Network impersonation* by sending signaling and/or user data to the target user, in an attempt to make the target user believe that they originate from a genuine network.
- Malicious insider: consists of a user unintentionally using a malicious application, or an administrator with authorized access to the network.
- Theft of service: involves a stealthy use of service without being charged. It can be achieved by exploiting a flaw in the authentication and authorization mechanisms or within the charging procedures to use services without being charged.

IV. THREATS AND ATTACKS IN 4G NETWORKS

In this section, we explore security and confidentiality attacks, IP-based attacks, signaling attacks, and jamming attacks. We also draw a categorization of the different attacks based on the network components. According to [83] and [84], attacks in 4G mobile network can result from failure of security requirements, which are focused on:
- The Application Security: is related to the integrity of the hardware, software, data and operating System (OS).
- The Network Access Security: is related to the Confidentiality, Integrity, Authentication and Authorization (CIAA) of data.
- The User Security: is related to the user's identity, confidentiality and authorization.
- The Network Area Security: is related to the MEs location authentication and confidentiality.
- The QoS maintenance: is related to the security against denial of service (DoS) attacks.
- The Physical Layer Security: is related to the resistance against tampering.

Failure of security requirements can be exploited by an attacker in order to perform various types of attacks such as confidentiality, integrity, and availability attacks, which may result into DoS or DDoS [78].

A. ATTACKS AGAINST SECURITY AND CONFIDENTIALITY

Attacks against security and confidentiality are presented in Table 2. These attacks are related to threats targeting the user and device identity confidentiality, mutual authentication and Key agreement (AKA protocols) [8], [10], [85].

Although EPS-AKA is used for authentication between a UE and 4G EPC CN, it still presents security issues such as the non-protection of authentication vectors between HSS and ME, the disclosure of user identity due to the lack of IMSI protection during ME registration (it may be possible to intercept IMSI), and the lack of protection of the SNID [11], [29], [31], [86]. In fact, the authentication procedure is triggered during mobility management procedures such as handover, paging, and location update, which are handled by MME [34].

In [87], performance of paging channel in presence of network overloads or attacks from internet has been investigated. Authors particularly pointed out the vulnerability in paging procedures.

Authentication procedures occur at every Tracking Area Update (TAU), mobile registration, call originating, call terminating, and handovers. However, in the case of handover key management, some vulnerabilities have been identified, which can lead to possible unsecured communication between user and network by carrying out rogue base station attacks [13]. In fact, rogue base station attack allows a mobile device to duplicate the functionality of a base station by exploiting network protocol vulnerabilities such as in IP stack. In practical terms, rogue base station can be used to perform *user identity forgery attack*, *eavesdropping attack*, *packet injection attack*, *packet modification attack*, and *desynchronization attack*. The *desynchronization attack* can particularly cause failure of handover key management, thus preventing a target eNB from maintaining the freshness of the handover keys [88]. In fact, there are two types of handovers in the EPS: the intra-MME and the inter-MME handovers. In the intra-MME handover, the preparation of the handover occurs between the source and target eNB in the same MME through X2 interface. In the case of inter-MME handover, the preparation entirely takes place in the MME without any direct signaling between base stations.

Since the main purpose of handover key management is to ensure separation of the session keys in a handover between base stations in such a way that a compromised session key is confined in one base station, consequently failure in handover key management can make it possible to decipher messages between eNB and UE, as well as RRC signaling and U-plane information.

Various attacks that can be performed using a rogue base station include redirection attacks, MITM attacks against subscriber location, false base station attacks by eavesdropping of SNID, and compromised Authentication Vectors (AV)s attacks. To mitigate these attacks, authors in [13] proposed an algorithm for the selection of an optimal root key update interval in order to mitigate the effect of desynchronization and key compromise attacks.

In addition, as mentioned above, the user identity privacy can be compromised in EPS-AKA during LTE initial attach procedure [89], as the IMSI is transmitted in plain-text. Moreover, other weaknesses in EPS-AKA can be used to per-

TABLE 2. Attacks against security and confidentiality.

Attack reference map in 4G mobile networks		
Attacks Targets	**Attacks Type**	**Proposed Solution**
LTE security	User identity and privacy threats: • Control plane data modification • Unauthorized access to the network, eNB attacks, UE USIM tracking	No solution proposed [1]
LTE security	Analyzed various attacks: • Attacks against Confidentiality • Attacks against Integrity • Attacks against Availability	No mitigation solution proposed [2]
DoS	WLAN-LTE integration attacks: • Internal attacks • External attacks without cooperation • External attacks with cooperative malicious device or relay	Stateful analysis monitoring system [3]
DoS	Redirection attacks/False base station attacks: • Unprotected Authentication vector in EPS-AKA • Subscriber malicious activities	Improved EPS-AKA combining vector and key KASME not accessible by an intruder carrying an attack in the network domain between MME and HSS [4]
DoS	MITM attacks against subscriber location: • Unprotected authentication vectors between HSS and ME • Unprotected SNID (eavesdropping of SNID) • SNID eavesdropping and False base station attack	Proposed: • SE-EPS-AKA • Digital certificate • Public key acquisition by HSS/ MME and UE [5]
DoS	Handover key management vulnerabilities: • Rogue base station attack • Identity forgery • Eavesdropping • Desynchronization attack • Packet injection and modification	An optimal Key Update Interval selection algorithm [6]
False Base station	Attack against IMSI in LTE: • At initial attach procedure • Inter-MME handoffs • Fake base station requesting UE IMSI	Enhancement to EPS-AKA based on a DMSI: • Transmission of DMSI by UE instead of IMSI • Update of DMSI using a random number received after each successful EPS-AKA procedure • IMSI access is restricted to UE and HSS [7]

form active attacks including the impossibility of retrieving IMSI from Globally Unique Temporary Identifier (GUTI), handoffs between MME, as well as the computational overhead and authentication delay are [33] and [50]. In fact, the purpose of GUTI is to identify the UE globally without revealing its identity when visiting a new MME or when a fake eNB requests IMSI from a UE.

To overcome vulnerabilities in EPS-AKA, authors in [90] proposed a secure efficient AKA protocol. Another scheme capable of improving performance of EPS-AKA has been proposed in [29]. This solution is a two steps enhanced EPS-AKA protocol scheme, which increases the computational overhead in the SN and can reduce: 1) the transaction messages load, 2) the bandwidth consumption, 3) the number of computed hash functions, which consist of a set of algorithms f1, f2, f3, f3, f5 and Key derivation functions (KDF) between entities in comparison with the original EPS-AKA framework. Algorithms f1 and f2 are known as *message authentication functions*, whereas f3, f4 and f5 are so called *key generating functions*. A key point in this solution is that it can improve the authentication performance and security by combining vector and key KASME, which cannot be accessed by an intruder carrying an attack to the network domain between MME and HSS, and prevents against active attacks.

Compared to [29], the solution proposed in [11] is a security enhanced authentication and key agreement (SE-EPS-AKA) based on Wireless Public Key Infrastructure (WPKI) using the ECC (Ellipse Curve Cipher) encryption, which provides protection of the user identity security and limited energy consumption during the exchanged information, and introduces the use of a digital certificate and public key to be acquired by HSS, MME and UE. The new scheme provides protection against MITM and Sequence Number (SQN) DoS attack, mutual authentication between UE, MME and HSS, protection of the transmission of private and confidential information among entities, as well as resolution of safety problems incurred by leakage of IMSI and SNID, and an increase of the safety strength of session cypher key.

Similarly, [50] proposed an enhanced EPS-AKA scheme in order to overcome vulnerabilities related to the user identity privacy by introducing a DMSI transmitted by UE instead of IMSI. The DMSI is updated based on a random number received at each successful EPS-AKA procedure and can achieve user identity privacy by restricting the knowledge of the IMSI at the UE and the HSS.

Furthermore, heterogeneity of access technologies is a major advance in LTE. Nevertheless, it poses new potential threats that need to be addressed, since fast and secure handoff is a key requirement for integration of heterogeneous networking technologies.

Few surveys have investigated issues related to mobility management in LTE networks. In [91], authors provide a comprehensive review of the LTE interworking architecture: Inter-Radio Access Technology (RAT) mobility is performed by S-GW providing mobility for inter eNB handovers, and inter-technology mobility, which is supported at higher layers based on the IP protocol, with the P-GW providing the WLAN 3GPP IP Access.

In [92], authors also examined handover procedures in LTE and pointed out the complexity in achieving seamless handovers, as well as the lack of a uniform procedure structure, the lack of backward security related to complex key management mechanism. To overcome these issues, they proposed a fast and secure handover authentication scheme in order to comply with different mobility scenarios in the LTE networks.

In [93], authors analyzed mobility management issues in mobile networks such as packet loss and high handoff latency, and proposed an enhanced fast handover with seamless mobility supports. This solutions aims at reducing the mobility signaling overhead, handover delay and packet loss when mobile users change their network attachment point.

In fact, the SAE /LTE architecture uses Extensible Authentication Protocol (EAP)-AKA authentication method to provide secure 3G-WLAN handover and authenticate UE attached to a WLAN in 3G-WLAN architecture. Despite the fact that the UE must be authenticated by HSS, HLR and Home Authentication Authorization and Accounting (HAAA), several threats against EAP-AKA have been examined in [36], including:

- threats against user identity and privacy,
- threats of UE/USIM tracking,
- threats related to base stations and handovers,
- threats related to broadcast or multicast signaling,
- threats related to DoS,
- threats against manipulation of control plane data,
- threats of unauthorized access to the network,
- compromise of eNB credentials as well as physical attacks on an eNB,
- protocol attacks on an eNB,
- attacks on the core network, including eNB location-based attacks,

In particular, theses threats can lead to the disclosure of identity that is sent in plain-text, DoS related to the lack of encryption of authentication messages (messages such as EAPoL-Start, EAP-success and EAP-failure), which can result in spoofing attack and UE localization discovery and tracking, MITM attack, SQN attack, and additional bandwidth consumption exposing legitimate user to risk and increasing the authentication delay [6], [30], [94]. In [32], authors have particularly analyzed issues of LTE-AKA internetworking with WiFi. They have also reviewed major privacy threats against users connecting to wireless Local Area Network (LAN) in relation with disclosure of user identity that is sent in a clear text allowing user identity attack. As a countermeasure, the solution proposed is a new LTE-AKA scheme that does not allow clear transmission of IMSI, and uses the WiFi APs connected to the internet in order to establish a secure side channel. The WiFi channel acts as a secure tunnel through which a new Random Identity (RID) will be exchanged. RID will be used at the HSS to identify the user and will be associated with an IMSI and a secret key K that resides only in the USIM and the HSS.

In addition, inter-operations between LTE, UMTS, and GSM also present several weaknesses related to their respective AKA schemes, which can be used to perform different types of attacks [51], [76]. Firstly, the weakness in GSM ciphering and the lack of integrity protection on the user plane traffic in 4G can be exploited to perform eavesdropping and network impersonation attacks on UMTS. Moreover, the lack of network authentication in GSM can also be exploited to carry out false base station attacks against 4G ME during the AKA procedure. This typically involves 4G SN, 4G MME and 3G HN. The fact that 3G HN can only generate 2G and 3G authentication vectors makes this attack possible, since 4G authentication vectors are not generated by 3G HN.

Similarly, when 4G AKA is executed by mixed SN (2G BS and a 4G MME), 4G MS, and a 4G HN, an attacker may also perform false base station attack. In addition, the inter-operation between GSM and UMTS is also vulnerable to MITM attacks. These vulnerabilities can also lead to attack against the Cipher Mode Command (CMC) message between the 2G BS and the MS, because of the lack of integrity protection of the CMC message.

Like the inter-operations between 4G and its predecessors (3G and 2G), DoS can also result from the integration of WLAN and 4G/LTE networks, since it brings new threats and vulnerabilities. As a countermeasure, in [23], authors have proposed to store behavioral information of Access Points issued from the authentication answers, handover, and disconnection protocols to develop efficient countermeasures such as *stateful analysis monitoring systems*, capable to detect corrupted access point (PoA) and any change in the network. This can help to protect against internal attacks like the decrypted message leakage that can lead to session eavesdropping, information disclosure, data corruption, removal threats, and cryptographic attacks, external attacks, and external attacks with cooperation.

Another weakness in 4G mobile networks is related to the wireless converged networks, particularly in WiMAX,

which is vulnerable to threats on the physical layer and Mac layer [24], [60]. Typical threats facing WiMAX are DoS attacks due to unprotected network entry, unencrypted management communication, unprotected management frames, and weak key sharing mechanism in multicast and broadcast operations. As possible countermeasures, authors in [60] suggested :

- use of authentication and digital signature to mitigate spoofing and MITM,
- use of encryption against eavesdropping
- use of spread spectrum and strong scheme techniques o protect against Physical layer attacks

In addition, in [24] authors rather proposed to extend the authentication mechanism to all management frames, as well as RRC ciphering and user plane protection in order to alleviate threats related to unprotected UE ID in LTE. Their solution is based on the authentication and the digital signature against spoofing and MITM, and it uses encryption to combat eavesdropping, spread spectrum and strong scheme techniques for protecting against physical layer attacks.

Finally, the lack of user data confidentiality is a major threat to physical layer and traffic analysis attacks [95]. In order to mitigate this threat, the authors proposed to generalize the phase encryption to any communication system independent of the underlying modulation scheme. This solution can resist the traffic analysis attack, which cannot be prevented by any security primitives in the upper layers.

In order to address vulnerabilities and attacks described above, authors in [37] suggested some enhancements to the security architecture as well as more research on opened issues such as:

- LTE system architecture: more security mechanisms need to be designed in order to protect the communications from traditional protocol attacks and physical intrusions in the LTE networks,
- LTE cellular security: enhancement in EPS AKA scheme is needed, as well as a design of secure access authentication mechanisms to be used during UE access to the EPC via non-3GPP networks, in order to protect against the disclosure of user identity, DoS attacks and other malicious attacks,
- LTE handover security: further enhancement is needed in the key management mechanisms and handover authentication procedures to prevent protocol attacks, desynchronization attacks and reply attacks,
- IMS security: design of fast and robust IMS access authentication mechanisms is required to simplify the authentication process and also prevent DoS attacks and other malicious attacks in the LTE networks,
- HeNB security: design of simple and robust mutual authentication mechanisms between the UEs and the HeNBs is required to prevent various protocol attacks,
- MTC security: design of the MTC security mechanisms in the LTE/Long Term Evolution-Advanced (LTE-A) is an emerging research work.

In [96], authors also investigated users privacy and anonymity in hybrid mobile network formed by distributed and mobile infrastructure integrating wireless, cellular, and wired connections, and proposed a protocol that relies on the capability of mobile devices to create a local WiFi network, based on a new fast packet filtering that leverages pseudo random number generation to guarantee communication integrity. This protocol provides protection of the system against possible abuses of anonymity by maintaining the ability to block malicious traffic, as well as its protection of the privacy of the requester from all parties involved in a communication.

B. IP-BASED ATTACKS

In this section, we present IP-based attacks in 4G mobile networks. As recent developments in mobile network technologies have favored the transition to IP-based technology in the transport network, new threats have been brought to the network [52], which are presented in Table 3. We will discuss IP-based attacks against the backhaul, GTP and diameter protocols.

1) IP-BASED ATTACKS AGAINST THE BACKHAUL

The backhaul is composed of IP-based control elements and interfaces, making it vulnerable to IP-based attacks. This vulnerability can be explained by the lack of mutual authentication of eNBs, the lack of prevention against IP-based attacks, and the lack of encryption of data and signaling traffic over non-trusted networks [12]. According to the authors, S1-U, S1-C, X2-U and X2-C are LTE backhaul interfaces where the transported traffic need to be secured. Potential attacks over these interfaces may be performed as spoofing attack at eNB, eavesdropping of user traffic, unauthorized access attacks (eNB and other network equipment), flooding attack (TCP Synchronization (SYN)-flood packet consisting in sending TCP SYN after changing source IP address and Port number), and TCP reset attacks by sending fake TCP packets with reset bit set to 0.

IP spoofing attack is also referred to as masquerade attack, and consists in the manipulation of TCP/IP packets, and falsification of the source IP address, thereby making the attacker appearing to be another user. It is possible for the attacker to use an IP address within the range of IP addresses of the network or use an authorized external trusted IP address providing access to network resources. Typically, this attack can lead to overbilling and power consumption for certain UE (Battery depletion attack) and induce an abnormal traffic into components in the mobile network concurrently to cause overload in the network or consume the resources of the UE and mobile network such as GPRS Gateway Support Node (GGSN), and P-GW.

In order to mitigate and reduce the number of threats based on the 3GPP standard, authors in [52] proposed a security solution which could be used at the deployment of the LTE network and provisioning of eNBs. This solution is based on two main components including security gateways, for the connections filtering, and traffic encryption based on IPsec,

TABLE 3. IP-based attacks.

Attack reference map in 4G mobile networks		
Attacks Targets	**Attacks Type**	**Proposed Solution**
	C-plane signaling storms: • NAS access procedure • Handover procedure • Desynchronization attacks • IMS, and HeNB security mechanisms	Proposed investigations to enhance: • Security mechanisms against protocol attacks and physical intrusions • EPS-AKA mechanisms against user identity privacy, desynchronization, and replay attacks • Fast and robust authentication mechanisms for IMS access, and betweenUEs and eNBs [37]
GTP attacks	Threats related to: • Packet tampering • Information leakage • Abnormal GTP messages	Proposed a detection system to: • Capture 4G network control and data traffic to generate useful information and abnormal pattern recognition • Detect 4G network attack traffic • Prevent 4G network intrusion (IPS) • Monitor and control 4G network security attacks [17]
VoLTE attacks	SIP security threats: • Network scanning • Resource exhaustion attacks • Messages forgery and tampering • SIP flooding	Proposed: • Session control management • Flow-based VoLTE detection system • Signature-Based VoLTE IPS. [97]
VoLTE attacks	Signaling bearer attacks: • VoLTE signaling bearer data injection attacks • VoLTE signaling bearer misuse attacks • VoLTE signaling bearer QoS abuse attacks	Proposed • Enforcement of strict routing regulation • Upgrading of 4G gateway with VoLTE bearers filters • Priority decrease deferral mechanism when requested resource exceeds quota [98]
VoLTE attacks	VoLTE vulnerabilities related to: • Call spoofing, Changing of SIP source port • The lack of Media proxy in mobile network • Sending data over a VoLTE bearer • The lack of SIP message authentication • The lack of session management in SIP servers	Proposed • DPI to be applied on P-GW • Strict session management • UE verification [99]
DoS	LTE transport vulnerabilities: • eNB spoofing • Eavesdropping of user traffic • Unauthorized access to network equipment	Proposed the use of security solutions including: • Security gateways • Certificate authority [52]
DoS	IP spoofing	Proposed implementation of IPS in the GTP [100]
DoS	Diameter interface congestion attacks	Proposed an ECN to mitigate Diameter congested interface [45]
DoS	Diameter DoS attacks: • Malformed message • Message flooding • Subscriber malicious activities	Proposed a solution based on: • Encryption of diameter signaling messages • Anomaly detection and signature-based detection using CUSUM [28]
DoS	LTE backhaul IP-based attacks : • TCP SYN/RESET packet flooding attack • TCP RESET attack	Proposed two VPN-based solutions: • L3 IPsec VPN using modified IKEv2 • L3 IPsec BEET VPN based on HIP [12]

and a Certificate authority to prevent from unauthorized access to data or network component and provide keys for traffic encryption. Authors also pointed out DPI as a future security improvement.

To mitigate security issues in the backhaul network of LTE, [12] proposed two solutions. First solution consists of a layer 3 IPsec tunnel mode VPN architecture, using a modified IKEv2 protocol to provide DoS attack protection. The

second solution is a layer 3 VPN architecture based on HIP protocol, and provides protection against spoofing attacks. It is used to create IPsec BEET (Bound End-to-End Tunnel) based-VPNs overlaid on top of the backhaul network. As a result, the proposed VPNs solution can provide protection of user authentication and authorization, payload encryption, and privacy protection against IP based attacks on LTE backhaul.

2) GTP-BASED ATTACKS

Another typical IP-based attack is the attack against GTP, whose impact in LTE networks has been demonstrated through simulation [25]. In fact, as shown in Fig. 4, GTP is a tunneling protocol used to transfer data in the 4G network, and assign IP or manage the network resources.

In addition, GTP is a User Datagram Protocol (UDP)-based non-connecting protocol, which exposes it to packet tempering attacks, as described and reported in [17] and [100]. As an illustration of GTP attacks, the following attacks listed below are most frequent:

a) GTP scanning attacks: consist in sending echo messages to scan network elements, and can cause information leakage on 4G mobile networks, as GTP echo/request can reveal identity of network components
b) Create Session Request attacks: consist in repetitive session creation request causing resource exhaustion due to an abnormal use of GTP create session request message to set resources during the initial attach of the MS. As IP addresses are allocated by P-GW in the create session response message, they can be exhausted if excessive create session requests are sent. A service interruption can result from a falsified normal user number sent in the create session requests.
c) Abnormal GTP packet attacks: can result in GTP fuzzing on 4G mobile network, and malfunction of GTP components after receiving abnormal GTP messages. These attacks can be performed from 3G network and Evolved Packet Data Gateway (ePDG) of WLAN.
d) Voice phishing attacks: may be performed by tampering of SIP protocol.
e) Infrastructure attacks: an insider can modify its own IP address and connect to the CN components like GGSN and target other mobile devices by encapsulating GTP attack packets [75].

To mitigate GTP attacks, [100] suggested different countermeasures against GTP-based attacks, which have shown that security solutions can be applied efficiently on the internet border of mobile cellular networks and user access devices, prior to arrival of any unwanted traffic at the core network so as to prevent IP spoofing attacks in mobile data networks. In comparison, [17] rather proposed a different mitigation solution against packet tampering and resource exhaustion attacks in relation with abnormal use of GTP create session request message for the resource setup during the initial attach of the MS. In fact, this solution consists of a detection system capable to capture 4G network control and data traffic on S11 and S1-U interfaces in order to generate useful information and identify abnormal patterns. Moreover, this solution also includes an attack detection engine (to detect 4G network attack traffic), an IPS (to prevent 4G network intrusion), and a monitoring and control system (to monitor and control 4G network security attacks from the detection system).

GTP Scan attack performed on internal GTP machine can be followed by IP spoofing attack. In that case, if an attack server abnormally alters the GTP protocol and sends it as attack traffic, unnecessary processes like exception handling of abnormal GTP packets and errors can cause each GTP machine to receive DoS attacks. Typically, an external attack server can send a large volume of attack traffic to the internal network machines, which in turn may find it burdensome to process the received attack traffic.

3) VoLTE SIP-BASED ATTACKS

SIP is a text-based protocol, which suffers several vulnerabilities.

In [97], authors analyze SIP security threats in VoLTE, which are categorized into threats against the network, and threats against the user. Typical threats include information exposure due to the scanning of VoLTE network, messages forgery, messages tampering, and SIP flooding. They can lead to resource exhaustion, VoLTE service degradation or interruption, VoLTE service overbilling, VoLTE phishing, and DoS. As a countermeasure, authors proposed session control management, Flow-based VoLTE detection system to protect against network scanning and resource exhaustion attacks, and signature-Based VoLTE IPS.

In [98], authors particularly pointed out VoLTE vulnerabilities related to the lack of access control at mobile software and hardware to prevent data injection on VoLTE signaling bearer, imprudent routing and forwarding in the mobile network side, which do not provide verification mechanism for the traffic carried over VoLTE signaling bearer, in addition to the insufficient data-plane access defense at mobile phone. By taking benefit of these vulnerabilities, it is possible to misuse the VoLTE signaling bearer, either by bypassing the billing mechanism in order to get data free of charge, or by exploiting VoLTE signaling bearer high priority so as to abuse high QoS of VoLTE signaling level. Such attacks can be performed by encapsulating data packet as an Internet Message Control Protocol (ICMP) packet leveraging ICMP tunneling to deliver data through the signaling bearer, since ICMP packets are forwarded by the 4G gateway to the internet or by another mobile phone. To mitigate above mentioned attacks, authors discussed and proposed several mitigations: 4G strict routing regulation enforcement to allow relay of traffic over VoLTE between phone and the signaling bearer server only, or media gateway in IMS; upgrading of 4G gateway by adding VoLTE bearers filters; charging of signals similar to data traffic; and deferral mechanism in order to decrease the

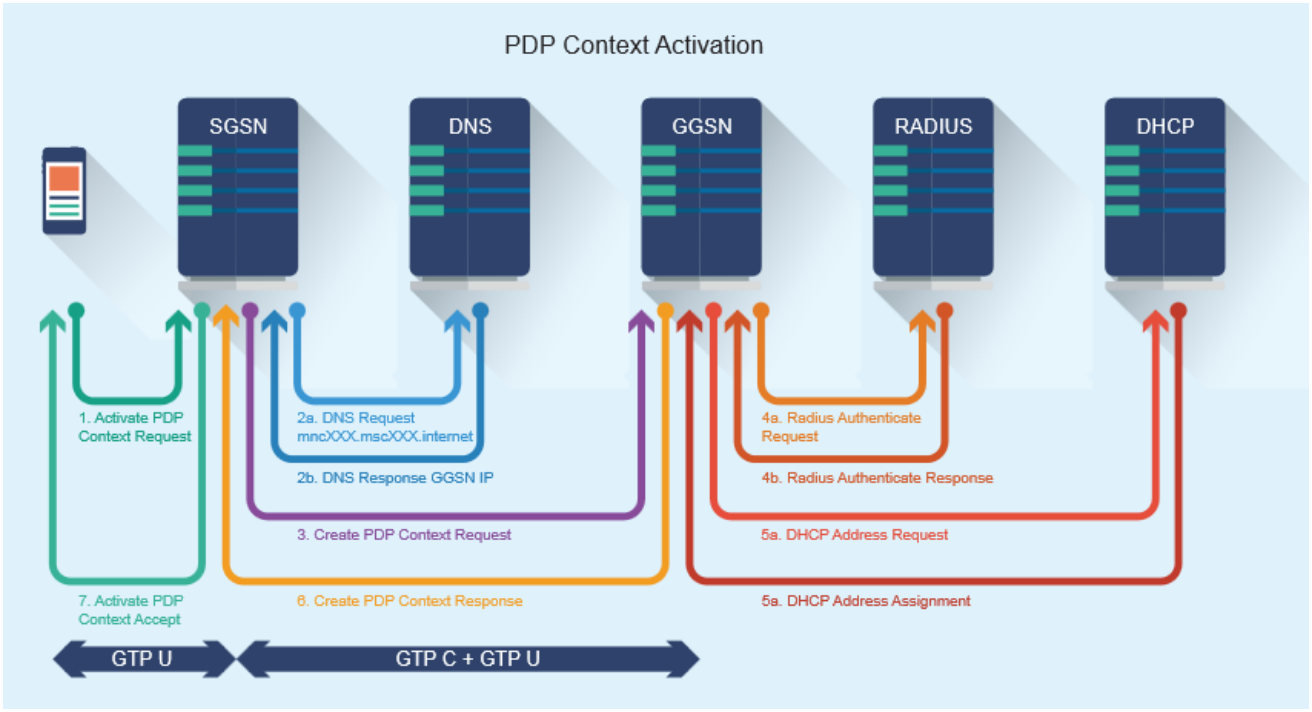

FIGURE 4. PDP context activation with GTP source [101].

priority at runtime whenever the requested resource exceeds the quota.

In [99], authors provided a comprehensive review of security mechanism related to the implementation of VoLTE in commercial mobile network. They have outlined several vulnerabilities such as: the possibility for a malicious software to change a SIP source port and thus launching VoLTE sessions on different source port, which are not rejected by SIP server; the lack of Media proxy in mobile network cannot prevent the UE to directly transfer media data; the possibility to send data through a VoLTE bearer, and manipulate QoS negotiation. Other vulnerabilities concern the UE permission model mismatch, direct SIP communication between UEs in relation with inappropriate access control of the default bearer for SIP signaling in P-GWs, the lack of SIP message authentication, and the lack of session management in SIP servers. This can be exploited to perform DoS attack on call by blocking a victim's mobile phone, and overbilling using a malicious software. As countermeasures, filtering of outgoing packet by P-GW except SIP messages is suggested, as well as strict session management, which can prevent from SIP tunneling, DoS, and cellular peer-to-peer. Other proposed solution include UE verification to protect against call spoofing, and DPI to be applied on P-GW in order to detect when the VoLTE bearer is being used. In addition to previous VoLTE attacks mention above, [102] analyze the impacts of silent call and ping-pong attacks. In fact, by exploiting VoLTE vulnerabilities related to abuse of signaling bearer for call establishment and Circuit-Switched FallBack (CSFB) requesting a user to downgrade to 3G networks without consent, these attacks can lead to an excessive power consumption and complete loss of LTE connectivity.

4) DIAMETER-BASED ATTACKS

Finally, one of the emerging threats in 4G mobile network is diameter injected signaling flood, which has a great impact on LTE networks [45].

In fact, diameter is expected to become the most important protocol for the control plane signaling in IMS used to provide Authentication Authorization and Accounting (AAA) services. It is in charge of managing device mobility, roaming, complex policy-based billing models, QoS, and new services (IMS-based services, including Rich Communication Services (RCS) and Voice over LTE (VoLTE), and generates high levels of signaling traffic directed at different core network elements. Security and network disruption threats related to diameter signaling affect uniquely IP-based mobile networks. diameter based signaling messages can be exploited by an attacker to launch attacks against subscribers and network components (diameter malformed messages, diameter message flooding) [28]. As a solution for the detection and mitigation of diameter related security issues and attacks, the authors proposed a proactive and reactive service-based approach, which includes an *anomaly detection system* using a specification enabler rule engine applying different rules to incoming call data, a *signature-based detection* for attacks profiling, and the CUSUM technique. This solution

can mitigate malicious activities and diameter related threats through the encryption of diameter message in order to detect malformed message, as well as flooding attacks using the CUSUM.

C. SIGNALING ATTACKS

In this section, we review signaling attacks, which are a major threat in the 4G mobile network, particularly in the LTE signaling plane. The Table 4 provides an overview of typical signaling DoS attacks in 4G.

In fact, the LTE signaling plane can be targeted by signaling attacks, particularly by exploiting vulnerabilities related to the Bearer activation and deactivation [15]. Bearer is a key element of the QoS in LTE networks, and consists in a virtual connection between P-GW and the UE.

3GPP requirements for the design of session and bearer control in LTE are focused on providing a default IP access service allowing an ''always-on'' IP connection with a default bearer establishment and service context activation signaling during the network attachment, network-controlled service requiring network initiated session establishment signaling, multiple PDN Access also requiring UE initiated session establishment signaling, QoS aggregation, and message concatenation (to reduce service setup delays).

To fulfill requirements for session bearers, [22] proposed an optimized session and bearer control signaling, consisting in network-initiated session activation, modification, and deactivation procedures, with a default IP access service and multiple PDN access support, and UE-initiated session activation procedure, capable of providing messages concatenation in order to optimize the session and bearer control signaling.

Depending on the level of QoS to be achieved, several bearers are standardized, each bearer has its own QoS parameters based on the type of the application. Typical bearers are:

- *E-RAB*: is a radio bearer between UE and eNB,
- *S1 bearer*: is a bearer between eNB and S-GW,
- *S5-S8 bearer*: is a bearer between S-GW and P-GW.

To activate/deactivate a bearer, twelve signaling messages are required, six of which are processed by the eNB. Thus, the resulting signaling overhead can be exploited to launch the LTE signaling attacks such as the attack examined in [15], which depends on repeatedly and simultaneously sending a large number of dedicated bearer requests in order to force bearer activation and deactivation.

Another typical bearer attack, known as *resource reservation attack*, can be performed by a small number of users reserving maliciously the resources at the eNB by requesting high bandwidth bearers while strategically having a low MCS, thus causing a denial of service for all other users of the same cell requesting TCP-based applications [16].

Compared to the signaling attack in [16], the attack presented in [44] depends on a signaling DoS attack on the RAB, which exploits the vulnerability related to the MCS index used to determine the MCS. In fact, a high MCS index indicates a good channel quality and leads to use higher-order modulation schemes, whereas a low MCS index indicates a poor quality channel and leads to use a low-order modulation scheme. Typically by using a low MCS Index, Guaranteed Bit Rate (GBR) bearers that need a high Bandwidth (BW) can be allocated more eNB RAB resources than required.

To mitigate such attack, authors in [16] proposed to define an adaptive minimum MCS threshold below which high BW bearers would be rejected. This threshold can be set by operators. It could be increased during times of network congestion and decreased when enough resources are available. Contrarily to the adaptive MCS threshold, authors in [44] proposed a two steps DoS detection system. First, the algorithm provides a classification of the radio resource allocation/release of UEs by analyzing GTP-C control messages of each UE, prior to proceeding to the detection of virtual setup by analyzing the data traffic during allocation time. Second, the algorithm detects signaling DoS by analyzing the time interval between the virtual setups. However, the efficiency of this solution has not been demonstrated, and still needs to be tested.

Another category of signaling attacks on LTE bearers can be performed by exploiting vulnerabilities in the TAU procedure, whose security entirely depends on MME. Due to the lack of user authentication and the lack of protection mechanisms in the S-GW for the TAU, illegal users may be able to launch various attacks against MME such as sending Create Bearer Request attack, overloading S-GW, or using compromised UE to continuously trigger TAU [103]. As a countermeasure against these attacks, [103] proposed a security enhancement scheme to address the issues of DoS, which can prevent S-GW from being attacked by malicious requests during the TAU procedure when UE enters new Tracking Area (TA). This scheme can distinguish legitimate users from illegal ones. In fact, by exploiting the fact that IMSI is present in every TAU Request, MME can send a Create Bearer Request to the S-GW with the IMSI, whom in turn checks whether it has received more than one Create Bearer Request for the user, or by using Query Request message sent to the old S-GW to check the user authenticity in case of an attack from the unauthenticated user.

An important point is the possibility to perform DDoS in 4G mobile networks by using coordinated signaling DoS attacks (or signaling amplification attacks) from botnets, which can have huge impacts on the LTE air interface. According to [25], DDoS from botnets can be achieved through signaling amplification attacks (signaling messages flood) in order to drain the network resources and affect its performance. As a countermeasure, ECN based congestion mitigation is proposed to avoid congestion in diameter interfaces. This solution is an extension of TCP/IP and uses a transport layer congestion avoidance algorithm in order to prevent the surge of messages at the router through ECN

TABLE 4. Signaling attacks.

Attack reference map in 4G mobile networks		
Attacks Targets	**Attacks Type**	**Proposed Solution**
DoS	Repetitive MME Create Bearer Request attack for triggering TAU procedure	Proposed a new security enhancement scheme to distinguish between legal and illegal user [103]
DoS	LTE Radio Interface and Bearer Control signaling	Proposed an optimized session and bearer control signaling, consisting in network-initiated session activation, modification, and deactivation procedures [22]
DoS	MS initiated signaling DoS	Proposed a new method of detection based on IP packet traces to infer the presence of a malicious application [104]
DoS	Signaling DoS attack: • Repetitive network connection/release	Proposed a 3-Steps DoS Detection System [44]
DoS	LTE air interface vulnerability to Botnet	No Solutions proposed [25]
DoS	• Low traffic volume DoS • DDoS attack in LTE network • Signaling Amplification Attacks • Diameter injected signaling flood attack	Proposed an ECN based congestion mitigation [45]
DoS	RRC LTE signaling attacks: • Resource reservation attacks • Repetitive dedicated bearer requests using incorrect MCS Index value	Proposed an adaptive minimum MCS threshold below which high Bandwidth bearers are rejected [15], [16]
DoS	HSS/AuC flooding attack using unprotected messages in LTE procedure	[14] analyzed threats of unprotected RRC messages, unprotected C-RNTI in layer 1 handovers procedure, and unprotected IMSI in connection establishment. No solution proposed
DoS	LTE NAS request attack	[77] discussed HSS flooding, false buffer status reports attack in relation with OFDM DoS-based jamming attacks

markings learning at the senders end. Upon receipt of a congestion marked packet, the TCP receiver informs the sender in the subsequent Acknowledgment (ACK) message about imminent congestion, which will in turn trigger the congestion avoidance algorithm at the sender.

In [104], authors have also analyzed DoS attacks and proposed a solution based on a detector of MS initiated signaling DoS. This solution analyzes IP packet traces by examining characteristics of wake-up IP packets in order to infer the presence of a malicious signaling attack application, and can also be applied to DDoS. According to the authors, their solution can improve attack prevention resulting from MS initiated signaling by detecting and quarantining infected terminals.

As mentioned earlier, LTE has introduced a sharp increase of video traffic in mobile networks, which can be used to congestion network. To address signaling overhead related to high volume of video traffic streaming, which can raises the OPEX for mobile operators, authors in [105] proposed a Content-Aware (CA) priority marking and layer dropping scheme in order to enable highly efficient Quality of Experience (QoE)-based layer dropping at eNB. In LTE, this scheme can be applied in two modules: a CA priority marking module that marks every packet of video layer with the correspondent priority, and a CA layer dropping, which in turns drops packet receives at eNB based on their priority. Compared to existing solutions, the proposed CA depends on video layer priority marking scheme that indicates the transmission order for the layers of all transmitted videos across all users, and QoE-based layer dropping mechanism at the eNB. This scheme can be performed at the application layer, depending on where video is available.

Finally, another typical signaling attack is related to the NAS request attack targeting the HSS/AuC. This attack can be performed by exploiting vulnerabilities in the NAS of the E-UTRAN due to the unprotected RRC messages exchanges during the attachment procedure: *RRCConnectionRequest*, *RRCConnectionSetup*, *RRCConnectionSetupComplete*, *RRCConnectionReject*, and *RRCConnectionRelease*. Details on RRC messages are provided in [106]. In addition, the unprotected transmission of IMSI during connection establishment, and unprotected transmission of Cell Radio Network Temporary Identifier (C-RNTI) during the layer 1 handovers procedure can also be used to launch such attack. In fact, since C-RNTI is a temporary identifier of a mobile within the cell radio network assigned by the network via RRC control signals, this vulnerability can be exploited to cause a DoS attack by flooding the HSS/AuC [14]. Even though the effectiveness and impact of control signal DoS attacks have been presented including flooding of HSS/AuC, they have not proposed any mitigation solution. However, they have pointed out how to exploit weaknesses in E-UTRAN in order to carry efficient DoS attacks.

D. JAMMING-BASED ATTACKS

In this section, we primarily detail jamming-based DoS attacks in 4G networks focusing on LTE, and review

TABLE 5. Jamming based attacks.

Attack reference map in 4G mobile networks		
Attacks Targets	**Attacks Type**	**Proposed Solution**
DoS	WiMAX and LTE Security threats: • LTE Physical layer attacks • MAC Layer attacks WiMAX	Proposed RRC ciphering and User Plane protection [24]
DoS	• eNB spoofing • Unauthorized access • Eavesdropping of user traffic	Proposed a new authentication scheme based on: • Physical layer authentication • Physical layer key generation • Physical layer encryption • Beamforming and precoding technique [107]
DoS	LTE availability attacks: • Low traffic volume DoS attacks • High traffic volume DDoS attacks • Insider attack	Proposed: • A new security-oriented network architecture • Investigations on broadcast and control channel protection, cognitive radio,reuse of legacy networks, and distributed bearer management procedure [108]
DoS	Service disruption attacks: • Maximum impact jamming attack • Minimum power jamming attack	Discussed detection measures based on the estimated received signal strength from their throughput degradation [109]
DoS	Attacks against WiMAX: • Jamming and scrambling attacks • Spoofing and MITM attacks • Eavesdropping attacks	Discussed solution based on: • Authentication and digital signature • Encryption • Spread spectrum and strong scheme techniques [60]
DoS	Smart Jamming attacks against: • LTE CS-RS • LTE physical channels (PBCH, PCFICH, PUCCH, PRACH LTE)	Proposed: • Repeated game learning algorithm • Pilot boosting • Change of eNB Frequency and Timing • Research on smart jamming impact on a multi-cell configuration [110]
LTE physical layer DoS	Correlated jamming attacks (Protocol aware Jamming)	Proposed: • Monitoring of excess PUCCH energy • Monitoring of eNB BER based on CQI value • Dynamic PUCCH sizing [39]
LTE physical layer	Correlated Jamming attacks: • Noise Jamming ,Interference Jamming, • OFDM Synchronisation and Equalization Jamming attacks • Control Channel jamming attacks	Proposed several mitigation techniques including: • Pilot tone transmitting • Monitor control channels extra energy • Randomize control channels • Use of shared key [19]
LTE physical layer	Jamming against LTE interfaces and control channel: • Attack at Gi/Sgi interface • Attack S1 interface • Attack Gp/S8 interface	Analyzed mitigation techniques based on: • Spread-spectrum modulation • PUCCH radio resource allocation scrambling • MIB and SIBs encryption • Periodic PUSCH resources allocation • Extra-blind decoding against PCFICH jamming attacks • Selective uplink smart jamming interference cancellation [5], [5], [18], [39], [62], [62], [108], [111]
LTE physical layer	Traffic analysis attack	Proposed physical layer phase encryption [95]

current existing solutions based on the research literature. Jamming attacks are known as interference attacks and can take place at different layers, particularly in the physical layer, where the main threat relates to the radio jamming. Radio jamming can be understood as the deliberate transmission of radio signals in order to disrupt communications by decreasing the Signal-to-Noise Ratio (SNR) of the received signal [108]. The Table 5,

presents different physical layer threats and jamming attacks.

In [40], authors have identified and examined several forms of jamming in wireless networks, which can be summarized as follows:

- *Constant jamming*: consists in continuous transmission of a jamming signal over the shared wireless medium. It can lead to an increase of the interference and noise level, and a degradation of the signal reception quality. As additional effect, the wireless channel is always busy, which keeps preventing the legitimate transmitter from gaining access to the channel. Therefore, it provides the constant jamming attack with ability to disrupt the legitimate communications, despite its energy-inefficient aspect due to continuous jamming signal emission.
- *Intermittent jamming*: consists in emitting a jamming signal from time to time.
- *Reactive jamming*: in order to corrupt data at the reception, a jamming signal transmission is started when the legitimate transmission is detected to be active. Compared to constant and intermittent jamming, reactive jamming has less impacts due to the fact that only data at the reception are corrupted while the legitimate transmitter is still able to access the wireless channel.
- *Adaptive jamming*: in this attack, the transmitted jamming signal is adjusted to the level of received power at the legitimate receiver. A similarity with the reactive jamming is the fact that the adaptive jamming does not transmit when the legitimate transmission is not detected and is inactive. However, the hardness to detect such attack due to the dynamically jamming adjustment is one of its challenging characteristics.
- *Intelligent jamming*: this typically exploits weaknesses of the upper-layer protocols in order to block the legitimate transmission. To perform such attack, a thorough understanding of the upper-layer protocols is required in order to target the vitally critical network control packets instead of data packets, based on the related protocol vulnerabilities. Typical attacks include jamming of the MAC control packets in WiFi, which can be grouped into Ready To Send (RTS) jamming attack, Clear To Send (CTS) jamming attack, and ACK jamming attack [112].

In the case of Physical layer jamming attacks, it comprises only the first four types of jamming, whereas intelligent jamming attacks essentially take advantage of the vulnerabilities of the upper-layer protocols such as the MAC, network, transport and application layers. In fact, some of these jamming attacks targeting the transport and network layers can be performed as packet injection and spoofing of network level control information, and are also known as *selective jamming attacks* [113]–[115].

In LTE networks, jamming attacks in the physical layer can be performed by taking advantages of vulnerabilities of LTE physical channels and physical layer signals [77]. Moreover, as LTE is based on the OFDM transmission technique, the lack of resistance of OFDM to jamming and interference, data integrity and information privacy attacks, is a major threat of LTE networks against DoS and loss of service attacks, compared to spread spectrum systems [110].

Different types of jamming attacks in LTE have been identified. These types include: Smart Jamming, Noise Jamming, Correlated Jamming and Jamming over the control channel.

1) SMART JAMMING

Depends on local disruption of LTE communications without raising alerts, by saturating uplink and downlink controls channels, and tends to be hardly detected and mitigated [108]. There are two forms of smart jamming attacks: downlink smart jamming and uplink smart jamming.

In *downlink smart jamming attacks*, a malicious radio signal is generated in order to interfere with the reception of critical downlink control channels information. In *uplink smart jamming attacks*, on the contrary, the uplink control channel is the main target. By targeting the uplink control channel, it can prevent the eNB from receiving essential signaling messages required for the correct operation of the cell. Performing such attack requires prior knowledge of the Physical Resource Block (PRB) assigned to an uplink control channel at the physical layer, which can be obtained from SIB unprotected messages carried by the PBCH and Physical Downlink Shared Channel (PDSCH) [18]. In fact, MIB and SIB unprotected messages are carried in PBCH channel in the initial access procedure to the LTE network and may be eavesdropped as mentioned in earlier sections. In practical terms, a rogue base station attack can be optimized by combining smart jamming on the LTE network in order to first obtain information from the unencrypted MIB and SIB messages, and then force the UE to camp on a fake GSM cell, as no network authentication is required [70].

In [110], authors also analyzed LTE networks vulnerabilities against the DoS and loss of service attacks launched by smart jammers, and provided an overview of possible jamming attacks in the LTE air interface. According to the authors [110], the impact of smart jamming on the performance of LTE networks is still an open problem. An attacker may perform smart jamming DoS attacks on the common control channels, and OFDM pilot symbols such as CS-RS in LTE, by using simple narrowband jamming techniques, without requiring hacking of the network or its users. This can be achieved through a power-limited smart jammer targeting the CS-RS, the PBCH, or the PCFICH, and can lead to loss of Control Format Indicator (CFI). Another impact is the loss of tracking of critical feedback information from UEs in the PUCCH. In addition, a blocking of PRACH reselection and handover of UEs from neighboring cells to the jammed cell, and also possible blocking of out-of-sync and idle mode UEs in the jammed cell to get uplink synchronized and transition to connected state, respectively, can also result.

To mitigate such attacks, authors proposed a repeated game learning and strategy algorithm and suggested different possible countermeasures such as increasing CS-RS Transmit Power (Pilot boosting) in order to mitigate CS-RS jamming, throttle all UEs throughput (threat mechanism), change of eNB frequency and timing, and change of SIB2 (PRACH and PUCCH configuration). However, effects of smart jamming on a multi-cell configuration still need to be understood as well as design of future solutions.

2) NOISE JAMMING

Depends on injecting noise into the receiver and takes different forms such as:

- Barrage jamming attack: this form of jamming is also referred to as Broadband noise Jamming attack, and consists in interfering with the entire bandwidth occupied by OFDM sub-carriers with a high noise level [19], [77].
- Partial-band noise jamming attack: this jamming technique consists in jamming a portion of the entire BW by transmitting Additive White Gaussian Noise (AWGN) over it. It can be performed as a Single-Tone Jamming attack, or Multi-Tone Jamming attack. Single tone jamming requires a single high powered impulse of AWGN noise to be transmitted so as to interfere with a certain band of interest. This can affect only LTE downlink single subcarriers. Multi tone jamming can be considered as a variant of partial barrage jamming, in which multiple numbers of equally powered noise are transmitted in order to take down a multiple number of frequency subcarriers within the LTE bands. This attack tends to be highly effective in case of limited power on the transmit side.
- Chirp jamming attack: consists in a continuous wave tone with constantly changing frequency over time. This type of jamming is the most difficult to mitigate.

3) CORRELATED JAMMING

Can cause severe impact on the OFDM transmission using minimal power. In particular, this type of jamming includes the *Protocol-Aware Jamming*, which requires a prior knowledge of the protocol used by the target. Different forms of correlated jamming attacks including synchronization jamming and equalization jamming have been identified.

First, *Synchronization Jamming Attacks* is a correlated jamming, which can target the timing acquisition and the carrier frequency offset estimation [19], [111]. These attacks can be performed as follows:

- *False Preamble Timing Attack*: depends on either moving the preamble, or destroying it altogether in order to disrupt the symbol timing estimation. This can be achieved by creating a new timing metric. Depending on knowledge that the jammer has about the preamble, it is possible to either transmit the false preamble, a false preamble altogether with the correct preamble or the correct preamble at an incorrect time.
- *Preamble Nulling Attack*: aims to null the preamble required for the synchronization by inverting the preamble symbol in time. It requires a perfect knowledge of the preamble as viewed by the receiver in order to transmit a structured waveform capable to drive the received energy of the preamble at the target receiver close to zero.
- *Preamble Warping*: aims to destroy timing correlation. It can be performed through attacks on the frequency domain structure of the preamble by destroying the correlation between the two halves of the first preamble symbol.
- *Preamble Phase Warping*: aims to disrupt the frequency offset estimate of the receiver by sending to it a frequency shifted preamble.
- *Differential Scrambling Attack*: the main goal is to disrupt the coarse frequency error estimation at the receiver by transmitting a constant stream of symbols across the sub-carriers used in the first preamble.

Second, *Equalization Jamming Attack* is also a correlated jamming attack. It aims at disrupting the equalization process. Several techniques can be used to perform this attack including:

- *Pilot Jamming Attacks*: can be achieved by transmitting AWGN on the pilot tone in order to raise its noise floor and disrupt the equalization process. It requires a perfect synchronization between the jammer and the target signal.
- *Pilot tone Nulling Attacks*: this form of jamming also requires prior knowledge of the channel, and aims to null the pilot tone at the target receiver by transmitting a channel-corrected signal, which is Π-radian phase shifted of the pilot tone. As a result, the original pilot tone is cancelled out, leading to the degradation of the network performance.
- *MIMO-OFDM channel sounding attacks*: this can be performed by exploiting the possibility of jamming the channel estimation procedure. In the case of the Multiple Input Multiple Output (MIMO), this attack is also referred to as the *singularity attack* and consists in a multi-antenna jammer that tries to manipulate pilot tone in order to skew the Channel State Information (CSI) at the receiver. CSI reports allow an eNB to decide what specific MIMO scheme can be employed at any given time [116]–[121].
- *Cyclic Prefix Jamming Attacks*: this attack targets the cyclic prefix, and can result in the knocking-off of the correlation and disruption of the received signal.

4) JAMMING OVER THE CONTROL CHANNEL

Is a typical form of jamming targeting the control channel in 4G LTE [77]. This attack can be performed by exploiting vulnerabilities related to the PCFICH and PUCCH channels in the down-link and up-link signals, the J/S ratio in OFDM physical channels (PDSCH/PUSCH, PCFICH,

PUCCH, PBCH, Physical Hybrid-ARQ Indicator Channel (PHICH)), the LTE physical layer signal Primary and Secondary Synchronization Signals (PSS), and the Downlink Reference Signals (RS)) [77]. In fact, control channels such as PUCCH play a key role in the LTE transmission, as they are used to transmit vital control signaling. Therefore, jamming the spectrum allocated to the PUCCH can result in the reduction of the LTE link availability within one or more cells due to the impacts of this attack. As examples of impacts of this attack, there are the impossibility of the control signaling to reach eNBs, the redundant re-transmission and delays of downlink data in relation with erroneous ACK and Non acknowledgment (NACK), and the phantom scheduling requests related to erroneous SR causing eNB to allocate PUSCH to a UE not requesting transmission. Other impacts include the poor link adaptation due to erroneous CQIs, and corrupted MIMO feedback due to erroneous CSI received on eNB.

Moreover, attacks on control channels can also be performed by jamming a portion of the uplink or downlink signals. In this case typical attacks include:

- *HARQ Acknowledgement Attack*: can cause delays and unnecessary re-transmission.
- *Random Access Channel Attack*: depends on interfering with the portion of the uplink bandwidth assigned to random access requests. By flooding the random access channel, this attack can result in the impossibility of the base station to allow a user to initiate communication.
- *Modulation Indicator Attack*: this attack can be carried out by jamming the Modulation Scheme Indicator (MSI) in order to cause an incorrect data demodulation at the receiver, a higher Bit Error Rate (BER), and corrupted CQI. In fact, corrupting CQIs can lead to either a lower modulation order on a subcarrier which would otherwise be able to handle more, or an excessively high modulation order which will increase the BER on the subcarrier.
- *Resource Allocation Attack*: this type of attacks can be performed by corrupting resource allocation information, which can result in DoS.

In order to mitigate AWGN noise and noise-like jamming attacks on OFDM, [19] proposed different solutions mitigated by using different techniques:

- Equalization attacks can be mitigated by transmitting pilot tones whose values are unknown to the attackers, or randomizing the pilot locations.
- Control channel attacks: can be mitigated by including the vulnerable control information in unoccupied data resources, monitoring of extra energy in control channels, randomizing control channels location in time and frequency, and using a shared key to pass location information to the user.

Other mitigation solutions and approaches against jamming attacks in LTE including physical layer authentication, physical layer key generation and physical layer encryption. As LTE physical security mechanisms are focused on physical layer authentication, physical layer key generation and physical layer encryption, mitigating attacks at the physical layer can be achieved through authentication process based on the physical-layer security techniques, in order to simplify the signaling interaction as well as enhance the security of the system, and provide reduction of the overhead of information exchange and signaling transmission [107]. Moreover, it does not require symmetric key in the system due to the use of the channel reciprocity to generate the key according to the channel characteristics, and ensures transmission security through beamforming and precoding techniques.

In addition, as a solution against the loss of orthogonality between the bonded or fragmented spectrum bands, which can be exploited to cause service disruption in IEEE 802.22-based DSA networks, LTE, and High Speed Packet Access (HSPA)+ networks, [109] proposed detection measures based on the estimated received signal strength from their throughput degradation. To be efficient, such detection mechanism depends on the difference between the average transmit power of the good users and the transmit power of the attackers, and can be enhanced by deploying a cooperative detection.

To mitigate effects of the *'protocol-aware'* jamming attacks against the PUCCH channel, [39] analyzed possible detection and mitigation methods, and proposed the monitoring of excess PUCCH energy, which allows attack detection based on the presence of energy in resource elements in PUCCH region that is not assigned. In addition, the monitoring can simply detect an abnormally high amount of energy in the PUCCH region altogether, detect an abnormal amount of PUCCH errors by monitoring eNB for a sudden increase in errors on the PUCCH, as well as Bit errors by watching received CQI values that are not valid.

As countermeasures, authors proposed to give the user PUSCH resources for each subframe it has uplink control information to send, as well as given periodic PUSCH resources, or by using dynamic PUCCH sizing, and to grant periodic PUSH for subcomponent in presence of phantom-SRs, delegating reliable transmission to higher layers by forcing all PDUs in the RLC to use unacknowledged mode (RLC-UM) to mitigate the impact of PUCCH interference on HARQ processes.

To achieve full availability and resiliency of cellular networks against security attacks, authors in [108] have outlined future research directions such as:

- Broadcast and Control Channel protection: will be needed for enhanced jamming resiliency.
- Initial access to the network: concepts of cognitive radio and reuse of legacy networks could be applied to design more robust radio resource allocation architectures.
- RRC bearer management: distributed bearer management procedure in order to distribute EPC signaling load and minimize its impact is required.

- Implementation of distributed solutions: to reduce central node dependency.
- Core network signaling: strong SoN and software-based network nodes could minimize the NAS signaling load at the EPC and provide mitigation features to balance, re-route, or filter network control traffic, and could be applied in a flexible and adapting architecture.

V. OPEN RESEARCH PROBLEMS

In this section, we identify open issues in mobile networks security by pointing out areas that need more research investigation.

A. MITIGATING 4G AVAILABILITY AND SECURITY ATTACKS

DoS and DDoS attacks in 4G mobile are still an open issue and can be performed by exploiting vulnerabilities presented in previous sections. Possibility to launch attacks in LTE converged networks (Physical and MAC layer of WiMAX) have been pointed out [24], [60]. However, there is still a need to design new protection and encryption mechanisms to be applied at the physical layer.

DoS attacks can also result from the integration of WLAN and 4G/LTE networks [23], [28]. Solutions proposed against these threats are based on a stateful analysis monitoring system. In the case of attacks on diameter, proactive and reactive service-based approaches have been proposed including *anomaly-based and signature-based detection systems*. Efficiency of these solutions on operational mobile networks has not been demonstrated. Future security research on mobility network attack detection in order to provide a RAN level advanced attack detection system is suggested [108].

In the LTE security architecture, there are some issues worth investigating. In fact, more security mechanisms in the system architecture must be designed in order to protect communications from traditional protocol attacks and physical intrusions in the LTE networks.

Additional enhancements in EPS AKA scheme are needed, as well as a design of secure access authentication mechanisms to be used during UE access to the EPC via non-3GPP networks, in order to protect against the disclosure of user identity, DoS attacks and other malicious attacks. In addition, the security of the LTE Handover procedure is still an open issue requiring further enhancements in the key management mechanisms and handover authentication procedures in order to prevent protocol, desynchronization, and replay attacks.

A new trend is the integration of Machine to Machine (M2M) in mobile networks. In this context, some investigations need to be carried regarding authentication threats that may raise. In fact, there have been several papers about issues related to EPS AKA weaknesses such as bandwidth consumption and signaling overhead between serving and home networks [11], [29], [50]. However, few of them have addressed potential threats and attacks from M2M towards 4G mobile networks.

In the E-UTRAN NAS, weaknesses in E-UTRAN are still some open issues related to control signal for the HSS/AuC flooding attacks [14]. Potential research areas include software-based network nodes in order to minimize the NAS signaling load at the EPC and provide mitigation features to leverage network control traffic.

B. MITIGATING LTE BACKHAUL ATTACKS

The backhaul threats are mainly IP-based attacks targeting control elements and interfaces.

GTP will still continue to be used as a tunneling protocol in 4G mobile networks, despite potential attack against GTP [25], [44]. The solution based on control traffic detection system cannot totally prevent and protect from packet tampering and resource exhaustion, as it is not efficient against an abnormal use of GTP create session request message during the initial attach of the MS.

To address IP-based threats in LTE backhaul networks, several existing solutions include security gateways used to filter connections, IPsec-based traffic encryption, and certificate authority. Certificate authority can prevent from unauthorized access to data and network components, and provide keys for traffic encryption. Potential future improvement can be achieved in DPI.

In addition, other solutions have been proposed, consisting in a layer 3 IPsec tunnel mode VPN architecture, based on a modified IKEv2 protocol, and HIP protocol. This allows to create IPsec BEET (Bound End-to-End Tunnel) based VPNs overlaid on top of the backhaul network in order to provide protection against spoofing attacks, user authentication and authorization, payload encryption, and privacy protection [12]. A particular interest is to investigate efficiency of this solution in the context of cloud-based virtualized network infrastructure and Software Defined Network (SDN).

Botnets are considered as major threats in 4G mobile networks, since they can be used to launch large scale DDoS (signaling amplification attacks) [45]. Some proposed countermeasures include ECN Based congestion mitigation. A typical threat related to Botnets is the signaling attack against session bearer management procedure. The proposed mitigation solutions suggest network-initiated session activation, modification, and deactivation procedures [22].

Through the analysis, we have shown that the E-UTRAN is vulnerable to false base station, eavesdropping, redirection attacks, MITM attacks and DoS attacks. Various solutions and countermeasures, which have been proposed to mitigate these issues, include physical layer security mechanisms (key generation and encryption), strong authentication, enhanced encryption schemes and security architecture. However, these current solutions are not fully efficient, for example in the scenario of attacks against paging procedure (user localization or tracking attack). Therefore, it will be required to enhance security mechanisms in order to mitigate this type of attack.

In the backhaul and EPC, threats related to unauthorized access, DoS/DoS, signaling storms and flooding, IP spoofing,etc. still affect the the ability of network elements to serve new traffic and can lead to service unavailability, despite current existing proposed solutions such as security

architecture, VPNs, encryption, network and traffic monitoring, IPS, etc. Typical, signaling attacks such as RAB establishment/release attacks, paging attacks, and attach request in the scenario of HSS flooding can not be prevented and detected. As these threats can have high impact on MME, HSS and HLR, designing a new integrated mechanism in 4G LTE to secure the initial attach request is still an open issue.

In addition, in the E-UTRAN physical layer, Jamming attacks are still a major threat needing more research investigations. Solutions based on information-theoretic security, artificial noise aided security, security-oriented beamforming techniques, diversity-assisted security approaches, and physical-layer secret key generation have been suggested by the researchers, but are still at their infancy and more investigation will be needed for practical implementation design.

Finally, with the evolution towards LTE-A networks, M2M communications are expected to be integrated and carried over mobile networks. New threats related to the application security and privacy are emerging as a major concern. Therefore, investigating the impact of coordinated joint attacks launch from dynamic connected devices is a challenging topic to be addressed by future research.

VI. CONCLUSION

Protecting and securing mobile networks is still a major concern for MNO. In this paper, we have reviewed the security issues in mobile networks. Due to the evolution in mobile network architecture, several weaknesses have been bought to the network introducing new threats, which can be used to perform attacks in the E-UTRAN and the EPC. These attacks can target both the AS and NAS protocols inside the C-plane and the U-plane. We have also provided an attack categorization and reviewed the current solutions and mitigation techniques that have been proposed in regards to the technology involved, type and category of attacks. Some open issues that need to be investigated further by the research have also been identified.

REFERENCES

[1] A. Kumar, Y. Liu, J. Sengupta, and Divya. (Dec. 2010). *Evolution of Mobile Wireless Communication Networks: 1G to 4G*. [Online]. Available: http://www.iject.org/pdf/amit.pdf

[2] M. Oğul and S. Baktır, "Practical attacks on mobile cellular networks and possible countermeasures," *Future Internet*, vol. 5, no. 4, pp. 474–489, 2013. [Online]. Available: http://www.mdpi.com/1999-5903/5/4/474

[3] GSM Association. (2015). *The Mobile Economy 2015*. [Online]. Available: http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf

[4] M. Sher and T. Magedanz, "3G-WLAN convergence: Vulnerability, attacks possibilities and security model," in *Proc. 2nd Int. Conf. Availability, Rel. Secur. (ARES)*, Apr. 2007, pp. 198–205.

[5] Z. Ahmadian, S. Salimi, and A. Salahi, "New attacks on UMTS network access," in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2009, pp. 1–6.

[6] S. Othmen, F. Zarai, M. S. Obaidat, and A. Belghith, "Re-authentication protocol from WLAN to LTE (ReP WLAN-LTE)," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 1446–1451.

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

[8] Y. Zheng, D. He, W. Yu, and X. Tang, "Trusted computing-based security architecture for 4G mobile networks," in *Proc. 6th Int. Conf. Parallel Distrib. Comput. Appl. Technol. (PDCAT)*, Dec. 2005, pp. 251–255.

[9] T. Wu and G. Gong, "The weakness of integrity protection for LTE," in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, New York, NY, USA, 2013, pp. 79–88. [Online]. Available: http://doi.acm.org/10.1145/2462096.2462110

[10] Y. Zheng, D. He, X. Tang, and H. Wang, "AKA and authorization scheme for 4G mobile networks based on trusted mobile platform," in *Proc. 5th Int. Conf. Inf. Commun. Signal Process.*, 2005, pp. 976–980.

[11] X. Li and Y. Wang, "Security enhanced authentication and key agreement protocol for LTE/SAE network," in *Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCOM)*, Sep. 2011, pp. 1–4.

[12] M. Liyanage and A. Gurtov, "Secured VPN models for LTE backhaul networks," in *Proc. IEEE Veh. Technol. Conf. (VTC Fall)*, Sep. 2012, pp. 1–5.

[13] C.-K. Han and H.-K. Choi, "Security analysis of handover key management in 4G LTE/SAE networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 457–468, Feb. 2014.

[14] D. Yu and W. Wen, "Non-access-stratum request attack in E-UTRAN," in *Proc. Comput., Commun. Appl. Conf. (ComComAp)*, Jan. 2012, pp. 48–53.

[15] R. Bassil, I. H. Elhajj, A. Chehab, and A. Kayssi, "Effects of signaling attacks on LTE networks," in *Proc. 27th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Mar. 2013, pp. 499–504.

[16] R. Bassil, I. H. Elhajj, A. Chehab, and A. Kayssi, "A resource reservation attack against LTE networks," in *Proc. 3rd Int. Conf. Commun. Inf. Technol. (ICCIT)*, Jun. 2013, pp. 262–268.

[17] S. Park, S. Kim, J. Oh, M. Noh, and C. Im, "Threats and countermeasures on a 4G mobile network," in *Proc. 8th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2014, pp. 538–541.

[18] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks," *EURASIP J. Inf. Secur.*, vol. 2014, no. 1, pp. 1–14, Dec. 2014. [Online]. Available: http://dx.doi.org/10.1186/1687-417X-2014-7

[19] C. Shahriar *et al.*, "PHY-layer resiliency in OFDM communications: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 292–314, 1st Quart., 2015.

[20] D. Forsberg, H. Leping, K. Tsuyoshi, and S. Alanara, "Enhancing security and privacy in 3GPP E-UTRAN radio interface," in *Proc. IEEE 18th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2007, pp. 1–5.

[21] Y. Park and T. Park, "A survey of security threats on 4G networks," in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1–6.

[22] J. Shin, K. Jung, and A. Park, "Design of session and bearer control signaling in 3GPP LTE system," in *Proc. IEEE 68th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2008, pp. 1–5.

[23] N. Qachri and J.-M. Dricot, "On the security of WLAN access points integrated in 4G/LTE architectures," in *Proc. 19th IEEE Workshop Local Metropolitan Area Netw. (LANMAN)*, Apr. 2013, pp. 1–6.

[24] B. Matt and C. Li, "A survey of the security and threats of the IMT-advanced requirements for 4G standards," in *Proc. IEEE Conf. Anthol.*, Jan. 2013, pp. 1–5.

[25] M. Khosroshahy, D. Qiu, and M. K. M. Ali, "Botnets in 4G cellular networks: Platforms to launch DDoS attacks against the air interface," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, Aug. 2013, pp. 30–35.

[26] G. Gorbil, O. H. Abdelrahman, M. Pavloski, and E. Gelenbe, "Modeling and analysis of RRC-based signalling storms in 3G networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 1, pp. 113–127, Jan. 2016.

[27] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[28] T. Q. Thanh, Y. Rebahi, and T. Magedanz, "A DIAMETER based security framework for mobile networks," in *Proc. Int. Conf. Telecommun. Multimedia (TEMU)*, Jul. 2014, pp. 7–12.

[29] M. Purkhiabani and A. Salahi, "Enhanced authentication and key agreement procedure of next generation evolved mobile networks," in *Proc. IEEE 3rd Int. Conf. Commun. Softw. Netw. (ICCSN)*, May 2011, pp. 557–563.

[30] I. E. Bouabidi, I. Daly, and F. Zarai, "Secure handoff protocol in 3GPP LTE networks," in *Proc. 3rd Int. Conf. Commun. Netw.*, Mar. 2012, pp. 1–6.

[31] M. Prasad and R. Manoharan, "Secure authentication scheme for long term evolution-advanced," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2013, pp. 11–15.

[32] K. Hamandi, I. Sarji, I. H. Elhajj, A. Chehab, and A. Kayssi, "W-AKA: Privacy-enhanced LTE-AKA using secured channel over Wi-Fi," in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2013, pp. 1–6.

[33] K. A. Alezabi, F. Hashim, S. J. Hashim, and B. M. Ali, "An efficient authentication and key agreement protocol for 4G (LTE) networks," in *Proc. IEEE Region 10 Symp.*, Apr. 2014, pp. 502–507.

[34] R.-H. Liou, Y.-B. Lin, and S.-C. Tsai, "An investigation on LTE mobility management," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 166–176, Jan. 2013.

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

[36] A. N. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," *IEEE Security Privacy*, vol. 11, no. 2, pp. 55–62, Mar./Apr. 2013.

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

[38] P. Rengaraju, C.-H. Lung, and A. Srinivasan, "QoS-aware distributed security architecture for 4G multihop wireless networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2886–2900, Jul. 2014.

[39] M. Lichtman, T. Czauski, S. Ha, P. David, and J. H. Reed, "Detection and mitigation of uplink control channel jamming in LTE," in *Proc. IEEE Military Commun. Conf.*, Oct. 2014, pp. 1187–1194.

[40] Y. Zou, J. Zhu, X. Wang, and L. Hanzo. (May 2015). "A survey on wireless security: Technical challenges, recent advances and future trends." [Online]. Available: https://arxiv.org/pdf/1505.07919.pdf

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

[42] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices," in *Proc. IEEE Symp. Secur. Privacy*, May 2011, pp. 96–111.

[43] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 446–471, 1st Quart., 2013.

[44] W. Jang, S. Kim, J. H. Oh, and C. T. Im, "Session-based detection of signaling DoS on LTE mobile networks," *J. Adv. Comput. Netw.*, vol. 2, no. 3, pp. 159–162, Sep. 2014. [Online]. Available: http://www.jacn.net/papers/103-A3003.pdf

[45] J. Henrydoss and T. Boult, "Critical security review and study of DDoS attacks on LTE mobile network," in *Proc. IEEE Asia Pacific Conf. Wireless Mobile*, Aug. 2014, pp. 194–200.

[46] 3GPP, *Feasibility Study for Evolved Universal Terrestrial Radio Access (UTRA) and Universal Terrestrial Radio Access Network (UTRAN)*, document TR 25.912, 3rd Generation Partnership Project (3GPP), Oct. 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/25912.htm

[47] Alcatel-Lucent. (2013). *The LTE Network Architecture A Comprehensive Tutorial, Strategic White Paper*. Available: http://www.cse.unt.edu/~rdantu/FALL_2013_WIRELESS_NETWORKS/LTE_Alcatel_White_Paper.pdf

[48] 3GPP, *3GPP System Architecture Evolution (SAE): Security Architecture Version 8.6.0 Release 8*, document TS 33.401, 3rd Generation Partnership Project (3GPP), Dec. 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33401.htm

[49] 3GPP, *3G Security; Security Architecture*, document TS 33.102, 3rd Generation Partnership Project (3GPP), Apr. 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33102.htm

[50] H. Choudhury, B. Roychoudhury, and D. K. Saikia, "Enhancing user identity privacy in LTE," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 949–957.

[51] C. Tang, D. A. Naumann, and S. Wetzel, "Analysis of authentication and key establishment in inter-generational mobile telephony," in *Proc. IEEE 10th Int. Conf. High Perform. Comput. Commun. IEEE Int. Conf. Embedded Ubiquitous Comput. (HPCC_EUC)*, Nov. 2013, pp. 1605–1614.

[52] D. Herceg, "LTE transport security," in *Proc. 34th Int. Conv. MIPRO*, May 2011, pp. 1464–1467.

[53] M. Paolini. (2012). *Wireless Security in LTE Networks*. [Online]. Available: http://www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili_WirelessSecurity_121029_FINAL.pdf

[54] G. Lyberopoulos, H. Theodoropoulou, and K. Filis, *Mobile Network Threat Analysis and MNO Positioning*. Cham, Germany: Springer, 2013, pp. 419–428. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-01604-7_41

[55] G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in *Proc. 34th Int. Conv. MIPRO*, May 2011, pp. 1468–1473.

[56] C. Szongott, B. Henne, and M. Smith, "Evaluating the threat of epidemic mobile malware," in *Proc. IEEE 8th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2012, pp. 443–450.

[57] U. Tupakula, V. Varadharajan, and S. K. Vuppala, "Security techniques for beyond 3G wireless mobile networks," in *Proc. IFIP 9th Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Oct. 2011, pp. 136–143.

[58] E. Gelenbe *et al.*, "Security for smart mobile networks: The NEMESYS approach," in *Proc. Int. Conf. Privacy Secur. Mobile Syst. (PRISMS)*, Jun. 2013, pp. 1–8.

[59] A. Bär, A. Paciello, and P. Romirer-Maierhofer, "Trapping botnets by DNS failure graphs: Validation, extension and application to a 3G network," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 393–398.

[60] M. Habib and M. Ahmad, "A review of some security aspects of WiMAX and converged network," in *Proc. 2nd Int. Conf. Commun. Softw. Netw. (ICCSN)*, Feb. 2010, pp. 372–376.

[61] M. Nagy and M. Kotočová, "An IP based security threat in mobile networks," in *Proc. 35th Int. Conv. MIPRO*, May 2012, pp. 667–670.

[62] CheckPoint Software Technologies. (Nov. 2013). *Next Generation Security for 3G and 4G LTE Networks*. [Online]. Available: https://www.checkpoint.com/downloads/product-related/whitepapers/wp-ng-mobile-network-security.pdf

[63] M. Khan, A. Ahmed, and A. R. Cheema, "Vulnerabilities of UMTS access domain security architecture," in *Proc. 9th ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw., Parallel/Distrib. Comput. (SNPD)*, Aug. 2008, pp. 350–355.

[64] H. Li, S. Guo, K. Zheng, Z. Chen, Z. Zhang, and X. Du, "Security analysis and defense strategy on access domain in 3G," in *Proc. 1st Int. Conf. Inf. Sci. Eng.*, Dec. 2009, pp. 1851–1854.

[65] Y.-L. Huang, C.-Y. Shen, and S. W. Shieh, "S-AKA: A provable and secure authentication key agreement protocol for UMTS networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 9, pp. 4509–4519, Nov. 2011.

[66] G. Kambourakis, C. Kolias, S. Gritzalis, and J. H. Park, "DoS attacks exploiting signaling in UMTS and IMS," *Comput. Commun.*, vol. 34, no. 3, pp. 226–235, Mar. 2011.

[67] E. Southern, A. Ouda, and A. Shami, "Solutions to security issues with legacy integration of GSM into UMTS," in *Proc. Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2011, pp. 614–619.

[68] K. Ammayappan, "Seamless interoperation of LTE-UMTS-GSM requires flawless UMTS and GSM," in *Proc. 2nd Int. Conf. Adv. Comput., Netw. Secur.*, Dec. 2013, pp. 169–174.

[69] S. Aragon, F. Kuhlmann, and T. Villa, "SDR-based network impersonation attack in GSM-compatible networks," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, May 2015, pp. 1–5.

[70] P. K. Nakarmi, O. Ohlsson, and M. Liljenstam, "An air interface signaling protection function for mobile networks: GSM experiments and beyond," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1. Aug. 2015, pp. 1192–1198.

[71] P. P. C. Lee, T. Bu, and T. Woo, "On the detection of signaling DoS attacks on 3G wireless networks," in *Proc. 26th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, May 2007, pp. 1289–1297.

[72] Z. Wu, X. Zhou, and F. Yang, "Defending against DoS attacks on 3G cellular networks via randomization method," in *Proc. Int. Conf. Edu. Inf. Technol. (ICEIT)*, vol. 1. Sep. 2010, pp. V1-504–V1-508.

[73] M. Chandra, N. Kumar, R. Gupta, S. Kumar, V. K. Chaurasia, and V. Srivastav, "Protection from paging and signaling attack in 3G CDMA networks," in *Proc. Int. Conf. Emerg. Trends Netw. Comput. Commun. (ETNCC)*, Apr. 2011, pp. 406–410.

[74] Y. Balmas. (Nov. 2013). *Mobile Network Security Availability Risks in Mobile Networks*. [Online]. Available: http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/Mobile_Networks_Security_Research_Paper.pdf

[75] X. Peng, Y. Wen, and H. Zhao, "Securing GPRS tunnel protocol in 3G core network," in *Proc. Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2010, pp. 469–473.

[76] S. Holtmanns, S. P. Rao, and I. Oliver, "User location tracking attacks for LTE networks using the interworking functionality," in *Proc. IFIP Netw. Conf. (IFIP Networking) Workshops*, May 2016, pp. 315–322.

[77] M. Lichtman, J. H. Reed, T. C. Clancy, and M. Norton, "Vulnerability of LTE to hostile interference," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Dec. 2013, pp. 285–288.
[78] S. Bhattarai, S. Rook, L. Ge, S. Wei, W. Yu, and X. Fu, "On simulation studies of cyber attacks against LTE networks," in *Proc. 23rd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2014, pp. 1–8.
[79] S. Bhattarai, S. Wei, S. Rook, W. Yu, R. F. Erbacher, and H. Cam, "On simulation studies of jamming threats against LTE networks," in *Proc. Int. Conf. Comput., Netw. Commun.(ICNC)*, Feb. 2015, pp. 99–103.
[80] A. Egners, E. Rey, H. Schmidt, P. Schneider, and S. Wessel. (Mar. 2012). *Threat and Risk Analysis for Mobile Communication Networks and Mobile Terminals*. [Online]. Available: http://www.asmonia.de/deliverables/D5.1_II_ThreatAndRiskAnalysisMobileCommunicationNetworksAndTerminals.pdf
[81] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," *ACM Comput. Surv.*, vol. 47, no. 4, pp. 55:1–55:33, Jul. 2015. [Online]. Available: http://doi.acm.org/10.1145/2716260
[82] A. M. Kanthe, D. Simunic, and M. Djurek, "Denial of service (DoS) attacks in green mobile ad-hoc networks," in *Proc. 35th Int. Conv. MIPRO*, May 2012, pp. 675–680.
[83] R. Muraleedharan and L. A. Osadciw, "Increasing QoS and security in 4G networks using cognitive intelligence," in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1–6.
[84] C. B. Sankaran, "Network access security in next-generation 3GPP systems: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 84–91, Feb. 2009.
[85] S. F. Mjølsnes and J.-K. Tsay, "Computational security analysis of the UMTS and LTE authentication and key agreement protocols," *CoRR*, vol. abs/1203.3866, 2012. [Online]. Available: http://arxiv.org/abs/1203.3866
[86] P. B. Copet, G. Marchetto, R. Sisto, and L. Costa, "Formal verification of LTE-UMTS handover procedures," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2015, pp. 738–744.
[87] J. Serror, H. Zang, and J. C. Bolot, "Measurement and modeling of paging channel overloads on a cellular network," *Comput. Netw.*, vol. 57, no. 13, pp. 2499–2513, Sep. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613001308
[88] P. K. Reddy K and B. R. Chandavarkar, "Mitigation of desynchronization attack during inter-eNodeB handover key management in LTE," in *Proc. 8th Int. Conf. Contemp. Comput. (IC3)*, Aug. 2015, pp. 561–566.
[89] H. Ghafghazi, A. El Mougy, H. T. Mouftah, and C. Adams, "Classification of technological privacy techniques for lte-based public safety networks," in *Proc. 10th ACM Symp. QoS Secur. Wireless Mobile Netw. (Q2SWinet)*, New York, NY, USA, 2014, pp. 41–50. [Online]. Available: http://doi.acm.org/10.1145/2642687.2642693
[90] C. Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Comput. Netw.*, vol. 57, no. 17, pp. 3492–3510, Dec. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613002570
[91] M. Zekri, B. Jouaber, and D. Zeghlache, "A review on mobility management and vertical handover solutions over heterogeneous wireless networks," *Comput. Commun.*, vol. 35, no. 17, pp. 2055–2068, Oct. 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366412002526
[92] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A simple and robust handover authentication between HeNB and eNB in LTE networks," *Comput. Netw.*, vol. 56, no. 8, pp. 2119–2131, May 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912861200076X
[93] L. J. Zhang and S. Pierre, "An enhanced fast handover with seamless mobility support for next-generation wireless networks," *J. Netw. Comput. Appl.*, vol. 46, pp. 322–335, Nov. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S108480451400157X
[94] Y. E. H. E. Idrissi, N. Zahid, and M. Jedra, "Security analysis of 3GPP (LTE)–WLAN interworking and a new local authentication method based on EAP-AKA," in *Proc. 1st Int. Conf. Future Generat. Commun. Technol.*, Dec. 2012, pp. 137–142.
[95] F. Huo and G. Gong, "Physical layer phase encryption for combating the traffic analysis attack," in *Proc. IEEE Int. Symp. Electromagn. Compat. (EMC)*, Aug. 2014, pp. 604–608.
[96] C. A. Ardagna, S. Jajodia, P. Samarati, and A. Stavrou, "Providing users' anonymity in mobile hybrid networks," *ACM Trans. Internet Technol.*, vol. 12, no. 3, pp. 7:1–7:33, May 2013. [Online]. Available: http://doi.acm.org/10.1145/2461321.2461322
[97] S. Park, S. Kim, K. Son, and H. Kim, "Security threats and countermeasure frame using a session control mechanism on VoLTE," in *Proc. 10th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, Nov. 2015, pp. 532–537.
[98] C.-Y. Li *et al.*, "Insecurity of voice solution VoLTE in LTE mobile networks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2015, pp. 316–327. [Online]. Available: http://doi.acm.org/10.1145/2810103.2813618
[99] H. Kim *et al.*, "Breaking and fixing VoLTE: Exploiting hidden data channels and mis-implementations," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2015, pp. 328–339. [Online]. Available: http://doi.acm.org/10.1145/2810103.2813718
[100] D. W. Kang, J. H. Oh, C. T. Im, W. S. Yi, and Y. J. Won, "A practical attack on mobile data network using IP spoofing," *Appl. Math. Inf. Sci.*, vol. 7, no. 6, pp. 2345–2353, Nov. 2013.
[101] D. Kurbatov, S. Puzankoz, and P. Novikov, "Vulnerabilities of mobile internet (GPRS)," Positive Technol., USA, Tech. Rep., 2014.
[102] G.-H. Tu, C.-Y. Li, C. Peng, and S. Lu, "How voice call technology poses security threats in 4G LTE networks," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 442–450.
[103] L. Qiang, W. Zhou, B. Cui, and L. Na, "Security analysis of TAU procedure in LTE network," in *Proc. 9th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. (3PGCIC)*, Nov. 2014, pp. 372–376.
[104] A. Gupta, T. Verma, S. Bali, and S. Kaul, "Detecting MS initiated signaling DDoS attacks in 3G/4G wireless networks," in *Proc. 5th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2013, pp. 1–60.
[105] B. Fu, D. Staehle, G. Kunzmann, E. Steinbach, and W. Kellerer, "QoE-based SVC layer dropping in LTE networks using content-aware layer priorities," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 12, no. 1, pp. 7:1–7:23, Aug. 2015. [Online]. Available: http://doi.acm.org/10.1145/2754167
[106] 3GPP, *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification*, document TS 36.331, 3rd Generation Partnership Project (3GPP), Apr. 2016. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36331.htm
[107] Y. Ming, "Analysis of physical-layer security in future mobile communication," in *Proc. Int. Conf. Mech. Sci., Electr. Eng. Comput. (MEC)*, Dec. 2013, pp. 3144–3147.
[108] R. P. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," in *Proc. 16th Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Jun. 2013, pp. 1–9.
[109] S. Anand, S. Sengupta, K. Hong, K. P. Subbalakshmi, R. Chandramouli, and H. Cam, "Exploiting channel fragmentation and aggregation/bonding to create security vulnerabilities," *IEEE Trans. Veh. Technol.*, vol. 63, no. 8, pp. 3867–3874, Oct. 2014.
[110] F. M. Aziz, J. S. Shamma, and G. L. Stüber, "Resilience of LTE networks against smart jamming attacks," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 734–739.
[111] M. J. La Pan, M. Lichtman, T. C. Clancy, and R. W. McGwier, "Protecting physical layer synchronization: Mitigating attacks against OFDM acquisition," in *Proc. 16th Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Jun. 2013, pp. 1–6.
[112] K. Pelechrinis, M. Iliofotou, and S. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, 2nd Quart., 2011.
[113] R. Akila, C. Chellaswamy, and T. J. Jeyaprabha, "An efficient jamming attack revocation in wireless network," in *Proc. Int. Conf. Adv. Commun. Control Comput. Technol. (ICACCCT)*, May 2014, pp. 784–789.
[114] M. Labib, V. Marojevic, J. H. Reed, and A. I. Zaghloul, "How to enhance the immunity of LTE systems against RF spoofing," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2016, pp. 1–5.
[115] M. Labib, V. Marojevic, and J. H. Reed, "Analyzing and enhancing the resilience of LTE/LTE-A systems to RF spoofing," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2015, pp. 315–320.
[116] D. Gesbert, S. Hanly, H. Huang, S. S. Shitz, O. Simeone, and W. Yu, "Multi-cell MIMO cooperative networks: A new look at interference," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 9, pp. 1380–1408, Dec. 2010.
[117] B. Makki and T. Eriksson, "On hybrid ARQ and quantized CSI feedback schemes in quasi-static fading channels," *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 986–997, Apr. 2012.
[118] W. Nam, D. Bai, J. Lee, and I. Kang, "Advanced interference management for 5G cellular networks," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 52–60, May 2014.

[119] R. Q. Hu and Y. Qian, "An energy efficient and spectrum efficient wireless heterogeneous network framework for 5G systems," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 94–101, May 2014.

[120] C. Papathanasiou, N. Dimitriou, and L. Tassiulas, "Dynamic radio resource and interference management for MIMO–OFDMA mobile broadband wireless access systems," *Comput. Netw.*, vol. 57, no. 1, pp. 3–16, Jan. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128612002824

[121] T. O. Olwal, K. Djouani, and A. M. Kurien, "A survey of resource management towards 5G radio access networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1656–1686, Apr. 2016.

[122] D. Inoue, R. Nomura, and M. Kuroda, "Transient MAC address scheme for untraceability and DoS attack resiliency on wireless network," in *Proc. Wireless Telecommun. Symp.*, Apr. 2005, pp. 15–23.

[123] E. Palomar, J. M. E. Tapiador, J. C. Hernandez-Castro, and A. Ribagorda, "Dealing with sporadic strangers, or the (un)suitability of trust for mobile P2P security," in *Proc. IEEE DEXA*, Sep. 2007, pp. 779–783.

[124] A. Eshmawi and S. Nair, "Smartphone applications security: Survey of new vectors and solutions," in *Proc. ACS Int. Conf. Comput. Syst. Appl. (AICCSA)*, May 2013, pp. 1–4.

[125] P. Traynor *et al.*, "On cellular botnets: Measuring the impact of malicious devices on a cellular network core," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2009, pp. 223–234. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653690

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

[127] C.-M. Huang and J.-W. Li, "Authentication and key agreement protocol for UMTS with low bandwidth consumption," in *Proc. 19th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, vol. 1. Mar. 2005, pp. 392–397.

[128] D. Caragata, S. E. Assad, I. Tutanescu, C. A. Shoniregun, and G. Akmayeva, "Security of mobile Internet access with UMTS/HSDPA/LTE," in *Proc. World Congr. Internet Secur. (WorldCIS)*, Feb. 2011, pp. 272–276.

[129] S. Kanchi, S. Sandilya, D. Bhosale, A. Pitkar, and M. Gondhalekar, "Overview of LTE-A technology," in *Proc. IEEE Global High Tech Congr. Electron. (GHTCE)*, Nov. 2013, pp. 195–200.

[130] 3GPP, *General Packet Radio Service (GPRS); Service Description Release 8*, document TS 23.060, 3rd Generation Partnership Project (3GPP), Apr. 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/23060.htm

[131] 3GPP, *Network Architecture*, document TS 23.002, 3rd Generation Partnership Project (3GPP), Sep. 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/23002.htm

[132] 3GPP, *UTRAN Iu Interface Radio Access Network Application Part (RANAP) Signalling*, document TS 25.413, 3rd Generation Partnership Project (3GPP), Sep. 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/25413.htm

[133] E. R. S. Jose and F. J. Velez, "Enhanced UMTS services and applications: A perspective beyond 3G," in *Proc. 5th Eur. Pers. Mobile Commun. Conf.*, Apr. 2003, pp. 146–150.

[134] A. Merlo, M. Migliardi, N. Gobbo, F. Palmieri, and A. Castiglione, "A denial of service attack to UMTS networks using SIM-less devices," *IEEE Trans. Dependable Secure Comput.*, vol. 11, no. 3, pp. 280–291, May 2014.

[135] G. Carneiro, J. Ruela, and M. Ricardo, "Cross-layer design in 4G wireless terminals," *Wireless Commun.*, vol. 11, no. 2, pp. 7–13, Apr. 2004. [Online]. Available: http://dx.doi.org/10.1109/MWC.2004.1295732

[136] P. Rysavy, "Transition to 4G 3GPP broadband evolution to IMT-advanced (4G)," Rysavy Res. LLC, Hood River, OR, USA: Tech. Rep., 2010.

[137] S. Sudin, A. Tretiakov, R. H. R. M. Ali, and M. E. Rusli, "Attacks on mobile networks: An overview of new security challenge," in *Proc. Int. Conf. Electron. Design (ICED)*, Dec. 2008, pp. 1–6.

[138] K. Osathanunkul and N. Zhang, "A countermeasure to black hole attacks in mobile ad hoc networks," in *Proc. IEEE Int. Conf. Netw., Sens. Control (ICNSC)*, Apr. 2011, pp. 508–513.

[139] F. Xing and W. Wang, "Understanding dynamic denial of service attacks in mobile ad hoc networks," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Oct. 2006, pp. 1–7.

[140] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Commun.*, vol. 14, no. 5, pp. 85–91, Oct. 2007.

[141] M. Zeshan, S. A. Khan, A. R. Cheema, and A. Ahmed, "Adding security against packet dropping attack in mobile ad hoc networks," in *Proc. Int. Seminar Future Inf. Technol. Manage. Eng. (FITME)*, Nov. 2008, pp. 568–572.

[142] V. K. Raju and K. V. Kumar, "A simple and efficient mechanism to detect and avoid wormhole attacks in mobile ad hoc networks," in *Proc. Int. Conf. Comput. Sci. (ICCS)*, Sep. 2012, pp. 271–275.

[143] M. Wazid, V. Kumar, and R. H. Goudar, "Comparative performance analysis of routing protocols in mobile ad hoc networks under Jelly-Fish attack," in *Proc. 2nd IEEE Int. Conf. Parallel Distrib. Grid Comput. (PDGC)*, Dec. 2012, pp. 147–152.

[144] K. Das and A. Taggu, "A comprehensive analysis of DoS attacks in Mobile Adhoc Networks," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2014, pp. 2273–2278.

[145] A. Gupta and R. K. Jha, "Security threats of wireless networks: A survey," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, May 2015, pp. 389–395.

[146] X. Su and R. V. Boppana, "Mitigating wormhole attacks using passive monitoring in mobile ad hoc networks," in *Proc. IEEE Global Telecommun. Conf.*, Nov./Dec. 2008, pp. 1–5.

[147] P. Sharma and A. Suryawanshi, "Enhanced security scheme against jamming attack in mobile ad hoc network," in *Proc. Int. Conf. Adv. Eng. Technol. Res. (ICAETR)*, Aug. 2014, pp. 1–5.

[148] M. Adeel, L. N. Tokarchuk, M. A. Azam, S. K. A. Khan, and M. A. Khalil, "Propagation analysis of malware families in mobile P2P networks," in *Proc. 11th Int. Conf. Inf. Technol., New Generat. (ITNG)*, Apr. 2014, pp. 220–226.

[149] V. N. Cooper, H. Shahriar, and H. M. Haddad, "A survey of Android malware characterisitics and mitigation techniques," in *Proc. 11th Int. Conf. Inf. Technol., New Generat. (ITNG)*, Apr. 2014, pp. 327–332.

[150] F. Ricciato, A. Coluccia, and A. D'Alconzo, "A review of DoS attack models for 3G cellular networks from a system-design perspective," *Comput. Commun.*, vol. 33, no. 5, pp. 551–558, Mar. 2010. . [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366409003168

SILVÈRE MAVOUNGOU received the bachelor's and master's degrees in electronic and communication systems from the Université de Bretagne Occidentale, Brest, France, in 2007. He is currently pursuing the M.Eng. degree in telecommunications networks with the École de Technologie Supérieure de Montréal. Since 2007, he has worked as a Consultant for several companies in mobile communication, rail signalling, and embedded systems sectors.

GEORGES KADDOUM received the bachelor's degree in electrical engineering from the École Nationale Supérieure de Techniques Avancées (Bretagne), Brest, France, the M.S. degree in telecommunications and signal processing (circuits, systems, and signal processing) from the Université de Bretagne Occidentale and Telecom Bretagne, Brest, in 2005, and the Ph.D. degree (Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences, University of Toulouse, Toulouse, France, in 2009. Since 2013, he has been an Assistant Professor of Electrical Engineering with the École de Technologie Supérieure (ETS), University of Québec, Montréal, QC, Canada. In 2014, he was the ETS Research Chair in physical-layer security for wireless networks. Since 2010, he has been a Scientific Consultant in the field of space and wireless telecommunications for several companies (Intelcan Techno-Systems, MDA Corporation, and Radio-IP companies). He has published over 100 journal and conference papers and has two pending patents. His recent research activities cover mobile communication systems, modulations, secure transmissions, and space communications and navigation. He received the best paper award at the 2014 IEEE International Conference on Wireless and Mobile Computing, Networking, and Communications, with three co-authors, and the 2015 IEEE Transactions on Communications Top Reviewer Award. He is serving as an Editor of the IEEE Communications Letters.

MOSTAFA TAHA (M'–) is an Assistant Professor with the Electrical Engineering Department, Assiut University, and a Post-Doctoral Fellow with Western University, Canada. He received the Ph.D. degree in computer engineering from Virginia Tech in 2014. He was a Post-Doctoral Associate with the Vernam Crypto Group, WPI, from 2014 to 2015. His research interests include hardware security and implementation attacks. He served as an Academic Reviewer for several conferences, including CHES, COSADE, CARDIS, and HOST, and several journals, including the IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN, the IEEE TRANSACTIONS ON COMPUTERS, the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION, and the *IACR Journal of Cryptographic Engineering*. He is a member of IACR.

GEORGES MATAR received the bachelor's and M.Sc. degrees in biomedical engineering from the Holy Spirit University of Kaslik, Kaslik, Lebanon, in 2014. He is currently pursuing the Ph.D. degree in signal processing and biomedical instrumentation with the Biomedical Information Processing Laboratory, École de Technologie Supérieure, University of Quebec, Montreal, QC, Canada. His research interest covers technologies and models for next generation health wireless networks, with a particular focus on the Internet of Things for remote medical monitoring and sleep quality assessment.