He, Limei; Yan, Zheng; Atiquzzaman, Mohammed

LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2018.2792534

Published: 11/01/2018

Document Version
Publisher's PDF, also known as Version of record

Received November 22, 2017, accepted January 2, 2018, date of publication January 12, 2018, date of current version February 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2792534

LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement: A Survey

LIMEI HE[1], ZHENG YAN[1], (Senior Member, IEEE), AND MOHAMMED ATIQUZZAMAN[2], (Senior Member, IEEE)

[1]State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710126, China
[2]School of Computer Science, The University of Oklahoma, Norman, OK 73019, USA

Corresponding author: Zheng Yan (zheng.yan@aalto.fi)

This work was supported in part by the National Key Research and Development Program of China under Grant 2016YFB0800704, in part by NSFC under Grant 61672410 and Grant U1536202, in part by the Project through the Natural Science Basic Research Plan in Shaanxi Province of China under Program2016ZDJC-06, in part by the 111 Project under Grant B08038 and Grant B16037, and in part by the Academy of Finland under Grant 308087.

ABSTRACT The long-term evolution (LTE)/LTE-advanced (LTE-A) network provides advanced services for billions of users with its higher bandwidths, better spectrum efficiency, and lower latency than legacy cellular networks. But it still suffers from new security threats due to its all IP-based heterogeneous architecture. Therefore, there is a critical need to perform a rapid and accurate network security measurement in the LTE/LTE-A network. To achieve LTE/LTE-A network security measurement, security-relevant data (in short security data) collection and data analysis for attack detection are required as prerequisites. However, most of the existing work only focuses on data collection and analysis for a certain type of LTE/LTE-A attacks. Little work has been done to comprehensively perform data collection and analysis for detecting various attacks on the LTE/LTE-A network. Different from previous work, in this paper, we review the security data collection and data analysis methods in terms of various attacks in order to provide the basis of security measurement in the LTE/LTE-A network. We first present a comprehensive taxonomy of attacks according to the LTE/LTE-A network structure. Then, we propose a number of criteria for evaluating the performance of data collection and analysis methods. And we lay our emphasis on the survey of data collection and analysis methods for significant active attack detection in the LTE/LTE-A network. All the reviewed methods are analyzed and discussed based on the proposed evaluation criteria. Furthermore, current open issues and future research challenges are presented with a view to stimulating future research. Finally, an adaptive data collection and data analysis model for security measurement in the LTE/LTE-A network is proposed.

INDEX TERMS Attack detection, data analysis, data collection, LTE/LTE-A network, security measurement.

I. INTRODUCTION

The 3rd Generation Partnership Project (3GPP) announced the 3GPP R8 version as the main technical standard for The Long Term Evolution (LTE) in 2008, which offers higher bandwidths, better spectrum efficiency, and lower latency than legacy cellular networks. Consequently, LTE network is widely deployed by mobile operators around the world. The R10 version of 3GPP brought the LTE-Advanced (LTE-A) network that extends LTE, and introduced new technologies to improve system performance. The standard version has now been updated to R14, and 3GPP has started discussion and study of 5G technologies.

The overall architecture of LTE/LTE-A has two distinct components: Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) and Evolved Packet Core (EPC). The new unique features of LTE/LTE-A network like flat IP connectivity and full interworking with heterogeneous access networks pose some new threats to itself. A few surveys of LTE/LTE-A security threats have already been published [1]–[4], and they analyzed LTE/LTE-A security threats from different aspects. A comprehensive analysis of LTE/LTE-A network security was reported in [1] where the vulnerabilities were analyzed from six aspects containing system architecture, access procedure, handover

procedure, IP Multimedia Subsystem (IMS) security, Home eNodeB (HeNB) security and Machine Type Communication security. Park and Park summarized the weaknesses in 3GPP Authentication and Key Agreement (AKA) [2], and indicated some malicious attacks that could take place, such as viruses, worms, and Voice over LTE (VoLTE) threats. Seddigh *et al*. [3] summarized security threats in different layers. They stated that LTE/LTE-A may suffer from interference and scrambling attacks at the physical layer. It also analyzed the attacks at Media Access Control (MAC) layer including location tracking attacks, bandwidth stealing attacks, Denial of Service (DoS) attacks and other security issues. In addition, security issues at higher layers were also summarized in this survey. Bikos and Sklavos [4] discussed LTE/LTE-A security issues from aspects of ciphering algorithms and integrity methods. They reviewed the current encryption and authentication techniques and pointed out the vulnerabilities of LTE/LTE-A security algorithms and procedures.

However, the above studies only analyzed the security threats and possible attacks in certain security aspects in LTE/LTE-A networks. A comprehensive and organized summary of attacks on LTE/LTE-A network is lacking. In this paper, we tease out almost all possible attacks on LTE/LTE-A networks according to its network structure.

The LTE/LTE-A network is increasingly vulnerable to various security threats, giving rise to a critical need to perform comprehensive network security measurements, which takes into consideration various security attacks and threats, as well as their detection and analysis methods. Security measurement is a real-time process that can detect existing attacks on network and evaluate the degree of network security. Efficient related data collection and data analysis can ensure the rapid and accurate detection of security attacks and provide the basis for network security measurement. We use the term ''data collection'' to refer to the procedure that captures security-relevant information in network devices. In our context, we review the original data and obtained features in data collection methods. We use the term ''data analysis'' to refer to the procedure that analyzes the collected data to achieve attack detection. In our context, we review the data analysis algorithms and strategies in existing literature.

Most of existing work focuses on data collection and analysis for a certain type of LTE/LTE-A attacks (e.g., RF jamming attacks [39]–[41], signaling attacks [20], [43], [44], abnormal SIP attacks [45], [46], and so on), little work has been done in terms of comprehensive data collection and analysis for security measurement in LTE/LTE-A. To the best of our knowledge, this is one of the first papers that provide a comprehensive summary of attacks on the LTE/LTE-A network and give a thorough survey on security data collection and data analysis methods for LTE/LTE-A attack detection. We first make an overview of the LTE/LTE-A network followed by a summary of almost all the significant attacks on LTE/LTE-A networks. We also provide an extensive review of data collection and analysis methods that are utilized to detect different attacks. We emphasize on existing data collection and analysis methods in the recent literature and conclude with a number of evaluation criteria proposed by us. We point out some open issues to highlight future research directions. Finally, we present a data collection and data analysis model for security measurement in the LTE/LTE-A network. The main contributions of this paper are:

- A comprehensive taxonomy of security attacks according to the LTE/LTE-A network;
- A description of evaluation criteria for evaluating and commenting the performance of data collection and analysis methods in terms of attack detection in the LTE/LTE-A network;
- A survey of data collection and data analysis methods for detecting significant active attacks on LTE/LTE-A network. The collected data, data analysis algorithms and strategies of the reviewed works are summarized. In addition, the advantages and disadvantages of existing methods are analyzed based on our evaluation criteria;
- An investigation of open issues and future research directions;
- A data collection and data analysis model for LTE/LTE-A security measurement.

The remaining of the paper is organized as follows. Section 2 briefly overviews the LTE/LTE-A network architecture. A classification of the main attacks according to its network structure is given in Section 3. In Section 4, we propose a number of evaluation criteria for commenting and comparing data collection and analysis methods, followed by a thorough review on existing methods in the literature. Furthermore, Section 5 highlights current open research issues and indicates future research directions. An adaptive data collection and analysis model for security measurement is proposed in Section 6. Finally, a conclusion is presented in the last section. For easy reference, Table 2 in appendix lists the abbreviations that are used in this paper.

II. LTE/LTE-A OVERVIEW

In this section, we make an overview of LTE/LTE-A network architecture and its security mechanism. This section provides basic knowledge for understanding the attacks on LTE/LTE-A networks as summarized in Section 3.

A. LTE/LTE-A NETWORK ARCHITECTURE

The LTE/LTE-A network architecture is shown in Fig. 1 [5], [6]. It is composed of a radio access network and a core network. The radio access network is called E-UTRAN, which evolved from the original 3GPP UMTS Terrestrial Radio Access Network (UTRAN). UMTS is the abbreviation of Universal Mobile Telecommunication System. The E-UTRAN is composed of multiple evolved-NodeBs (e-NodeBs), which have the functionality of the NodeBs and assume most of the functions of Radio Network Controller in UTRAN. The User Equipment (UE) and the e-NodeB are connected through the air interface

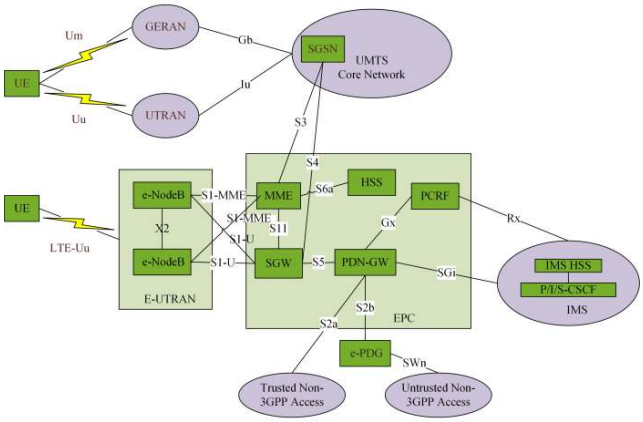

FIGURE 1. LTE/LTE-A network architecture.

(Uu interface). The e-NodeB connects to each other by X2 interface and mainly implements the functions as follows: radio resource management, IP header compression and encryption for user data, connection to the Mobility Management Entity (MME) by S1-MME interface (to achieve mobility management, paging users, and passing None Access Stratum (NAS) signaling, etc.), and connection to the Serving Gateway (SGW) by the S1-U interface. In addition, LTE-A also supports HeNBs and Relay Node (RN), and when a large number of HeNBs are deployed, Home Base Station Gateway should be deployed.

LTE/LTE-A core network is called EPC network. It provides connections to multiple heterogeneous access networks, containing 3GPP access networks (E-UTRAN, GERAN and UTRAN), and non-3GPP access networks (WiMAX, CDMA2000, etc.).The EPC consists of MME, Home Subscriber Server (HSS), SGW, Packet Data Network Gateway (PDN-GW) and Policy and Charging Rules Function (PCRF). The EPC achieves the separation of the control surface and the user surface. The MME achieves control surface functions and the SGW achieves user surface functions. The MME hosts the following functions: NAS signaling, NAS signaling security, Access Stratum (AS) security control, idle state mobility handling, bearer control, etc., while HSS provides services for LTE/LTE-A core network and IMS network as a central data base. The MME connects to the HSS through the S6a interface in order to transfer authentication data. The main functions of the SGW are to route and forward. The PDN-GW is mainly for UE's IP address allocation, packet filtering and legitimate monitoring. PCRF is mainly to perform flow based charging and network control regarding service data flow detection to guarantee Quality of Service (QoS). Trusted and Distrusted non-3GPP Access Networks are IP access networks whose specifications are out of the scope of 3GPP. The functionality of evolved-Packet Data Gateway (e-PDG) includes allocation and transportation of a remote IP address, local mobility anchor within distrusted non-3GPP access networks, tunnel authentication and authorization, etc.

In the LTE/LTE-A network, IMS network is used to handle Packet-Switched services like VoLTE. In addition, GSM and UMTS networks support Circuit Switched Fallback procedures (CSFB). It can be triggered when IMS is not employed. IMS is a powerful framework deployed by the LTE/LTE-A network to provide various types of multimedia services such as VoLTE, Short Messaging Service (SMS), streaming video, etc.

IMS is composed of user plane, control plane, and application plane. The user plane is a Session Initiation Protocol (SIP) application that is inserted into devices. The main function of the control plane is session control. The control plane includes Call Session Control Function (CSCF) and HSS. The CSCF can be further divided into Proxy-Call Session Control Functions (P-CSCF), Interrogating-Call Session Control Functions (I-CSCF) and Serving-Call Session Control Functions (S-CSCF). Each of them has a visible IP address in Domain Name Service (DNS). P-CSCF is the first connected point when a user connects to the IMS network, it forwards the SIP register requests and the SIP messages to th e SIP server. I-CSCF assigns an S-CSCF to every user performing SIP registration and routes incoming requests towards the assigned S-CSCF. The S-CSCF performs the session control services, like SIP registration and incoming service requests. HSS holds the information of IMS users and performs user authentication in user registration process. The application plane is comprised of application servers which can provide various services like VoLTE, SMS, etc. The signaling data transmission in IMS is based on SIP and the packet data is mainly transmitted based on Real-time Transport Protocol (RTP). The SIP layer is of great importance in IMS, controlling various multimedia services. But it has several vulnerabilities due to its text-based property, thus the IMS system could suffer from SIP-related attacks.

B. LTE/LTE-A NETWORK SECURITY

In this section, we first give a brief overview of LTE/LTE-A network security architecture, and then we introduce LTE/LTE-A security key hierarchy, LTE/LTE-A handover key management, and IMS security.

1) LTE/LTE-A NETWORK SECURITY ARCHITECTURE

The content of this part mainly refers to the specification of 3GPP [7]. As shown in Fig. 2, five security levels are defined by 3GPP to confront certain threats and achieve certain security requirements, the details of their features are introduced as below:

- Network Access Security (I): It provides secure access to services for users and protects the radio access link against attacks.
- Network Domain Security (II): It provides a safe way to transmit signaling data and user data.
- User Domain Security (III): It provides secure access to mobile stations including mutual authentication between Universal Subscriber Identity Module (USIM) and UE.

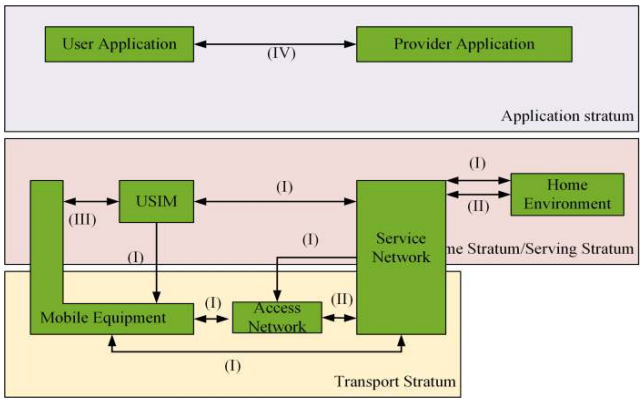

FIGURE 2. LTE/LTE-A network security architecture.

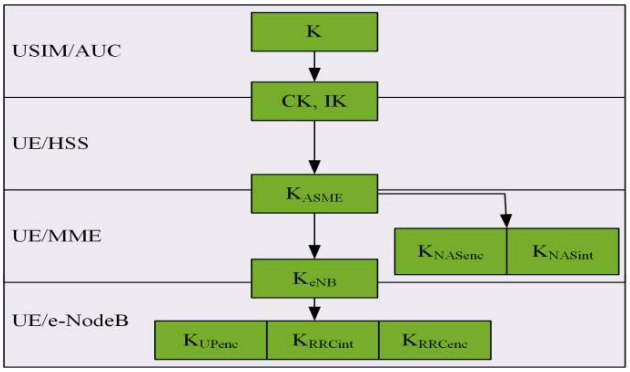

FIGURE 3. LTE/LTE-A key hierarchy.

- Application Domain Security (IV): It ensures the secure message exchange of applications in both the user domain and the provider domain.
- Visibility and Configurability of Security (V): They enable a user to inform himself/herself whether a security feature is in operation or not and whether the use and provision of services should depends on the security features.

2) LTE/LTE-A SECURITY KEY HIERARCHY

The LTE/LTE-A network uses the Key Derivation Function to derive a variety of keys. The hierarchy is depicted in Fig. 3 as follows:

- K is a permanent master key that is securely stored in both USIM and Authentication Centre (AuC).
- CK and IK are ciphering keys and integrity keys derived in USIM and AuC from K for encryption and integrity check, respectively.
- K_{ASME} is derived from CK and IK, and it is shared between UE and MME to generate a series of session keys.
- K_{eNB} is derived in UE and MME or a target e-NodeB from K_{ASME} in according with the state of UE.
- K_{NASint} and K_{NASenc} is a pair of keys derived by the UE and MME from K_{ASME} to protect NAS traffic.
- K_{UPenc} is derived in UE and e-NodeB from K_{eNB} to protect user plane traffic.
- K_{RRCint} and K_{RRCenc} is a pair of keys derived in UE and e-NodeB from K_{eNB} to protect Radio Resource Control (RRC) traffic.

3) LTE/LTE-A HANDOVER KEY MANAGEMENT

The LTE/LTE-A network supports both inter Radio Access Technology handover and intra E-UTRAN handover. The intra E-UTRAN handover contains intra-MME handover and inter-MME handover. The intra-MME handover occurs between two e-NodeBs in the same MME that is connected with each other using the X2 interface, while the inter-MME handover is based on the S1 interface and involves the MME in the process. The inter-MME handover procedure always runs the complete EPS (Evolved Packet System)-AKA procedure to achieve a secure environment, while the intra-MME handover just simply handovers a new K_{eNB} (K^*_{eNB}) from a source e-NodeB to a target e-NodeB. The backward key separation of the session key derivation in intra-MME handover is achieved using a one-way hash function, which means the e-NodeB cannot derive past session keys from the current keys. At the same time, forward key separation is also needed to ensure that the source e-NodeB cannot predict the key of the target e-NodeB. This is achieved by using Next Hop (NH) key and the NH Chaining Counter (NCC) to generate new keys.

K^*_{eNB} can be derived using horizontal key derivation or vertical key derivations. The former procedure derives K^*_{eNB} from the previous K_{eNB} and it happens when the source eNodeB does not have a fresh (NH, NCC) pair or the NCC value in source eNodeB is not less than that received from MME. The latter procedure is more common and secure, and it derives K^*_{eNB} using NH key received from the MME. It is used when the NCC value in the source eNodeB is less than the NCC value received from MME.

4) IMS SECURITY

Both EPS-AKA and IMS-AKA authentication should be performed before UE getting access to multimedia services. In IMS, a new IMS Subscriber Identity Module (ISIM) is allocated in each UE. Similar to the USIM, which is used to connect to the LTE/LTE-A network, the ISIM stores the IMS-authentication keys and functions. The S-CSCF processes UE requests to perform authentication using the HSS, which holds the copy of IMS-authentication keys.

III. TAXONOMY OF ATTACKS ON LTE/LTE-A

The LTE/LTE-A network is deployed by mobile operators around the world with excellent performance. But the new features of its architecture like flat IP connectivity and full interworking with heterogeneous wireless access networks bring new threats to the LTE/LTE-A network. In this section, we summarize the LTE/LTE-A attacks that were proposed in recent decade years, the reviewed work is searched in four database including IEEE Explorer digital library, ACM digital library, Springer digital library, and ScienceDirect based on keywords: (attack or detection or security) and LTE.

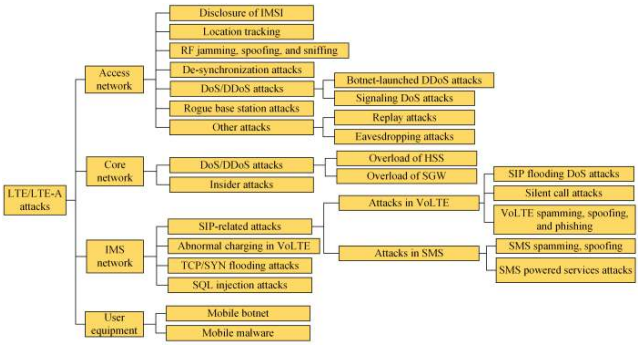

FIGURE 4. Taxonomy of LTE/LTE-A attacks.

We classify the LTE/LTE-A attacks according to its network framework and provide a summary of the main LTE/LTE-A attacks in each group. Fig. 4 describes the taxonomy of LTE/LTE-A attacks according to the network structure.

A. ATTACKS ON ACCESS NETWORK

In this subsection, we primarily summarize the significant attacks on LTE/LTE-A access network.

1) DISCLOSURE OF THE INTERNATIONAL MOBILE SUBSCRIBER IDENTITY (IMSI)

IMSI is a permanent identifier of a subscriber. It should be transmitted as infrequently as possible for the sake of confidentiality of user identity. LTE/LTE-A specifications minimize the IMSI transmission frequency over the air interface. In the radio transmission, a Globally Unique Temporary Identifier (GUTI) is used to identify subscribers. Disclosure of the IMSI can result in the leakage of subscriber information, location information, and even conversation information. Attackers can disguise a real UE of normal subscriber and launch attacks like DoS attacks [1]. IMSI disclosure attacks can be launched by abusing a false base station and an AKA protocol. Here are a few attacks that can obtain the IMSI, as proposed in the literatures. Rao *et al*. [8] proposed an IMSI retrieval method that misused the SMS protocol. An attacker with an interconnection access who knows the Mobile Station International Subscriber Directory Number (MSISDN) and Diameter Routing Agents/Diameter Edge Agents address can identify a subscriber's IMSI.

Holtmanns *et al*. [9] described a procedure to obtain IMSI based on the knowledge of MSISDN in a Diameter-based network. An attacker can impersonate as a partner Short Message Service Center or Interworking Function (IWF) (for two IWFs scenarios) in a querying network and send a request containing the MSISDN to the targeted victim's network. After a series of signaling procedure, the attacker can receive a response message that includes the desired information such as the targeted victim's IMSI, serving node address and possibly the address of the HSS.

In addition, IMSI Catchers were also used in mobile networks to identify and eavesdrop on phones [10]. Shaik *et al*. [11] indicated that the IMSI can be extracted by sniffing the LTE/LTE-A air interface.

2) LOCATION TRACKING

Undoubtedly, the location data of mobile phone users are considered as private personal information. The design of mobile communication technologies allows the mobile operators to know the physical locations of the users to perform continuous cellular services. In addition, the advance of recent positioning technologies and location-based services also pose a threat to user location confidentiality.

Rao *et al.* [8] described some location disclosure attacks using Insert-Subscriber-Data-Request (IDR) and User-Data-Request (UDR). In the former attack, an attacker can impersonate the partner HSS and send the IDR that is used by the HSS to request the EPS location information of a UE to MME, MME returns the EPS location information that contains Cell-Global-Identity, Location-Area-Identity, and Service-Area-Identity after receiving the IDR. In the latter attack, an attacker can impersonate the IMS application server and send a UDR message to the HSS. In most cases, the answer contains the Location Area ID and Cell ID, so the attackers can identify where the subscriber is currently located or where it was previously located.

Holtmanns *et al*. [9] gave detailed explanation of several user location tracking methods that translate existing SS7 attacks into Diameter-based attacks in the LTE/LTE-A network. The core idea is that an attacker pretends to be a legacy SS7 network or a network node. Hence, the more secure LTE/LTE-A Diameter networks are forced to use less secure SS7 protocols for interoperability reasons. The location tracking attack using SMS protocol messages is of the same set of steps of the IMSI disclosure attack as mentioned above, and the serving node information can provide a coarse-grained estimation of a victim's location.

Shaik *et al*. [11], tracked down the location of a user to a cell level and localized a target user within about a 2km2 area using passive attacks and semi-passive attacks. They further determined the precise position of the user using active attacks. In the passive attacks, an attacker needs to get the IMSI or GUTI of a victim to decide whether the target user is in that area. The semi-passive attack generates signaling messages using VoLTE calls and monitors any single cell within a Tracking Area (TA) for paging messages, then reveals the mapping between the GUTI and the victims' phone number. Once the mapping is successful, it can be confirmed that the target user is in that TA. It can even be determined that which particular cell within the TA that the target user is located using social network applications. In active attacks, an attacker can abuse the vulnerabilities in the RRC protocol to track the victims in a more fine-grained way. The attacker forces victims to send Measurement Report (MR) or Radio Link Failure (RLF) report messages to a rogue e-NodeB. Both MR and RLF reports provide signal strengths, maybe even GPS coordinates of victims, so the attacker can calculate the distance between the UE and the rogue e-NodeB using

a trilateration technique or directly determine the accurate location of the victims using GPS coordinates.

Additionally, location tracking attacks could possibly be launched based on the cell radio network temporary identifier, packet sequence numbers [12], and emergency location service messages.

3) RADIO FREQUENCY (RF) JAMMING, SPOOFING, AND SNIFFING

Wireless networks are vulnerable to jamming-style attacks because of their shared medium. Like other wireless systems, the LTE/LTE-A network can also suffer from RF jamming, spoofing, and sniffing, all of which are common physical-layer attacks.

RF jamming targets receivers and disrupts communications by decreasing the Signal-to-Noise Ratio (SNR) of the received signal to cause DoS attacks. For a smart jammer, 3GPP specifications declare the required frequency and timing information for specific critical channels, so they can launch jamming attacks toward control channels instead of the entire network bandwidth in an efficient way. RF spoofing refers to transmitting a fake signal meant to masquerade as an actual signal. RF sniffing gives the adversary useful information to efficiently launch attacks. Herein, we just give a brief introduction to several effective attacks [13]–[15].

Jamming the synchronization signals (containing Primary Synchronization Signal (PSS) and the Secondary Synchronization Signal (SSS)) prevents the UE from selecting the cell. A more efficient method for denying cell selection is RF spoofing by transmitting a fake signal. In [16], PSS and SSS were created and periodically transmitted on the LTE/LTE-A carrier frequency by fake e-NodeB, and the experiment showed that the UE cannot camp on a legal e-NodeB.

Jamming the Physical Broadcast Channel (PBCH) is an efficient synchronous jamming attack, which only requires jamming about 10 percent of the downlink subcarriers with a 3 percent duty cycle. A more simply attack is PBCH sniffing that can give the adversary information useful to launch more efficient attacks.

The Physical Control Format Indicator Channel (PCFICH) is an extremely sparse channel, making it vulnerable to efficient jamming. This channel carries all essential control information for UE to be able to decode the Physical Downlink Control Channel.

Physical Uplink Control Channel (PUCCH) is located on the edges of the system bandwidth in a static location, that makes jamming PUCCH easy to be launched. PUCCH jamming attack has an impact on the entire cell by corrupting the control information sent on the PUCCH, and is feasible when the jammer knows the LTE/LTE-A system bandwidth and center frequency. PUCCH jamming is a serious threat since it is easy for an adversary to know the PUCCH's spectrum allocation and has high efficiency in disrupting the uplink channel.

Jamming the Physical Random Access Channel (PRACH) prevents new UEs from accessing a base station. The UE initiates a random access procedure by transmitting a random access preamble on the PRACH, the UE lets the e-NodeB know of its presence and that it wants to connect to the cell. The location of the PRACH is conveyed to the UE in the SIB2 message, which is carried over the Physical Downlink Control Channel. Therefore, the jammer only needs to decode the SIB2 message fields.

Jamming the common control channels can prevent UEs in the cell shifting to RRC Connected state or prevent incoming UEs from transitioning to the cell, this can lead to effective DoS attacks.

4) DOS/DDOS ATTACKS

DoS and Distributed Denial of Service (DDoS) attacks are both severe attacks on LTE/LTE-A network. A common method of DoS attacks is that attackers send floods of messages to a target server and exhaust its CPU resources, making the target unable to provide services for legitimate users. In addition to this type of DoS attacks, other DoS attacks always misuse the loophole in the LTE/LTE-A network protocol. In the DDoS attacks, attackers can generate heavy traffic volume using botnet managed by Command and Control Centers (C&C) or hacked mobile UE. An attacker can abuse the security loopholes of the operating system and applications downloaded from app stores to compromise mobile devices [17].

DoS attacks have one single attacker, and the traffic maliciously generated is of low volume. DDoS attacks have high traffic volume, and they can be launched by a large number of multiple devices that are well synchronized [18].

In addition to jamming-style attacks, a variety of other methods can lead to DoS/DDoS attacks in the access layer.

a: SIGNALING DoS ATTACKS

The radio resources in the LTE/LTE-A network should be managed in an efficient manner because the radio resources are limited and insufficient to provide services for all subscribers at the same time. In addition, the maintaining of the RRC connected state can harm the battery life of a mobile device. The RRC layer in the LTE/LTE-A air interface performs the radio resources reassignment. It sets up the radio bearer between the mobile device and the core network when a user triggers a signaling procedure called random access in 4G LTE/LTE-A to transfer data. Then the resources are released and reassigned to another UE. A number of control messages are generated in the process of bearer setup and release. The transmission of these control messages among different LTE/LTE-A network entities including UE, e-NodeB, MME, SGW, and PDN-GW can give rise to network congestion and compromise the network services. The fact that each UE has the ability to initiate up to eight dedicated bearers aggravates the signaling overhead [19]. These provide the probability of a DoS attack.

Bassil *et al*. [20] argued that if a group of well-coordinated malicious users require to set up and release a bearer repeatedly, network resources will be strained and network services

can be degraded and even DoS could happen. In fact, a botnet of infected mobile devices could be used by attackers to synchronize the behaviors of a group of malicious users.

b: BOTNET-LAUNCHED DDoS ATTACKS

Khosroshahy *et al*. [21] argued that botnet in 4G cellular networks can be used as platforms to launch DDoS attacks against the air interface. The core idea of this proposed attack scenario is botmasters activate all botnet nodes at the same time and let them start downloading a large file or send dummy data to create congestion on the downlink or the uplink. The simulations indicated that an outage in cellular services can occur when a botnet spreads to only 6% of subscribers and the 4G/LTE/LTE-A network seems to be much more vulnerable to botnet-launched DDoS attacks.

Here we need to stress that the two kinds of DoS/DDoS attacks mentioned above also have impact on the core network [22], and the core network may suffer more than the access network.

5) DE-SYNCHRONIZATION ATTACKS

Han and Choi [23] proposed a scheme to launch de-synchronization attacks on the intra-MME handover management. An attacker can disrupt the forward key separation using a rogue base station until the update of root key. An attacker can force the UE to perform the horizontal handover key derivation by setting high chaining count value using the rogue e-NodeB or manipulating the S1 path switch ACK message. In this way, the key derivation is void of the forward key separation. Then the attacker can compromise the K_{eNB} in the handover key chaining and launch further active attacks.

6) ROGUE BASE STATION ATTACKS

A rogue base station is a fake base station controlled by an attacker. An attacker can purchase a personal e-NodeB or compromise a commercial base station by several means such as physically penetration, botnet attacks, etc. An attacker can launch many attacks using the rogue base station, like location tracking attacks, DoS attacks, or even Man-In-The-Middle (MITM) attacks. For example, an attacker can send certain ''Tracking Area Update (TAU) Reject'' messages using the rogue e-NodeB to force UE to downgrade to non-LTE/LTE-A network or deny mobile network services. The attacker can also add malicious messages in the attached procedure and make UE deny selected services.

7) OTHER ATTACKS

In addition to the attacks mentioned above, there also exist many other attacks such as replay attacks and eavesdropping attacks. In replay attacks, hackers will tamper with intercepted messages, and send it to UE or MME to gain trust, making a receiver confuse which is the legal one. Eavesdropping is a typical passive attack on wireless network due to its broadcast nature. An attacker can maliciously eavesdrop the wireless channel or directly intercept UE to get useful information. However, the detection of eavesdropping attacks is difficult. The two-way authentication of LTE/LTE-A can effectively defend these attacks but is unable to completely eliminate these attacks.

B. ATTACKS ON CORE NETWORK

In this section, we give the introduction of different attacks on LTE/LTE-A core network.

1) DOS/DDOS ATTACKS

The role of the core network is very important for normal data transmission so the DoS/DDoS attacks aiming at core network elements are serious threats in LTE/LTE-A network.

As mentioned before, mobile botnet can be utilized to launch DDoS attacks on access network, meanwhile, it can also be used to generate flood of attach and detach messages and flood the MME, SGW, and PDN-GW by initiating the attach procedure repeatedly [17]. In addition to this, here we list several other attacks to overload the LTE/LTE-A core network elements.

a: OVERLOAD OF HSS

HSS plays an important role in EPC, and it holds subscriber information in the network such as IMSI, billing and account information, and authentication key. It is also integrated with AuC and generates vectors for authentication. Therefore, the overload of HSS could potentially downgrade the network service performance. The overload of HSS is easy to launch, for example, an attacker can disguise a legitimate UE and send fake IMSIs to HSS constantly. As a result, the HSS needs to generate authentication vectors for the authentication of UE, so the HSS consumes excessive computational resources.

b: OVERLOAD OF SGW

The work in [24] presented several cases that may lead to the overload problems of SGW. Some attack methods are described as follows: (1) an attacked MME may send flood of bearer setup messages to the SGW in a short period of time; (2) a programmable mobile device can frequently trigger the TAU procedures in a short time.

2) INSIDER ATTACKS

Insider attacks are often neglected or assumed unlikely [18]. An insider who has the privileges of accessing to specific network elements can be maliciously persuaded to disrupt the normal communications in the LTE/LTE-A core network. For example, an insider could physically or remotely shut down a network node in the core network. Moreover, the insider can also shut down a base station.

C. ATTACKS ON IMS

The IMS system suffers from various SIP-related attacks due to the fact that the SIP protocol is context-based, and the IMS system is vulnerable to many common attacks on the Internet due to its connectivity to the Internet. This section

summarizes the SIP-related attacks and their extension to IMS services.

1) SIP-RELATED ATTACKS

The most severe threat in IMS is the SIP-related attacks, such as SIP flooding attacks. To launch the SIP flooding attacks, an attacker can transmit a great deal of SIP request messages such as SIP REGISTER messages, SIP INVITE messages with a spoofed source IP address to cause resource exhaustion and result in DoS attacks. The work in [25] concluded these attacks in detail.

Besides, it is easy to get the format of the SIP messages by decoding the SIP messages that are captured by monitoring the IMS-specific interface with a root right in mobile devices. This shortcoming together with the text-based property of SIP protocol enables the attacks like injection of forged SIP messages, malformed SIP messages, or modified SIP messages. For example, an attacker can abuse the BYE request to terminate a victim's session call. To launch this attack, the attacker needs to learn all necessary session parameters (Session-ID, RTP Port, etc.). It worth noticing that plenty of IMS network equipment information is involved in the SIP message header, leaving the information such as the IP address of the registered S-CSCF available to attackers. The vulnerabilities of the SIP protocol can be abused to launch further active attacks on the IMS-based services such as VoLTE and SMS. Herein, we list some significant attacks documented in the literature.

a: ATTACKS ON VoLTE

In the LTE/LTE-A network, the voice service is supported by VoLTE or CSFB techniques. CSFB makes users shift from the LTE/LTE-A network back to the circuit-switched system while VoLTE provides voice call services based on the IMS. Here, we give a brief overview of the most significant attacks of VoLTE:

(i) SIP FLOODING DoS ATTACKS [26]

An attacker can send a large amount of SIP messages to the P-CSCF using numerous devices in order to exhaust resources for VoLTE services.

(ii) SILENT CALL ATTACKS [27]

In VoLTE, an attacker can send call signaling messages to a victim and the victim is forced to remain in a high-power RRC state, the victim's battery can be drained fast in this way. If this attack is well-time performed by the attacker repetitively, which means the dials are terminated before victims' phones ring up, the victims will suffer from DoS attacks without any awareness.

(iii) VoLTE SPAMMING [28]

An attacker can use automatic call systems and call normal subscribers randomly to transmit commercial messages.

(iv) VoLTE SPOOFING

Since the SIP message format is easy to learn, an attacker can modify the From Number of the SIP message header and call the victim, the victim can mistakenly assume that the call is from someone he or she knows. At the same time, the corresponding user of the modified From Number can be illegally charged.

(v) VoLTE PHISHING

The above spoofing attacks can be used to trick the victim and may bring a financial misfortune to the victim.

b: ATTACKS ON SMS

SMS is a fundamental service for mobile users to communicate with short text messages. With the development of all-IP LTE/LTE-A network, the technology to support SMS service is based on the IMS system, in which the short text messages are transmitted over packet-switched networks. The common attacks existing in IMS-based SMS are summarized as follows [29], [30].

(i) SMS SPAMMING

SMS spam are the junk SMS messages delivered to mobile devices, SMS can be misused to transport mobile botnet, commercial messages, phishing messages, and malicious links.

(ii) SMS SPOOFING

The same to the VoLTE spoofing attacks, an attacker can send messages to the recipient on behalf of another mobile user without their awareness, both the recipient and the simulated user can be victims in this type of attacks.

(iii) SMS POWERED SERVICES ATTACKS

Nowadays, many commercial companies interact with their customers via SMS, for example, some e-commerce platform employ SMS to authenticate their customers, but the SMS threat mentioned above can be manipulated to launch attacks against them such as account hijacking, which can result in the leakage of victims' private information.

2) ABNORMAL CHARGING IN VOLTE

In VoLTE, the signaling bearer is used to exchange signaling messages through SIP, while the data bearer is used to transmit voice packets. Li *et al*. [31] found that the VoLTE is lack of control-plane access control. So, an attacker can abuse the VoLTE signaling bearer to transmit data packets. This can make the attacker get free data access to the VoLTE services due to the fact that the signaling traffic is free of charge. This process can also cause DoS attacks. The VoLTE provides highest QoS to control-plane signaling, if an attacker injects a large amount of traffic into the signaling bearer, the traffic will occupy all the service resources of the victims, thus the victims can suffer from data DoS attacks.

Peng *et al*. [32] explored three attacks on data charging containing free charging, fraud charging and overcharging.

In the free charging attack, an attacker can get free charge of uplink traffic using IP spoofing. In the fraud charging attack, an attacker firstly trips the normal users to set up a connection with an external spamming server, and then sends spamming data traffic to victims so the traffic volumes as well as the charging bill are increased. This can be accomplished by abusing VoIP tools. In over-accounting attack, an attacker can modify the Time-To-Live of incoming IP packets thus the packets are discard after being accounted.

3) TCP/SYN FLOODING ATTACKS

SYN Flooding attacks abuse the loopholes in the TCP protocol to launch DoS attacks. The attackers can send a large number of forged TCP connection requests to a target server, but never send an ACK message responding to the SYN-ACK messages from the target server. The resource of the target server is freed only after the TCP connection is timeout. In this way, the target server can be resource strained. And even worse, the target server may be unable to provide services for legitimate users.

4) SQL INJECTION ATTACKS

SQL injection attack allows attackers to modify the data in SIP proxies, causing denial-of-service in the authentication procedure between UE and P-CSCF. In addition, HTTP messaging can also be abused by attackers to launch SQL injection attacks.

D. ATTACKS ON END-USER EQUIPMENT

The security of end-user equipment is also of great importance in LTE/LTE-A security. The main security threats in end-user equipment are mobile botnet and malicious mobile malware. Here we give a brief overview of them.

1) MOBILE BOTNET

The connection between the Internet and mobile devices acts as a gateway for mobile botnet to move from the Internet to mobile networks. Mobile botnet is a powerful attack against mobile networks, which is launched by a large number of infected mobile devices. There are many potential threats that can be posed by mobile botnet. In addition to botnet-launched DoS/DDoS, botnet can steal data from bots to a botmaster. The botmaster has many ways to infect mobile devices including SMS botnet, Bluetooth, malwares, email attachments, and other vulnerable network services. The most common C&C channel in the LTE/LTE-A network is SMS, since SMS is widely used. There are many approaches to send SMS in a low-cost way such as some web interfaces that provide free SMS services. In this way, the SMS mobile botnet becomes efficient and economic [33].

A SMS-based mobile botnet using flooding algorithms was proposed in [34]. It can propagate commands using an Internet server. In addition, data-encryption and data-hiding were used to guarantee the stealth of this botnet. Mulliner and Seifert [35] presented SMS-only mobile botnet and SMS-HTTP hybrid mobile botnet, in which a communication tree was used. Zeng [36] proposed a mobile botnet algorithm, in which C&C communication was performed by SMS messages. Moreover, P2P topologies were also introduced to organize the botnet construction.

2) MOBILE MALWARE

Mobile malware has severe impact on the LTE/LTE-A network security, it can be abused by attackers to launch attacks such as DoS attacks, mobile botnet attacks, SMS spamming attacks and abnormal charging attacks. In addition, mobile malware can perform malicious behaviours including creating a backdoor, sensitive data stealing and privilege escalation.

Felt *et al*. [37] gave a comprehensive survey of mobile malware. They classified mobile threats into malware, personal spyware and grayware, and also described their behaviors in detail. Yan and Yan [38] provided definition and classification of mobile malware. They also summarized mobile malware detection methods, thus we will not survey mobile malware detection in this paper.

IV. DATA COLLECTION AND ANALYSIS TOWARDS ATTACKS ON LTE/LTE-A

In this section, we proposed our evaluation criteria for data collection and data analysis respectively to evaluate the advantages and disadvantages of the reviewed work. We survey the data collection and analysis literature that was oriented towards attacks on LTE/LTE-A and published in recent ten years.

A. EVALUATION CRITERIA FOR DATA COLLECTION AND ANALYSIS

In this section, we summarize a list of evaluation criteria to indicate the requirements of data collection and data analysis algorithms for the purpose of attack detection. For comparative purposes, we select the criteria as general as possible, but there are still some criteria that are critical to certain type of attack detection methods, but are inapplicable to others. We take these criteria into consideration when they are of great importance and ignore them when they are not applicable.

1) EVALUATION CRITERIA FOR DATA COLLECTION

It should be noted that in the practical communication process of the collected data, the security principles such as integrity (verify if the there is any changes of original data), confidentiality (encrypt collected data from a source contributor and decrypt them in a destination), non-repudiation (the supplied data can be certificated by a trusted third party to prevent repudiation) and authentication should be taken into consideration. It is due to the fact that the collected data are supplied to a server or system to perform analysis, attackers can obtain some privacy information from that, or they can modify the collected data to prevent an attack detector from discovering their attacks. These sanitization process of original data is beyond the scope of most of the reviewed literature, so here

we ignore them since we just evaluate theoretic data collection methods. We take the requirements listed below into account to make our evaluation.

a: EFFICIENCY

On one hand, the collected data should be compact, in other words, the unnecessary data that are useless in attack detection should not be collected. On the other hand, the needed data should be collected or calculated in a real-time and high-speed manner to decrease the time delay of attack detection.

b: PRIVACY

In the process of data collection, the sensitive information related to mobile users should be well-protected.

c: RESOURCE CONSUMPTION

The consumption of resources including power, memory, and network bandwidth in the process of data collection and data communication should be well considered.

2) EVALUATION CRITERIA FOR DATA ANALYSIS

The evaluation criteria for data analysis in the LTE/LTE-A network are summarized as follows:

a: DETECTION ACCURACY

In different detecting schemes, there are generally four metrics used by researchers to evaluate performance on accuracy, containing true positives, false positives, true negatives, and false negatives. Here, we simply judge accuracy according to the experiment results reported in the literature.

b: TIME DELAY

The duration of time from attack initiation to its being detected. If the time delay of data analysis procedure is long, the harm of attacks grows.

c: COMPUTATION COMPLEXITY

It refers to the inherent difficulty of the algorithms. If an algorithm is of bad performance on computing complexity, it requires significant resources with regard to computation time and storage.

d: HANDLING CAPACITY

Considering that the data collected can be massive, the capacity of a system to process large-scale data is of great importance.

e: ROBUSTNESS

The systems should maintain good attack detection performance when they are affected by some parameters and factors, e.g., detecting threshold, attack pattern variation, etc.

f: ADAPTIVITY

It refers to as the ability of the system to automatically adjust itself without manual configuration for the purpose of attack detection.

g: EFFECT ON SERVICE PERFORMANCE

Some certain attack detection methods may have influence on service performance of the LTE/LTE-A network. For example, the spamming detection procedure can delay the receipt time of SMS or VoLTE. It is expected that the effect of a detection method on the service performance can be negligible.

B. DATA COLLECTION AND ANALYSIS METHODS FOR ATTACK DETECTION

Here, we summarize the data collection and data analysis methods that are used in the present literature to detect the attacks on the LTE/LTE-A network. It should be noticed that we only review the detection methods of some significant active attacks. This is due to the fact that there is little existing work that focuses on the detection of passive attacks and other active attacks.

1) RF JAMMING

In recent years, the jamming detection methods in wireless sensor networks and ad-hoc networks have been widely researched. But there is little available literature related to detecting LTE/LTE-A jamming attacks, and in most cases, this kind of attacks are difficult to detect and resolve. In wireless networks, to detect jamming attacks, the basic mechanism is to collect the variety of properties of the sending or receiving nodes and estimate whether a jamming attack is happening.

Xu *et al.* [39] discussed the effectiveness of three single measurements as the basis for detecting a jamming attack, including signal strength, carrier sensing time, and Packet Delivery Ratio (PDR). The results showed that no single measurement is sufficient to determine the presence of a jammer under certain circumstances. Both signal strength and carrier sensing time can only detect the constant jammer and deceptive jammer but they are powerless in detecting a random jammer or a reactive jammer. And PDR is unable to differentiate the jamming attack from other network dynamics. To address the above issues, the authors presented two consistency checking algorithms by combining signal strength and location information with PDR respectively. Their experiments showed that their scheme is pretty powerful to detect jamming attacks. It worth noticing that the location consistency checks have a drawback that the jamming of isolated nodes is hard to be detected since the PDR of these nodes are low even when they are not jammed. This work did not consider any data collection requirements we listed before. But the data analysis algorithms in this work are powerful, and we think it satisfies two of our criteria for data analysis: detection accuracy and computation complexity.

Fragkiadakis *et al.* [40] presented an anomaly-based intrusion detection algorithms by observing the changes in the SNR statistical characteristics including average SNR, minimum SNR, and max-minus-min SNR. The authors first investigated local algorithms using simple threshold algorithms

and Cumulative Sum (CUSUM) algorithms respectively, then they investigated a fusion algorithm using Dempster-Shafer algorithm to fuse the output of the local algorithms and detect jamming attacks in a collaborative way. The performance of these algorithms was evaluated in terms of the detection probability, false alarm, average detection delay, and robustness. In this literature, all the proposed algorithms detect jamming attacks based on SNR, so the performance of the algorithms depends on the distance between jamming sources and monitored nodes. In a nutshell, the data collection procedure is efficient since they only need to collect some SNR statistical characteristics, and the local data analysis algorithms and fusion algorithms achieve good performance on detection accuracy, time delay, and computing complexity. In the local algorithm, CUSUM algorithm has better performance than the simple threshold algorithm. And the fusion algorithm using Dempster-Shafer algorithms achieves better robustness and higher performance than the local algorithm.

Lichtman *et al*. [41] proposed a jamming detection method for LTE/LTE-A especially on the PUCCH based on monitoring the excess PUCCH energy and abnormal amount of PUCCH errors. The power levels on the PUCCH should be in accordance with the transmit power commands assigned by e-NodeB, so the detection method uses a simple energy detector on the baseband samples to detect the presence of excess energy or abnormally high amount of energy in the PUCCH region. The detection method based on abnormal amount of errors monitors the bit errors in received Channel Quality Indicator values to seek for the sudden increase in errors on the PUCCH, and compares to other physical channels like PUSCH to determine if there is a jamming attack. This work did not consider any data collection requirements we defined, but we think the data collection procedure has high efficiency and low resource consumption. The authors in this work just described the detection method, but there was no simulation experiment conducted to evaluate the performance of it, so we cannot evaluate the data analysis method using our criteria, but we think its computation complexity is low.

2) SIGNALING ATTACKS

The LTE/LTE-A signaling attackers always send malicious wakeup packets to trigger the bearer setup procedure, this can lead to transmission of a large number of control messages among different network elements and saturate the LTE/LTE-A network's resources, so most of signaling attack detection methods are based on the observation of bear inter-setup time or the wakeup packet generation rate [42].

Bassil *et al*. [20] proposed a detecting method for signaling attacks. The collected data used for detection include UE number, bearer number, and time of activation or deactivation of a particular bearer. The number of bearer requests per UE and the inter-setup time can be obtained from the above data. This resulted in obtaining the average lifetime per bearer, and the number of bearer activation requests issued by a certain UE for a specific bearer. UE can be considered as malicious if inter-setup time is less than a threshold. The choice of the inter-setup time threshold is vital and can be adaptable according to the load on the e-NodeB. When the load on the e-NodeB is light, a low inter-setup time threshold will be set, since there are sufficient resources to handle the traffic. When the load is heavy, the threshold will be increased to improve the detecting sensibility. An additional feature is the number of bearer activations/deactivations per minute. If the number of bearer requests per minute of UE is more than a threshold, this UE should be considered to be malicious. The threshold determination can affect detection performance, how to choose the bearer threshold is not presented in this paper. The authors just implemented their detection scenario in OPNET but did not give experiments to show the efficiency of their method. This work did not consider any evaluation criteria we proposed. We think the data analysis method is of low computation complexity.

Gupta *et al*. [43] collected features of uplink wake-up packets, like their frequency, destination IP, destination port, etc. to obtain a set of feature vectors, containing normalized destination IP entropy, normalized destination port entropy, normalized source port entropy, normalized packet length entropy, normalized wake-up rate, variance of inter wake-up times, response-request ratio. Support Vector Machine (SVM) was used to perform supervised learning of normal data. This work needs to calculate a set of vectors in data collection procedure, so the efficiency may be not good. Privacy and resource consumption were not considered in this work. The performance on detection accuracy is pretty good when the experimental data were generated by the authors themselves, but the performance of this method in practical attacks is unknown.

Pavloski *et al*. [44] proposed a simple signaling attack detection mechanism by observing the fact that this kind of attacks can be identified by their low band-usage of communication resources. The data containing the total connected time and the connected but no data transmit time can be collected in each mobile device or in a centralized node such as e-NodeB for detecting this attack. The proposed method defines a cost function using Exponential Weighted Moving Average (EWMA) and makes decision by comparing a real-time cost with an average cost in a period of time. If the real-time cost exceeds the average cost, an attack is detected. In fact, the average cost is an adaptive threshold, it can be affected by many special circumstances and downgrade detection performance. For example, video streaming or voice communication can bring out a very low threshold, thus normal usage is wrongly judged as abnormal. The authors proposed upper and lower thresholds to improve the performance. The experimental results showed that the average detection delay, false positive as well as false negative of this method are satisfactory. The advantage of this work is that the algorithm does not require any high computational, storage or energy demands to achieve real-time detection. However, the upper and lower thresholds as well as the parameters in the cost function are unable to dynamically adapt to communication environments, thus decreases the effectiveness of this method.

In a nutshell, the data collection procedure in this work is efficient, and the detection accuracy, time delay and computation complexity of its data analysis method satisfy our criteria.

In a brief summary, most of the above methods did not concern any criteria we proposed in data collection procedure, and their data analysis methods did not take handling capacity, robustness and effect on service performance into consideration.

3) ABNORMAL SIP MESSAGES

We first review two comprehensive methods that can detect abnormal SIP messages. Then we will review some detection methods that focus on SIP message attacks and SIP flooding attacks. The following presents the detecting methods against abnormal SIP messages.

Wahl *et al*. [45] presented a signature-based anomaly detection method in which SIP messages are embedded in a vector space to reflect the characteristics of the SIP traffic. The presented method first extracts feature strings using the definitions of ''tokens'' and ''n-grams'', then both global and local anomaly detection methods based on geometric learning models are used to detect unknown attacks. The core of geometric models is to calculate the Euclidean distance in the vector space. The global model calculates the distance between the incoming SIP message and the center of an optimal hypersphere. The points that exceed the super-sphere can be identified as anomalies. Since the global model is not efficient to detect inherently heterogeneous points, the local model based on k-nearest neighbour algorithms is used to assess the deviation of messages. Anomalies can be found due to their large distance to neighbouring points. Then the signatures of the detected attacks are generated by clustering the anomalies using linkage clustering or k-means. Distributing these signatures to the signature-based detection system can improve detection accuracy. Their experiments showed that the local model has higher accuracy than the global model. There are two drawbacks in this method: one is that the feature extraction process is cumbersome, and the other is that its computational cost is high. But, its detection accuracy is excellent.

Nassar *et al*. [46] presented an online monitoring approach based on SVM to detect SIP-related attacks. In the proposal, the SIP traffic is cut into small slices and 38 features of SIP traffic flows are extracted containing general statistics, Call-ID based statistics, distribution of final state of dialogs, distribution of SIP requests, and distribution of SIP responses. These features are input of a SVM learning machine. This method performs well for detecting flooding attacks and Spam over Instant Messaging (SPIM). But the heavy features that need to be collected may affect the efficiency of data collection procedure and lead to high resource consumption. Meanwhile, privacy in data collection was not considered. The experimental results showed high accuracy of the data analysis algorithm, but its computation complexity is a little bit high.

Given that the malformed SIP messages attacks and the SIP flooding attacks are the most common attacks on IMS, we here list some detection methods that specifically target at these two attacks. Seo *et al*. [47] presented an anomaly detection method based on Stateful Rule Tree. The main idea is refining the rules of original RFC 3261 rules and creating a rule tree structure. In detection of malformed SIP messages, they applied a rule matching algorithm to check if the header of a packet follows the secure rules they designed and detect unmatched or undefined message headers. In detection of the SIP flooding attack, they adopted the state transition models in the RFC 3261. The flooding attacks can be detected if the number of received messages exceeds pre-defined thresholds, which are determined according to states. This detection method has good performance in terms of accuracy and detection speed. In addition, the effect on networking service and overhead is also reduced. In a word, we think the data collection procedure is efficient and of low resource consumption. The data analysis method satisfies most of our criteria except robustness and adaptivity.

Zhang *et al*. [48] presented an automatic detection scheme of SIP flooding attacks and SIP malformed messages attacks on VoLTE. To detect the former attacks, it employs threshold-based algorithms in which the instant amount of SIP packets received from VoLTE interface within one minute is compared with a threshold. Nevertheless, determination of the threshold is not specified and the performance of their detection scheme was not evaluated by experiments. To detect the latter attacks, it matches the collected SIP messages with ontology formalization rules. The experiments showed that the performance on false negative need to be further improved with regard to detective ontology description. It should be noticed that this scheme was designed from the view of mobile users and it should be implemented at user mobile devices. The data collection procedure satisfies all of our criteria. The computation complexity of data analysis algorithm is low, but the detection accuracy for malformed SIP messages is not so good. In addition, the detection accuracy for SIP flooding attacks is not illustrated.

The detection methods for SIP flooding attacks have drawn many researchers' attention. Introduced below are some work concern with SIP flooding attacks. Lee *et al*. [28] presented a statistical and learning-based detection method for SIP flooding based DoS attacks. The presented algorithm just simply compares the collected factors of the traffic including IP, URI (Uniform Resource Identifier), Call-ID, and Method (e.g., INVITE, BYE) with their detection rules. Every detection rule has a corresponding threshold value that is updated dynamically. The data collection of this work did not consider data privacy, but its performance on efficiency and resource consumption is good. Experiments showed that the detection rate of this method can be maintained at a high level regardless of the volume of transmitted packets. This method achieves good performance in terms of detection accuracy, computation complexity and handling capacity.

Ko *et al*. [49] presented a threshold-based detection method for detecting SIP amplification attack. SIP amplification attack is a kind of SIP flooding attack, to launch this attack, an attacker sends floods of SIP register messages with a spoofed identity to server, and the server will send a challenge message to the normal user with the same ID, but the normal user won't response to it, so the server can't receive any confirmation response message, it will repeatedly retransmission the 401 unauthorized messages to the normal user. The proposed method detects this attack by monitoring the amount of repeated 401 unauthorized messages. To improve the efficiency, this work only focuses on 401 response messages packet that is sent from network to users, the collect data of target packets containing call-ID, source/destination IP, command sequence, and timestamp are recorded in a table. Attacks can be detected if the count of the same record exceeds certain threshold in a fixed time interval. The data collection procedure is efficient and of low resource consumption. However, there is no experiment reported in [49] to show the performance of the presented method.

It should be noted that the volume-based monitoring technique is not able to distinguish between low-rate flooding and normal fluctuation, so Hellinger Distance (HD), Tanimoto Distance (TD) and CUSUM metric are employed in detecting gradually increasing flooding attacks. The HD-based flooding detection algorithms adapt the dynamics of network traffic using a window mechanism and show an excellent sensitivity in detecting flooding attack. In addition, Mehta *et al*. [50] indicated that the Euclidean classifiers are inefficient for detecting self-similar SIP messages.

Sengar *et al*. [51] presented a detection scheme for flooding attacks, the proposal employs HD to measure the deviations of SIP attributes between training data and test data. If the HD exceeds the dynamic threshold computed by a stochastic gradient algorithm, an attack is detected. The data collection of the proposed work is efficient and of low resource consumption. Their experiments showed that their scheme is of great accuracy and high detection speed in detecting high-rate flooding attacks. Moreover, computation consumption, adaptivity and the effect on service performance were considered in this work. Its drawback is that the threshold may be imprecise when a low-rate attack happens.

An online detection scheme for SIP flooding was proposed in [52] based on sketch technique combining with HD. The sketch technique is used to generate a probability mode from a SIP call set up process and predetermine future distribution based on historical information. The HD between current traffic distribution and estimated distribution is used to detect attacks. The dynamic threshold is calculated by EWMA algorithms, and an alarm will arise when the HD exceeds the threshold. This scheme can deal with low-rate flooding attack as well as multi-attribute flooding attack efficiently. The data collection criteria like efficiency and resource consumption are satisfied in this work. In addition, the data analysis algorithm achieves good performance on detection accuracy, computation complexity, and adaptivity.

Hecht *et al*. [53] proposed a HD-based detector for IMS DoS attacks that are caused by flooding of SIP messages. Their method first puts the probability of six types of SIP messages containing INVITE, OK, ACK, BYE, REGISTER, and SUBSCRIBE into a vector, and then calculates the square of the HD between the vector of a training phase and that of a production phase. If the square of the HD exceeds the dynamic smoothing threshold calculated by an exponential averaging procedure, an attack may exist in the network. The experiments showed that the detection accuracy is sensitive to several key parameters such as the length of the training phase and its accuracy is poor in low-rate flooding rate conditions. This demonstrates that the method is not sufficient enough to detect flooding attacks in complicated network environments. But we think the data analysis method is adaptive and of low computation complexity.

Chaisamran *et al*. [54] proposed a statistical anomaly detection system based on TD. The system is similar to [53]. They divided incoming traffic into training and testing segments. The probability distributions TD of five SIP message types containing REGISTER, INVITE, ACK, 200 OK, and BYE segments are calculated. An alarm will raise if a measured distance exceeds a dynamic threshold. The estimate of threshold is based on mean deviation of SIP attributes in recent SIP packets by using EWMA and the track of data trends. However, the threshold-based detection algorithms have a common drawback that it is not effective in detecting slightly increasing traffic attacks. This work improves this drawback by introducing an oscillator indicator module, in which slightly increasing traffic can be detected when the calculated momentum exceeds a desired level. The performance evaluation dedicated that the proposal is excellent in both sensitivity and specificity. Our data analysis criteria such as detection accuracy, computation complexity and adatptivity are satisfied well, but this work didn't show its time delay, handling capacity, robustness, and effect on service performance.

An approach to detect flooding DoS attacks on IMS system was described by Rebahi *et al.* [55]. The proposed detector first observes SIP traffic from a P-CSCF server in the same time intervals and counts the number of certain SIP requests such as INVITE, then EWMA is used to estimate its mean rate during a certain time interval and identify flooding attacks. The performance evaluation indicated that the approach is efficient in detecting both constant rate and increasing rate attacks. The detection time delay of the former attacks is more satisfactory than that of the latter attacks. This work lacks consideration on handling capacity, robustness, and effect on performance.

In addition, two comprehensive studies investigated the efficiency of different machine learning algorithms for detecting SIP flooding attacks [56], [57].

According to the above analysis, we can see that most of existing work detects abnormal SIP messages by collecting and analyzing SIP message attributes. Data collection achieves good performance on efficiency. The data

analysis procedure normally adopts machine learning algorithms or combines threshold-based algorithms with distance algorithms like HD and TD. The calculation method of threshold is of great importance in detection accuracy. However, the threshold-based algorithms always have bad performance on detecting low-rate flooding attacks. EWMA algorithms are commonly used in the calculation of threshold to improve this problem. It is obvious that most of above work ignored handling capacity, robustness and effect on service performance in data analysis.

4) VOLTE SPAMMING

There is little work on VoLTE spamming attack detection. We introduce below some proposals on VoIP spamming detection.

Kim *et al*. [58] presented a model of spam caller's behaviours using Discrete Event System Specification formalism. Its input factors contain Requests from Administrator, Call Rejection Rate, Number of Call Recipients, Call Duration, Call Traffic, Call Rate, and Inter-Call Rate. This model can calculate the spam level of users and detect spammers. To calculate the spam level, the system derives a normalized value for every input factors, these values reflect the spam level based on the weighting coefficient. Then a decision threshold will be defined, a caller can be considered as spammer if he/she's spam level exceeds the threshold. Nevertheless, this model suffers from an accuracy issue especially on high false positive due to impropriate weight of certain factors in decision making. The proposal did not take data privacy into consideration. Most of the data analysis criteria is not satisfied in this work except the computation complexity.

Lee *et al*. [28] proposed a scheme that can detect VoIP spamming using behaviour-based detection algorithm. The collected factors were referred to [58]. But this work optimized the performance of the scheme in [58] by changing decision making criteria. The false positive in [28] is better than that of [58]. This work also ignored the privacy issue in data collection procedure, but its detection accuracy and handling capacity is good.

In the above two studies, the efficiency and resource consumption of the data collection procedure are satisfied. But the data analysis algorithm ignored most of our criteria except for computation complexity.

5) SMS SPAMMING

This type of attacks can be detected in both user side and network side. The former detection system provides users with configurable spam filtering service. The main technique is content-based filtering which uses feature extraction algorithms and text classifiers, such as Naive Bayes, Decision Tree, SVM, Artificial Neural Network (ANN), k-Nearest Neighbor (kNN), and Hidden Markov Model (HMM). SVM and Naive Bayes are the most accurate techniques for SMS spam filtering. Meanwhile, Neural Network, HMM and Decision Tree are complicated and time consuming [59]. The content-based SMS spam detection techniques may touch upon user privacy issue and huge memory requirements at the server side. The latter detection system in the network side can help reducing the cellular bandwidth consumed by SMS spam, and achieve real-time transmission of the massive SMS messages. The detection can be based on behaviour analysis, content-based analysis, subscriber feedback-based methods, sender reputation-based schemes, and traffic analysis technologies [60], [61].

From aspect of user side, a large amount of SMS spam filtering systems for mobile devices have been studied in the past years. The main technologies are based on black/white list and text classification. The former compares words in the SMS content to black list keywords that are manually chosen by users, while the latter uses pattern recognition algorithms such as SVM, Naive Bayes, Decision Tree, etc.

Nuruzzaman *et al*. [59] proposed an independent SMS filtering system based on text classification by using Naive Bayes. They employed a word occurrence table instead of creating a vector table to reduce storage consumption and computation complexity. The SMS spam are filtered with a continually updated Naive Bayes filter. This work satisfies all our data collection criteria. The detection accuracy and time delay achieved by this system is excellent. One deficiency of this proposed filtering system is that it is unable to adapt quickly to user's new perception due to the fact that the word occurrences table is pre-generated. In addition, issues like handling capacity, robustness and effect on performance were not considered.

Vural and Venter [62] detects SMS spam using artificial immune systems in an Android device. A unique advantage of artificial immune systems is that it only requires normal SMS in training. The features such as the number of white spaces, capital letters, punctuation characters, digits, words, URL, and telephone numbers are collected to detect abnormal behaviours. Taking care of privacy implications, the authors chose to analyze the data in the mobile device. But it brings the drawback that a software package needs to be installed in the mobile device, which has limited processing power and storage space. Experimental results showed that the proposed detection method can effectively detect invalid SMS messages, but it still need to be improved by collecting more features such as the time of day that the messages are sent and perhaps the number of recipients per SMS. This work supports all the data collection criteria as we proposed. However, the data analysis criteria such as time delay, handling capacity, robustness, adaptivity and effect on performance were not considered.

Yadav *et al*. [63] also proposed an SMS spam filtering system based on SVM and Bayesian approaches. It first learns the occurrence of words in spam and legitimate SMS, and then determines if a message is a spam by analyzing the message contents. In addition, the spam can also be detected based on a sender's phone number. The proposed system employs a server in which users can share spam keywords and a sender blacklist to improve spam detection accuracy. The performance evaluation showed that the

SVM-based approach has higher spam detection accuracy than the Bayesian-based approach, while the Bayesian-based approach has higher legitimate SMS detection accuracy. The data collection criteria are satisfied well in this work. Detection accuracy, time delay, computation complexity, and adaptivity are also satisfied in data analysis.

In network side, cellular service operators always deploy a reporting mechanism to detect spammers. Thus, subscribers can report received spam messages to specific servers. The drawback of this method is that the report rate may be low and the time delay is significant, which leads to spammer detection inefficiency.

There are many studies about SMS spam detection on the network side. Das *et al*. [30] proposed a detection module at the PDN-GW in the LTE/LTE-A network where the collected data packets are represented as a set of vectors. Known spam messages and legitimate messages are used to train a classifier. The authors evaluated performance (with regard to accuracy and time delay) of four machine learning algorithms including Naive Bayes, SVM, AdaBoost and J48 in a campus mobile network. The data collection in this proposal is efficient, but it did not take privacy and resource consumption into consideration. The results showed that SVM has the best detection accuracy, while AdaBoost has the lowest time delay. The detail performance of the four machine learning algorithms is summarized in Table 1, Naive Bayes and SVM have good detection accuracy, but their time delay is long. On the contrary, the detection accuracy of AdaBoost and J48 is not good, but the time delay is short and their computation consumption is low.

Zhang *et al*. [64] presented an SMS spammer detection scheme based on behaviour analysis. The scheme integrates multiple behaviour attributes of users and extracts statistical properties from SMS records which records the information of each SMS, including calling number, called number, transmission time, receiving time and message length. Then five machine learning algorithms including Binary Decision Tree, Random Forest, SVM, Logistic Regression, and Self-Organized Feature Mapping are used to train the classifier of spammer and non-spammer. The data collection procedure is efficient and of low resource consumption. And it is worth mentioning that this scheme is based on SMS records without containing SMS messages, which can protect the privacy of users somehow. The detail performance of these machine learning algorithms is summarized in Table 1, experiments showed that Random Forest can achieve the best precision rate and recall rate in an acceptable time. The data analysis procedure did not take handling capacity, robustness and adaptivity into account. This scheme has a better performance in terms of accuracy and recall rate than the traditional methods based on keywords and sending frequency. Even though, the accuracy of this proposal also needs to be further improved by combining with content-based analysis.

Liu and Lu [65] presented a spam inspection system. Its core module is an intelligent analysis module. The main function of the intelligent analysis module is data mining and making judgment of spam based on such data as frequency of called/calling numbers, message length, successful sending rate, etc. The system first checks if there is someone sending messages frequently, then his/her number will be compared to a white list and a black list, as well as keywords, respectively. If it satisfies a certain condition, the system stops message forwarding, and updates the keywords listed in the blacklist. The drawback of this system is its performance is affected by certain parameters, so parameter optimization is needed. But usually, spammers can bypass detection by adapting their strategy according to these parameters. The proposed system collects data in an efficient way with low resource consumption. However, its detection accuracy is not so good. The data analysis criteria such as time delay, robustness, adaptivity and effect on service performance were not considered.

Coskun and Giura [66] proposed a fast online detection scheme by employing robust text signatures to detect repetitive similar SMS spam messages before their delivery. In the proposal, Jaccard similarity metric is used to calculate the similarity between two SMS messages. Two messages are considered as similar if the calculated result exceeds a threshold. They used Counting Bloom Filters to observe if there are massive similar spam messages transmitted in a short period of time. The proposed scheme does not store any information in a centralized server in consideration of privacy, resource consumption and efficiency. It is also robust in detecting slightly modified SMS spam messages and sender number variation. Experimental tests showed that the proposed scheme can achieve real-time detection of SMS spam with a high detection rate and great handling capacity. But the main limitation of this work is its false positive is high when a large bloom filter is used. The authors also indicated that the scheme can be optimized by increasing the computing complexity to improve its detection accuracy. Because this scheme is based on content analysis and sending frequency, spammers can somehow evade or mislead the detectors easily. In a word, the data collection in this work has good performance on efficiency, privacy and resource consumption. What's more, its data analysis supports almost all our criteria except for adaptivity and effect on service performance.

Chen *et al*. [67] presented a trust management based SMS control system. In the proposed system, hosts first detect unwanted SMS and report SMS spam detection result to Service Provider, then the Service Provider evaluates the trust of SMS senders based on collected data and triggers SMS spam control at a Global Trust Operator, which can identify the source of spam. Its performance evaluation showed that the system prototype is of great accuracy, efficiency and robustness. However, handling capacity, adaptivity and effect on service performance were not concerned.

To sum up, the user side detection methods in [59], [62], and [63] adopt content-based methods and analyze SMS contents through machine learning. Some network side detection method [66] is also based on the analysis of text signature in message contents, while other network side works [64], [65], [67] are based on other characteristics

TABLE 1. Comparison of data collection and data analysis methods for main attacks on LTE/LTE-A.

Attacks	RE	Collected data	E	P	RC	Data processing and analysis algorithm	ST	Platform	DA	TD	CC	HC	R	A	EP
RF jamming	[39]	Signal strength Carrier sensing time PDR Location information	*	*	*	Threshold-based algorithms	/	MICA2 Motes	√	*	√	*	*	*	/
	[40]	SNR-based metrics Timestamp	√	/	*	Threshold-based algorithms	A-B	Ath5k driver	◊	√	√	*	×	×	/
						CUSUM algorithms			√	√	√	*	×	√	/
						Dempster-Shafer algorithms			√	√	√	*	√	×	/
	[41]	Channel energy Bit errors	√	/	√	Comparing algorithms	/	*	*	*	√	*	*	*	/
Signaling attacks	[20]	Devices number Bearer number Activation time Deactivation time	*	*	*	Threshold-based algorithms	/	OPNET	*	*	√	*	*	*	*
	[43]	Destination IP Destination port Source port Packet length Wake-up rate Inter wake-up time Response ratio	×	*	*	SVM algorithms	A-B	*	◊	*	◊	*	*	*	*
	[44]	Connected time Connected but no transmission time	√	/	√	EWMA algorithms Threshold-based algorithms	/	SECSIM simulator	√	√	√	*	*	◊	*
Abnormal SIP messages	[45]	SIP messages	◊	*	◊	Euclidean Distance Geometric models KNN algorithms	S-B	Codenomi-con Defensics	√	*	◊	*	*	*	*
	[46]	SIP messages	◊	*	◊	SVM algorithms	A-B	LibSVM, OpenSER	√	*	◊	*	*	*	*
Malformed SIP attacks	[47]	SIP messages	√	*	√	Stateful Rule Tree Rule matching algorithms	A-B	PROTOS, SiVuS	√	√	√	√	*	*	√
	[48]	SIP messages	√	√	√	Rule matching algorithms	A-B	Jena, JAIN	◊	*	√	*	*	√	*
SIP flooding attacks	[28]	Packets (IP, URI, Call-ID, and Method)	√	*	√	Threshold-based algorithms	A-B	ThreatEX	√	*	√	√	*	*	*
	[47]	SIP messages	√	*	√	Stateful Rule Tree State transition models	A-B	PROTOS, SiVuS	√	√	√	√	*	*	√
	[48]	SIP messages	√	√	√	Threshold-based algorithms	/	Jena, JAIN	*	*	*	*	*	*	*
	[49]	Packets (Call-ID, Source IP, Destination IP, Command sequence, Timestamp)	√	*	√	Threshold-based algorithms	/	*	*	*	*	*	*	*	*
	[51]	SIP attributes (INVITE, BYE, 200OK, ACK)	√	/	√	Hellinger Distance Stochastic gradient algorithms Threshold-based algorithms	A-B	NISTNET	√	√	√	*	*	√	√
	[52]	SIP attributes (INVITE, BYE, 200OK, ACK)	√	/	√	Hellinger Distance Sketch techniques EWMA algorithms Threshold-based algorithms	A-B	MATLAB	√	*	√	*	*	√	*
	[53]	SIP attributes (INVITE, OK, ACK, BYE, REGISTER, SUBSCRIBE)	√	/	√	Hellinger Distance EWMA algorithms Threshold-based algorithms	A-B	Libpcap, Anjuta, SiVuS	◊	*	√	*	*	√	*
	[54]	SIP attributes (INVITE, OK, ACK, BYE, REGISTER, SUBSCRIBE)	√	/	√	Tanimoto Distance EWMA algorithms Threshold-based algorithms	A-B	Seagull	√	*	√	*	*	√	*

TABLE 1. *(Continued.)* **Comparison of data collection and data analysis methods for main attacks on LTE/LTE-A.**

	[55]	SIP attributes	√	/	√	CUSUM algorithms EWMA algorithms Threshold-based algorithms	/	SNOCER	√	√	√	*	*	√	*
VoLTE Spamming	[28]	Call rejection rate Number of Recipients Call duration Call traffic Call rate Inter-call rate	√	*	√	Behavior-based algorithms	A-B	ThreatEX	√	*	*	√	*	*	*
	[58]	Call rejection rate Number of Recipients Call duration Call traffic Call rate Inter-call rate	√	*	√	Discrete Event System Specification formalism	A-B	OPNET	◊	*	√	*	*	*	*
SMS Spamming	[30]	Signaling packets Data packets	√	*	*	Naive Bayes	/	Weka, OPNET	√	◊	√	*	*	*	*
						SVM algorithms			√	◊	◊	*	*	*	*
						AdaBoost			×	√	√	*	*	*	*
						Decision Tree (J48)			◊	√	√	*	*	*	*
	[59]	SMS messages	√	√	√	Naive Bayes	/	UE	√	√	√	*	*	×	*
	[62]	White spaces Capital letters Punctuation Characters Digits Words URLs Phone numbers	√	√	√	Artificial immune systems	A-B	Android emulator	√	*	√	*	*	*	*
	[63]	SMS messages	√	√	√	SVM algorithms Bayesian algorithms	/	Symbian, SVMLib	√	√	√	*	*	√	*
	[64]	Calling number Called number Transmission time Receiving time Message length	√	◊	√	Decision tree	A-B	*	◊	√	√	*	*	*	/
						Random forest			√	√	√	*	*	*	/
						SVM Gaussian algorithms			√	×	◊	*	*	*	/
						SVM Linear algorithms			×	×	◊	*	*	*	/
						Logistic regression			◊	√	√	*	*	*	/
						Feature mapping			◊	√	√	*	*	*	/
	[65]	Calling number Called number Message length Sending success rate Timestamp	√	*	√	Data mining Threshold based algorithms	/	*	◊	*	√	√	*	*	*
	[66]	SMS messages	√	√	√	Jaccard similarity metric Counting Bloom Filter Threshold based algorithms	/	*	√	√	√	√	√	*	*
	[67]	Time Phone number SMS content Changes Similarity	√	√	√	Trust management Threshold based algorithms	/	SQLite	√	√	√	*	√	*	*
Mobile botnet	[68]	Source IP address Source port Destination port Protocol types Time stamps	√	*	√	Neural Networks	/	*	*	*	*	*	*	*	*
	[69]	Sender number Receipt number URLs links Specific words Phone numbers	√	√	√	Pattern-matching Rule-based techniques	S-B	*	√	√	√	*	*	*	*
	[70]	Phone ID Action Category Component	√	√	√	Threshold-based algorithms	/	MySQL	√	*	√	*	*	*	*
		Details of bundle Time stamp													
	[71]	Incoming SMS volume Outgoing SMS volume Consistency of volume SMS sending delay	√	*	√	Behaviour-based algorithms Fuzzy techniques	A-B	*	*	*	√	*	*	*	*

*RE: Reference; E: Efficiency; P: Privacy; RC: Resource Consumption; ST: Strategy; DA: Detection Accuracy of Algorithms; TD: Time Delay; CC: Computation Complexity; HC: Handling Capacity; R: Robustness; A: Adaptivity; EP: Effect on Service Performance; A-B: Anomaly-Based; S-B: Signature-Based; √: has good performance on the criterion; ×: has bad performance on the criterion; ◊: partially meet the criterion; *: not mentioned in the literature; /: no need to meet the criterion*

of SMS messages, like phone number and message length. To summarize the performance of the above reviewed work, most of them satisfy the requirements on efficiency, privacy and resource consumption in data collection. It is obvious that the SMS spamming detection in user side has less privacy risk than that in network side. Moreover, issues in data analysis like detection accuracy, time delay and computing complexity are supported while other issues are concerned in only few researches.

6) MOBILE BOTNET

There are many studies about botnet detection in both the Internet and mobile networks. The detection of botnet in the Internet is beyond the scope of this survey, so here we just give a literature review on the botnet detection methods in mobile networks.

Oulehla *et al*. [68] proposed a double Neural Network architecture to detect both client-server botnet and hybrid botnet. The data collected for detection consist of source IP address, source TCP/UDP port, destination TCP/UDP port, protocol (TCP or UDP) and time stamps. Suitable features can be deduced from the collected data and used as the input vectors of detection analysis. The detail data analysis algorithm was not given and its efficiency was not evaluated through experiments since the proposed architecture is still in a preliminary stage.

We found the literature has many studies on SMS-based mobile botnet detection. Alzahrani and Ghorbani [69] proposed a real-time content-based signature detection mechanism in a mobile device to combat SMS botnet. Pattern-matching and rule-based techniques were applied to implement signature-based detection. Pattern-matching method can detect malicious SMS by looking for specific patterns of selected features, which include sender phone number, receipt phone number, URLs, specific words, phone number in content and phishing words, and determine if there is a match with the signatures of known botnet and malware. Rule-based techniques were used to decide whether the incoming or outgoing SMS is abnormal by applying certain rules. This scheme also suffers from the general drawbacks of signature-based detection. One is that its input signatures should be frequently updated, the other is that it is unable to effectively detect unknown attacks. Almost all of our data collection criteria are satisfied in this work. But the data analysis procedure only supports such requirements as high detection accuracy, low time delay, and low computation complexity. Other criteria were not considered.

Johnson and Traore [70] also presented a system to detect non-user initiated malicious SMS messages. The system is composed of an intent capture module on mobile devices and a center server to provide further analysis of collected data from multiple sources. The proposed system loads an application onto the mobile device to log the activity events of mobile devices and communicate with the center server. The activity events are described with such collected data as phone ID, action, category, component, details of bundle, time stamp. The data are analyzed by using a white list along with a simple temporal threshold to determine if one SMS activity is malicious. The performance evaluation result on accuracy is encouraging. But further improvement is still needed, e.g., algorithm simplification and optimization. The data collection of this work takes every criterion we proposed into consideration. But its data analysis ignores most of our criteria except for its high detection accuracy and low computation complexity.

Vural and Venter [71] proposed a mobile botnet identification scheme with network forensics. Its main idea is that a cellular network server monitors the significant deviations of users' behaviours. The behaviour profile for users is described by metrics containing weekly incoming/outgoing SMS volume, consistency of weekly incoming/outgoing SMS volume, SMS sending delay, median of SMS sending delays. These metrics are used to train computational intelligence to learn normal behaviours. Then fuzzy techniques are used to compare current behaviours with the normal behaviours, and identify abnormal users. Unfortunately, performance evaluation was not provided in [71]. We think this scheme may not be accurate. Because SMS spammer also has similar changes of users' behaviour, so the changes of collected metrics does not indicate that the user is affected by mobile botnet. Maybe the user just becomes a SMS spammer. The data collection of this scheme is efficient and of low resource consumption. Its data analysis did not consider most of our criteria but its computation complexity is not high.

We can see that current work related to mobile botnet (especially the SMS-based mobile botnet) detection generally adopted content-based or behavior-based algorithms. The data collection methods in the above works satisfy most of our criteria especially the privacy. The data analysis methods lack considerations on handling capacity, robustness, adaptivity and effect on service performance.

C. SUMMARY OF DATA COLLECTION AND ANALYSIS IN ATTACK DETECTION

We apply the proposed evaluation criteria to summarize the data collection and data analysis methods reviewed above in Table 1. In Table 1, the crucial items including collected data, data analysis algorithms and strategies (abnormal-based or signature-based), and experimental platforms of the reviewed works are listed.

According to Table 1, we can see that efficiency and resource consumption in data collection methods were concerned in most of existing work. But the privacy issue was not considered in many works though the privacy is of great importance for users.

The data analysis methods of existing work always adopt threshold-based or machine learning algorithms. Most of the data analysis and detection methods can be classified into signature-based (also be refer to as misuse-based) and abnormal-based (can also be refer to as behaviour-based) techniques. The signature-based detection methods are based on a set of rules and signatures to detect known attacks. The

false positive rate of this mechanism is always satisfactory. But this kind of methods is not suitable in large-scale network security measurement since a large amount of attack signatures are needed and should be frequently updated in order to achieve high detection accuracy. The anomaly-based detection methods build a normal activity profile and observe the deviation of monitored traffic from normal traffic in order to detect attacks. This kind of methods are able to detect unknown novel attacks. But the false positive rate is high. Hybrid-based techniques are also studied in recent years, they combine the above two approaches. In one hand, they inherit the high accuracy of signature detection techniques to detect known attacks. In the other hand, they take advantages of the anomaly detection techniques to detect unknown attacks.

Most of the reviewed work can achieve good performance on detection accuracy, time delay, and computation consumption, but other data analysis criteria like handling capacity, robustness, adaptivity and effect on service performance were rarely considered.

In brief, none of existing work we described above can achieve perfect performance on every criterion we proposed, further improvement on the proposal is needed since all of our criteria is crucial for LTE/LTE-A network security measurement.

V. OPEN ISSUES AND FUTURE RESEARCH TRENDS

Based on the survey and analysis presented in Sections 4, we identified the following open issues on data collection and data analysis in the LTE/LTE-A network with a view to stimulate future research.

First, a comprehensive scheme that is able to detect all types of attacks in a lightweight way is required. Most of existing work only performs data collection and data analysis against a certain type of LTE/LTE-A attacks, full-scale work aiming at various attacks is still lacking. Therefore, how to integrate the collected security data in existing work and perform real-time data analysis is think-worthy. There are many attacks that have similar feature appearance, for example, SMS spamming attacks and mobile botnet attacks have similar properties in message content. We believe that collaborative detection of these related-attacks can improve the efficiency of the security measurement system.

Second, protecting data security and user privacy in data collection, storage and transmission procedure is a challenging research topic. Most of existing work did not take secure metrics such as integrity, confidentiality, non-repudiation and authentication into consideration. But there is a critical need to ensure data security since the collected data always involve privacy information of users. The other reason is attackers can modify the collected data to mislead the data analysis procedure, so they can evade detection. In a nutshell, privacy protection and security assurance of collected data are open research issues that deserve special attention. Secure channels and protocols with encryption techniques should be established in the whole system. In addition, data sanitization techniques like Boom filters should be applied to protect the security of the data. But it should be noticed that the trade-off among computing cost, utility of data and security of data should be well balanced.

Third, minimal overhead is of great significance in data collection and analysis. This problem should be considered in many aspects including power and memory consumption in data collection stage, bandwidth consumption in data transmission stage, and computation and memory consumption in data analysis stage. Resource consumption of data collection especially in large-scale LTE/LTE-A network can be huge. A good data collection mechanism should collect data in an adaptive way to save the cost of power, memory, and bandwidth usage of data transmission. What's more, the data analysis cost should be well concerned. We think feedback mechanism that can report data collection requirements from data analysis module to data collection module is of benefit to improve the efficiency of whole security measurement system. It can reduce the amount of collected data and cut down the data analysis cost.

Fourth, perform data pre-processing is challenging due to the fact that the original data are heterogeneous and of massive scale. How to perform security-related data sampling, filtering, and gathering is a significant research topic that is worth exploring.

Last but not least, existing data analysis methods need further improvement since most of them lacked consideration on handling capacity, robustness, adaptivity and effect on service performance.

VI. A DATA COLLECTION AND ANALYSIS MODEL

In this section, we present a model architecture for data collection and analysis for LTE/LTE-A network security measurement. The flowchart in Fig. 5 depicts our model. Our model contains four layers: distributed data collection layer, data pre-processing layer, data analysis layer, and system self-guard layer, which are described below.

A. DISTRIBUTED DATA COLLECTION LAYER

The main component of the first layer is data collector, which is embedded into different network entities and performs distributed original data collection from different network entities such as e-NodeB, GW, and UE. To achieve good performance on resource consumption in terms of memory, transmission band usage, and so on, periodic based and request and response based methods could be applied. In different contexts, the data types and frequency of data collection can be adaptively and intelligently decided according to the feedback of the data analysis layer or the self-environment of the data collector. For example, if the data analysis layer finds anything abnormal of SIP messages, it will request the data collectors to collect more detail data like SIP attributes to determine which SIP attack is happening.

B. DATA PRE-PROCESSING LAYER

The databases of the data pre-processing layer can get and store the data collected by the data collectors. This data

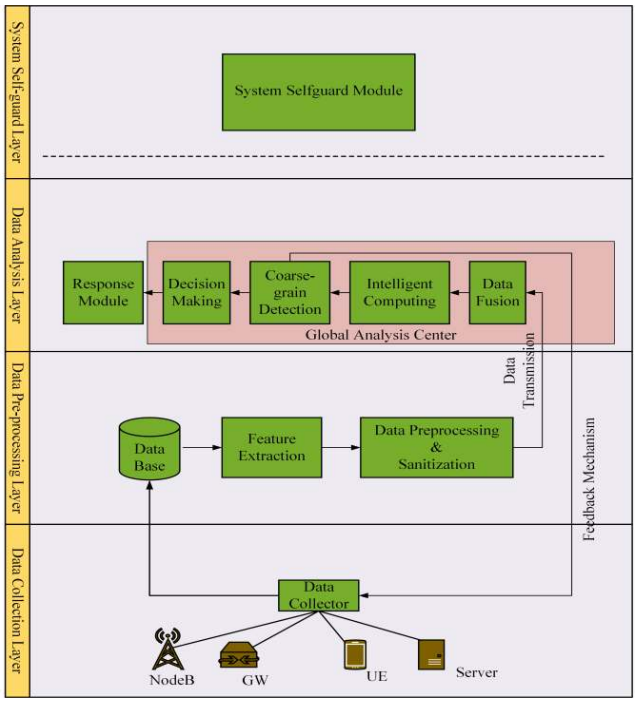

FIGURE 5. A data collection and analysis model.

pre-processing layer is responsible for pre-processing the collected data and calculating the features we need in the data analysis layer. In this procedure, protection and sanitization of security data should also be carried out before the data is transmitted to the data analysis layer, this is for the purpose of achieving data integrity, confidentiality, and non-repudiation. In data sanitization, the collected data should be encrypted, in addition, noises should be added to protect user privacy. It should be noticed that the data sanitization procedure should not destroy the usefulness of data.

C. DATA ANALYSIS LAYER

Since the collected data are normally in a large scale and their analysis is of great burdensome, we transmit the collected data to a specific server (that can be cloud based), called global analysis center for analysis. Efficient data fusion and machine learning techniques can be employed to ensure the accurate and real-time collaborative analysis to determine which type of attacks the network is suffering from and make appropriate responses (like triggering a defense function and informing a network security administrator). The design of the global analysis center is complicated due to the lack of a comprehensive method that can detect all types of attacks. Fortunately, there are always some correlations between attacks such as SMS spam and mobile botnet, abnormal SIP messages and VoLTE attacks, so the identification of these attacks can be linked together. Considering the overhead of computation and communication, the global analysis center first monitors the network traffic in a coarse-grained way,

TABLE 2. Abbreviations

AKA	Authentication and Key Agreement
ANN	Artificial Neural Network
AS	Access Stratum
AuC	Authentication Center
C&C	Command and Control Center
CSCF	Call Session Control Function
CSFB	Circuit Switched Fallback procedures
CUSUM	Cumulative Sum
DDoS	Distributed Denial of Service
DNS	Domain Name Service
DoS	Denial of Service
e-NodeB	evolved-NodeB
e-PDG	evolved-Packet Data Gateway
E-UTRAN	Evolved-Universal Terrestrial Radio Access Network
EDGE	Enhanced Data Rate for GSM Evolution
EPC	Evolved Packet Core
EPS	Evolved Packet System
EWMA	Exponential Weighted Moving Average
GERAN	GSM Edge Radio Access Network
GSM	Global System of Mobile communication
GUTI	Globally Unique Temporary Identifier
HD	Hellinger Distance
HeNB	Home e-NodeB
HMM	Hidden Markov Model
HSS	Home Subscriber Server
I-CSCF	Interrogating-Call Session Control Functions
IDR	Insert-Subscriber-Data-Request
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
ISIM	IMS Subscriber Identity Module
IWF	Interworking Function
kNN	k-Nearest Neighbor
LTE	Long Term Evolution
LTE-A	LTE-Advanced
MAC	Media Access Control
MITM	Man-In-The-Middle
MME	Mobility Management Entity
MR	Measurement Report
MSISDN	Mobile Station International Subscriber Directory Number
NAS	None Access Stratum
NCC	NH Chaining Counter
NH	Next Hop
P-CSCF	Proxy-Call Session Control Functions
PCFICH	Physical Control Format Indicator Channel
PBCH	Physical Broadcast Channel
PCRF	Policy and Charging Rules Function
PDN-GW	Packet Data Network Gateway
PDR	Packet Delivery Ratio
PRACH	Physical Random Access Channel
PSS	Primary Synchronization Signal
PUCCH	Physical Uplink Control Channel
QoS	Quality of Service
RAN	Radio Access Network

TABLE 2. *(Continued.)* **Abbreviations**

RF	Radio Frequency
RLF	Radio Link Failure
RN	Relay Node
RRC	Radio Resource Control
RTP	Real-time Transport Protocol
S-CSCF	Serving-Call Session Control Functions
SGW	Serving Gateway
SIP	Session Initiation Protocol
SMS	Short Messaging Service
SNR	Signal-to-Noise Ratio
SPIM	SPAM over Instant Messaging
SSS	Secondary Synchronization Signal
SVM	Support Vector Machine
TA	Tracking Area
TAU	Tracking Area Update
TD	Tanimoto Distance
UDR	User-Data-Request
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VoLTE	Voice over LTE
3GPP	3rd Generation Partnership Project

if there is any suspicion of a certain attack, a fine-grained analysis should be performed to make a concrete decision. In other words, there is a feedback mechanism between global analysis center and data collector, if the global analysis center detects certain abnormal traffic and suspects that there might be a certain type of attacks, it will send a request to the data collector, the data collector would adapt itself to collect more detailed data at a higher frequency to provide sufficient data for the purpose of detecting the suspected attacks. To our best knowledge, there is no prior work involves this feedback function. Once an attack is detected, the decision-making module must trigger the alarm module and execute a response plan. The global analysis center together with the response plan module makes up the data analysis layer.

D. SYSTEM SELF-GUARD LAYER

The top layer called system self-guard layer should be employed to guarantee the resilience of the security measurement system. Any failure in the components of the system or any attacks towards the system should not breakdown its availability. In a nutshell, the security measurement system must have its safeguard system to prevent malicious damage on it.

VII. CONCLUSION

In this survey, we first provided a brief overview of the LTE/LTE-A network architecture and its security mechanism. We then pointed out the vulnerabilities of the LTE/LTE-A network to various attacks due to its heterogeneity and all IP-based architecture. Furthermore, we discussed the attacks on the LTE/LTE-A network according to the network structure. We focused on the review of existing work related to data collection and analysis for the purpose of detecting main attacks on the LTE/LTE-A network. We presented our evaluation criteria and evaluated the current literature in order to highlight open issues and future research trends. Finally, we proposed an adaptive data collection and data analysis model towards security measurement in the LTE/LTE-A network.

APPENDIX

Table 2 lists the important abbreviations in this paper.

REFERENCES

[1] 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.
[2] Y. Park and T. Park, "A survey of security threats on 4G networks," in *Proc. IEEE GLOBECOM Workshops*, Nov. 2007, pp. 1–6.
[3] N. Seddigh, B. Nandy, R. Makkar, and J. F. Beaumont, "Security advances and challenges in 4G wireless networks," in *Proc. Int. Conf. PST*, 2010, pp. 62–71.
[4] 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.
[5] *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture Enhancement for Non-3GPP Accesses (Release 14)*, document 3GPP TS 23.402 V14.3.0, 2017.
[6] *3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description; Stage 2 (Release 14)*, document 3GPP TS 36.300 V14.1.0, 2016.
[7] *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 14)*, document 3GPP TS 33.401 V14.2.0, 2017.
[8] S. P. Rao, B. T. Kotte, and S. Holtmanns, "Privacy in LTE networks," in *Proc. EAI Int. Conf. Mob. Multimedia Commun. (ICST)*, 2016, pp. 176–183.
[9] S. Holtmanns, S. P. Rao, and I. Oliver, "User location tracking attacks for LTE networks using the interworking functionality," in *Proc. IFIP Netw. Conf. Workshops*, May 2016, pp. 315–322.
[10] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, 2014, pp. 246–255.
[11] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J. P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *Proc. NDSS*, 2016, pp. 21–24.
[12] D. Forsberg, H. Leping, K. Tsuyoshi, and S. Alanärä, "Enhancing security and privacy in 3GPP E-UTRAN radio interface," in *Proc. IEEE Int. Symp. Pers., Indoor Mobile Radio Commun*, Sep. 2007, pp. 1–5.
[13] 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. 7–20, 2014. [Online]. Available: https://doi.org/10.1186/1687-417X-2014-7
[14] 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.
[15] F. M. Aziz, J. S. Shamma, and G. L. Stüber, "Resilience of LTE networks against smart jamming attacks: Wideband model," in *Proc. IEEE Int. Symp. Pers., Indoor Mobile Radio Commun.*, Aug./Sep. 2015, pp. 1344–1348.
[16] 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.*, 2016, pp. 1–5.
[17] 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.

[18] R. P. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," in *Proc. Int. Symp. Wirel. Pers. Multimedia Commun.*, Jun. 2013, pp. 1–9.

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

[20] R. Bassil, A. Chehab, I. Elhajj, and A. Kayssi, "Signaling oriented denial of service on LTE networks," in *Proc. ACM Int. Symp. Mobility Manage. Wireless Access*, 2012, pp. 153–158.

[21] 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. MoWNeT*, 2013, pp. 30–35.

[22] P. Traynor *et al.*, "On cellular botnets: Measuring the impact of malicious devices on a cellular network core," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2009, pp. 223–234.

[23] 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.

[24] L. Qiang, W. Zhou, B. Cui, and L. Na, "Security analysis of TAU procedure in LTE network," in *Proc. Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.*, 2014, pp. 372–376.

[25] 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.

[26] S. Park, S. Kim, K. Son, and H. Kim, "Security threats and countermeasure frame using a session control mechanism on VoLTE," in *Proc. Int. Conf. Broadband Wireless Comput Commun. Appl.*, Nov. 2016, pp. 532–537.

[27] 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.*, Sep. 2015, pp. 442–450.

[28] J. Lee, K. Cho, C. Lee, and S. Kim, "VoIP-aware network attack detection based on statistics and behavior of SIP traffic," *Peer-to-Peer Netw. Appl.*, vol. 8, no. 5, pp. 872–880, Sep. 2015.

[29] G.-H. Tu, C.-Y. Li, C. Peng, Y. Li, and S. Lu, "New security threats caused by IMS-based SMS service in 4G LTE networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 1118–1130.

[30] S. Das, M. Pourzandi, and M. Debbabi, "On SPIM detection in LTE networks," in *Proc. IEEE Can. Conf. Elect. Comput. Eng.*, Apr./May 2012, pp. 12–15.

[31] C.-Y. Li *et al.*, "Insecurity of voice solution VoLTE in LTE mobile networks," in *Proc. CCS*, 2015, pp. 316–327.

[32] C. Peng, C.-Y. Li, H. Wang, G. H. Tu, and S. W. Lu, "Real threats to your data bills: Security loopholes and defenses in mobile data charging," in *Proc. CCS*, 2014, pp. 727–738.

[33] A. J. Alzahrani and A. A. Ghorbani, "SMS mobile botnet detection using a multi-agent system," in *Proc. Int. Workshop Agents CyberSecur.*, 2014, pp. 1–8.

[34] J. Hua and K. Sakurai, "A SMS-based mobile botnet using flooding algorithm," in *Proc. WISTP*, 2011, pp. 264–279.

[35] C. Mulliner and J.-P. Seifert, "Rise of the iBots: Owning a telco network," in *Proc. Int. Conf. Malicious Unwanted Softw.*, 2010, pp. 71–80.

[36] Y. Y. Zeng, "On detection of current and next-generation botnets," Ph.D. dissertation, Comput. Sci. Eng., Univ. Michigan, Ann Arbor, MI, USA, 2012.

[37] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proc. ACM CCS Workshop Secur. Privacy Smartphones Mobile Devices*, 2011, pp. 3–14.

[38] P. Yan and Z. Yan, "A survey on dynamic mobile malware detection," *Softw. Quality J.*, pp. 1–29, May 2017. [Online]. Available: https://link.springer.com/article/10.1007/s11219-017-9368-4, doi: 10.1007/s11219-017-9368-4.

[39] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2005, pp. 46–57.

[40] A. G. Fragkiadakis, V. A. Siris, and A. P. Traganitis, "Effective and robust detection of jamming attacks," *Future Netw. Mobile Summit*, 2011, pp. 1–8.

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

[42] J.-H. Bang, Y.-J. Cho, and K. Kang, "Anomaly detection of network-initiated LTE signaling traffic in wireless sensor and actuator networks based on a Hidden semi-Markov model," *Comput. Secur.*, vol. 65, pp. 108–120, Mar. 2017.

[43] A. Gupta, T. Verma, S. Bali, and S. Kaul, "Detecting MS initiated signaling DDoS attacks in 3G/4G wireless networks," in *Proc. Int. Conf. Commun. Syst. Netw.*, 2013, pp. 1–60.

[44] M. Pavloski, G. Görbil, and E. Gelenbe, "Bandwidth usage—Based detection of signaling attacks," *Inf. Sci. Syst.*, vol. 363, pp. 105–114, Sep. 2015.

[45] S. Wahl, K. Rieck, P. Laskov, P. Domschitz, and K. R. Müller, "Securing IMS against novel threats," *Bell Labs Tech. J.*, vol. 14, no. 1, pp. 243–257, 2009.

[46] M. Nassar, R. State, and O. Festor, "Monitoring SIP traffic using support vector machines," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*, 2008, pp. 311–330.

[47] D. Seo, H. Lee, and E. Nuwere, "SIPAD: SIP-VoIP anomaly detection using a stateful rule tree," *Comput. Commun.*, vol. 36, no. 5, pp. 562–574, Mar. 2013.

[48] S. Zhang, L. Zhou, M. Wu, Z. Tang, N. Ruan, and H. Zhu, "Automatic detection of SIP-aware attacks on VoLTE device," in *Proc. IEEE Veh. Technol. Conf.*, Sep. 2016, pp. 1–5.

[49] A. E. Ko, S. Park, S. Kim, K. Son, and H. Kim, "SIP amplification attack analysis and detection in VoLTE service network," in *Proc. Int. Conf. Inf. Netw.*, 2016, pp. 334–336.

[50] A. Mehta, N. Hantehzadeh, V. K. Gurbani, T. K. Ho, J. Koshiko, and R. Viswanathan, "On the inefficacy of Euclidean classifiers for detecting self-similar Session Initiation Protocol (SIP) messages," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage.*, May 2011, pp. 329–336.

[51] H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia, "Detecting VoIP floods using the Hellinger distance," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 6, pp. 794–805, Jun. 2008.

[52] J. Tang, Y. Cheng, and C. Zhou, "Sketch-based SIP flooding detection using Hellinger distance," in *Proc. IEEE GLOBECOM Conf.*, Nov./Dec. 2009, pp. 3380–3385.

[53] C. Hecht, P. Reichl, A. Berger, O. Jung, and I. Gojmerac, "Intrusion detection in IMS: Experiences with a Hellinger distance-based flooding detector," in *Proc. Int. Conf. Evolving Internet*, 2009, pp. 65–70.

[54] N. Chaisamran, T. Okuda, and S. Yamaguchi, "A proposal for anomaly traffic detection in the IP Multimedia Subsystem using Tanimoto distance and a modified moving average," in *Proc. SAINT*, 2012, pp. 278–283.

[55] Y. Rebahi, M. Sher, and T. Magedanz, "Detecting flooding attacks against IP Multimedia Subsystem (IMS) networks," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl.*, Mar./Apr. 2008, pp. 848–851.

[56] M. A. Akbar, Z. Tariq, and M. Farooq, "A comparative study of anomaly detection algorithms for detection of SIP flooding in IMS," in *Proc. Int. Conf. Internet Multimed Services Archit. Appl.*, Dec. 2008, vol. 66. no. 16, pp. 1–6.

[57] M. A. Akbar and M. Farooq, "Application of evolutionary algorithms in detection of SIP based flooding attacks," in *Proc. GECCO*, 2009, pp. 1419–1426.

[58] H.-J. Kim, M. J. Kim, Y. Kim, and H. C. Jeong, "DEVS-Based modeling of VoIP spam callers' behavior for SPIT level calculation," *Simul. Model. Pract. Theory*, vol. 17, no. 4, pp. 569–584, Apr. 2009.

[59] M. T. Nuruzzaman, C. Lee, and D. Choi, "Independent and personal SMS spam filtering," in *Proc. IEEE Int. Conf. Comput. Inf. Technol.*, Aug. 2011, pp. 429–435.

[60] C. Wang *et al.*, "A behavior-based SMS antispam system," *IBM J. Res. Develop.*, vol. 54, no. 6, pp. 3:1–3:16, Nov./Dec. 2010.

[61] A. Modupe, O. O. Olugbara, and S. O. Ojo, "Filtering of mobile short messaging service communication using Latent Dirichlet allocation with social network analysis," in *Power Technology and Engineering*, Dordrecht, The Netherlands: Springer, 2014, pp. 671–686.

[62] I. Vural and H. S. Venter, "Combating mobile spam through botnet detection using artificial immune systems," *J. Univ. Comput. Sci.*, vol. 18, no. 6, pp. 750–774, 2012.

[63] K. Yadav, P. Kumaraguru, A. Goyal, A. Gupta, and V. Naik, "SMSAssassin: Crowdsourcing driven mobile-based system for SMS spam filtering," in *Proc. Workshop Mobile Comput. Syst. Appl.*, 2011, pp. 1–6.

[64] Z. Bin *et al.*, "Behavior analysis based SMS spammer detection in mobile communication networks," in *Proc. IEEE DSC*, Jun. 2016, pp. 2–7.

[65] G. Liu and T. J. Lu, "Research on an effective rubbish short message inspection system and its optimization," in *Proc. WiCOM*, 2008, pp. 4–7.

[66] B. Coskun and P. Giura, "Mitigating SMS spam by online detection of repetitive near-duplicate messages," in *Proc. IEEE ICC*, Jun. 2012, pp. 999–1004.

[67] L. Chen, Z. Yan, W. Zhang, and R. Kantola, "Implementation of an SMS spam control system based on trust management," in *Proc. IEEE Int. Conf. Green Comput. Commun.*, Aug. 2013, pp. 887–894.
[68] M. Oulehla, Z. K. Oplatková, and D. Malanik, "Detection of mobile botnets using neural networks," in *Proc. FTC*, 2017, pp. 1324–1326.
[69] A. J. Alzahrani and A. A. Ghorbani, "Real-time signature-based detection approach for SMS botnet," in *Proc. Int. Conf. PST*, 2015, pp. 157–164.
[70] E. Johnson and I. Traore, "SMS botnet detection for Android devices through intent capture and modeling," in *Proc. IEEE Symp. Rel. Distrib. Syst. Workshop*, Sep./Oct. 2015, pp. 36–41.
[71] I. Vural and H. Venter, "Mobile botnet detection using network forensics," in *Proc. FIS*, 2010, pp. 57–67.

LIMEI HE received the B.Sc. degree in electronic information science and technology from Tianjin Normal University, Tianjin, China, in 2016. She is currently pursuing the master's degree with the State Key Laboratory on Integrated Services Networks, Xidian University. Her main research directions are security measurement in the LTE/LTE-A network and anonymous authentication in pervasive social network.

ZHENG YAN (M'06–SM'14) received the B.Eng. degree in electrical engineering and the M.Eng. degree in computer science and engineering from the Xi'an Jiaotong University, Xi'an, China, in 1994 and 1997, respectively, the second M.Eng. degree in information security from the National University of Singapore, Singapore, in 2000, and the Licentiate of Science degree and the Doctor of Science degree in technology in electrical engineering from the Helsinki University of Technology, Helsinki, Finland. She is currently a Professor with the Xidian University, Xi'an, and a Visiting Professor with the Aalto University, Espoo, Finland. Her research interests are in trust, security and privacy, social networking, cloud computing, networking systems, and data mining. She serves as an organization and program committee member for over 70 international conferences and workshops. She is also an Associate Editor of many reputable journals, e.g., the IEEE IoT Journal, *Information Sciences*, *Information Fusion*, JNCA, the IEEE Access, and SCN.

MOHAMMED ATIQUZZAMAN (M'88–SM'94) received the M.S. and Ph.D. degrees in electrical engineering and electronics from The University of Manchester, U.K. He currently holds the Edith Kinney Gaylord Presidential Professorship with the School of Computer Science, The University of Oklahoma. His research interests are in communications switching, transport protocols, wireless and mobile networks, satellite networks, and optical communications. His research has been funded by the National Science Foundation, NASA, U.S. Air Force, Cisco, Honeywell, and other funding agencies. He has co-chaired numerous IEEE international conferences, including the IEEE Globecom. He is the Editor-in-Chief of the *Journal of Networks and Computer Applications* and a Founding Editor-in-Chief of *Vehicular Communications*. He has served/serving on the editorial boards of various IEEE journals.