Detecting Signalling DoS Attacks on LTE Networks

Ginés Escudero-Andreu[1(✉)], Konstantinos Kyriakopoulos[1,2], James A. Flint[1], and Sangarapillai Lambotharan[1]

[1] Wolfson School of Engineering, Loughborough University, Loughborough LE11 3TU, UK
{g.escudero-andreu,k.kyriakopoulos,j.a.flint,s.lambotharan}@lboro.ac.uk
[2] Institute for Digital Technologies, Loughborough University London, London E15 2GZ, UK

Abstract. As mobile communications increase their presence in our life, service availability becomes a crucial player for the next generation of cellular networks. However, both 4G and 5G systems lack of full protection against Denial-of-Service (DoS) attacks, due to the need of designing radio-access protocols focused on providing seamless connectivity. This paper presents a new method to detect a DoS attack over the Radio Resource Control (RRC) layer, offering three original metrics to identify such attack in a live Intrusion Detection System (IDS). The proposed metrics evaluate the connection release rate, the average session establishment and the session success rate to identify the attack. The presented results provide an average detection rate above 96%, with an average false positive rate below 3.8%.

Keywords: LTE security · DoS attacks · RRC signaling attack · Dempster-Shafer

1 Introduction

The 4$^{\text{th}}$ Generation (4G) of mobile cellular networks has been designed to provide high-speed access to broadband mobile services even in the worse scenarios, such as high mobility scenarios, overcrowded cells or rural areas; without detriment to the *Quality-of-Service* (QoS). Additionally, 4G systems are expected to provide safe communications among a huge number of cellular users, which is growing constantly every year.

The major contribution of the 4G is the portability of the entire network architecture into a flat, all-IP infrastructure where all the services are provided over IP networking and circuit switching is no longer used. This improvement facilitates easy mobility among different radio-access technologies, such as

This work has been supported by the Gulf Science, Innovation and Knowledge Economy Programme of the UK Government under UK-Gulf Institutional Link grant IL 279339985.

T. Q. Duong et al. (Eds.): INISCOM 2019, LNICST 293, pp. 283–301, 2019.
https://doi.org/10.1007/978-3-030-30149-1_23

Worldwide Inter-operability for Microwave Access (WiMAX), *Wireless Fidelity* (WiFi), *Global System for Mobile communications* (GSM) or *Universal Mobile Telecommunications System* (UMTS), besides making easy backward compatibility with previous technologies.

However, compatibility with heterogeneous access technologies, which are provided by multiple *Mobile Network Operators* (MNOs), produces an increase in the number of Radio Access Network (RAN) hangovers. The main consequence of this effect is the mandatory negotiation of strict security policies between the MNOs with the purpose of defining trust policies and authorize users' migration, as well as defining secure countermeasures against identified vulnerabilities.

Since the first release of the 3^{rd} *Generation Partnership Project* (3GPP) for the Long Term Evolution (LTE) standard, several publications have pointed out important shortcomings with regards to the security capabilities of this technology [1–4]. Most of the weaknesses were identified in the RAN, which is the most vulnerable part of the entire system due to its wireless nature and attacks can be easily performed remotely without having physical access to the infrastructure (Fig. 1).

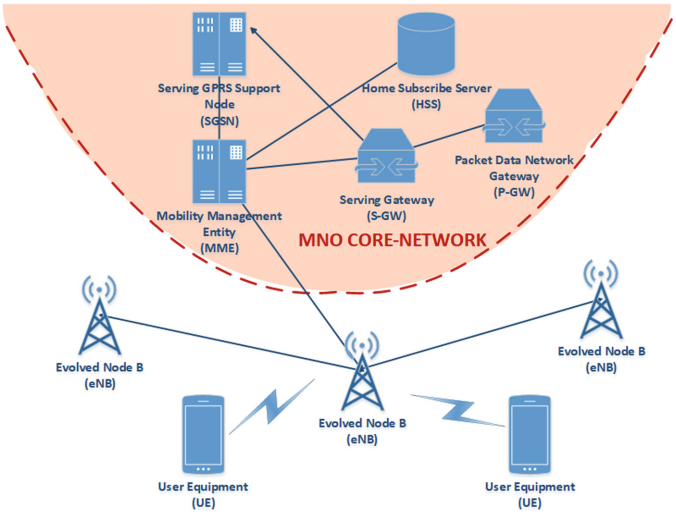

Fig. 1. LTE End-to-End network architecture

The security capabilities of LTE to protect the radio link are based in predefined secure domains with limited scopes and security contexts associated to each user, which are established during the user attachment procedure. The security context enables the encryption of the communications and is built based on a master key, K, previously shared between the mobile operator and the UE. Additional keys are dynamically computed on every session to guarantee their freshness, protecting the master key from being directly used.

The procedure in which the session keys are derived is called EPS-AKA [5], or Authentication and Key Agreement Protocol for *Evolved Packet System*, and it is triggered during the initial attachment of the mobile device. The EPS-AKA protocol plays an important role into the establishment of an initial security context for each user. At the same time, it exhibits most of the identified vulnerabilities of LTE, such as breach of privacy for the user's identity, weak mutual authentication between core-network elements or lack of perfect forward secrecy into the key hierarchy [6].

The AKA protocol has been redefined in recent specification drafts [7,8] for the 5th Generation (5G) of mobile communications, to enhance the privacy for the identity of the mobile subscriber. The *International Mobile Subscriber Identity* (IMSI) has been replaced by the *Subscriber Permanent Identifier* (SUPI), which should never be transferred through the radio channel.

Instead, an encrypted version of it is used as identifier, named as *Subscription Concealed Identifier* (SUCI). However, the 3GPP recognises several scenarios in which the privacy of the SUPI cannot be guaranteed [7]. Specifically, during the execution of any emergency services and/or whenever the Mobile Equipment (ME) is in use of the null-scheme, as the home network has not provisioned the Home Network Public Key in the *Universal Subscriber Identity Module* (USIM). These two exceptional cases make the next generation of cellular networks also vulnerable against the aforementioned DoS attack over the RRC layer.

This paper focuses in the detection of a particular vulnerability of the EPS-AKA protocol which allows the attacker to perform a DoS attack against the core network. Section 2 describes the vulnerability itself, how LTE networks are secured and a description on how to perform a local DoS attack over the *Radio Resource Control* (RRC) layer. Section 3 presents the detection methodology, defines the metrics proposed to detect the attack and explains the application of Dempster-Shafer theory [9] as a data fusion technique. Section 4 presents the experimental environment and Sect. 5 presents and evaluates the results. Finally, conclusions and future work are stated in Sect. 6.

2 Background Work

Looking at the work carried out by the research community, two main research areas are clearly defined: the identification and impact assessment of the studied signalling DoS attack, and the enhancements on the AKA mechanism.

The first publication acknowledging the studied signalling DoS attack was presented in [2], where the authors described the entire process of launching the attack. First, the UE is lured to transmit the IMSI value instead of using the temporary identity. This action allows the attacker to gather the required list of legitimate IMSIs, and finally perform the signalling attack as explained in Sect. 2.2.

Other signalling DoS and intelligent jamming attacks have been identified on LTE networks [10,11], exploiting the initial allocation of radio bearers to exhaust the resources within the radio cell and disrupt the service. The authors

in [10] successfully managed to replicate the attack in an OPNET simulator, and provide a detection mechanism without evaluating its performance thoroughly. However, such type of attacks go beyond the scope of this work, which focuses only on DoS attacks above the physical layer.

The other area of research has focused on improving the existing AKA mechanism proposed by the 3GPP. The disclosure of the IMSI during the initial UE attachment to the RAN is the main vulnerability exploited for performing DoS attacks [12] in LTE networks.

The research community has proposed interesting solutions to deal with this shortcoming, proposing a list of amendments on the original AKA protocol. The author in [13] enhanced the AKA mechanism to provide mutual authentication between RAN and UE. The protocol includes a new concept of USIM card [13], called *Enhanced Subscriber Identity Module* (ESIM), which is capable of computing pseudo-random values. The new feature enables the generation of challenge requests inside the UE, which are used to confirm the identity of the serving network. However, this proposal adds additional computational load to the original radio access mechanisms, and imposes further challenges when maintaining compatibility with legacy systems.

The authors in [12] modified the security architecture to act as a wireless public key infrastructure and used digital certificates to confirm identity. The certificates have to be provided in advance to all involved entities in the authentication process, to be able to gain access to the radio system. This requirement makes more difficult the actual implementation on a real LTE deployment.

A more robust solution is introduced in [14,15] that combines passwords with fingerprints and public keys to provide full mutual authentication. Unfortunately, the high computational cost to execute the Diffie-Hellman key agreement and mutual authentication, and the requirement of storing biometric parameters, make its implementation less viable in a commercial deployment.

Due to the aforementioned inconveniences, the authors of this paper believe that further research is required to improve the existing LTE standard without actually modifying the specification documents. A detection mechanism is proposed to provide security against signalling DoS attacks while still transferring the IMSI in clear-text whenever the use of temporary identities is not possible.

2.1 Authentication and Key Agreement (AKA) Preliminaries

User identification is the first step before gaining access to the network, as shown in the blue section of Fig. 2. UE establishes contact with the nearest *evolved-Node B* (eNB) triggering the registration process. During the first attempt, there is no *Globally Unique Temporary Identity* (GUTI) available for the UE to be identified by the *Mobile Management Entity* (MME). Therefore, the MME sends a User Identity Request message.

A reply message is made by the *Mobile Equipment* (ME) with its IMSI transferred in clear text, because no security context has been established before. This action, does not comply with the user identity confidentiality requirements [16], which exposes the user identity to eavesdropping attacks over the radio interface.

Once the MME receives the User Identity Response, a GUTI is allocated and paired with the corresponding IMSI. The Temporary Mobile Subscriber Identity (TMSI) may change due to different reasons, being no necessary to transfer the IMSI unless serving network can not retrieve a new TMSI from the GUTI.

Before the establishment of a security context, mutual authentication between the ME and the UE is achieved using the EPS-AKA protocol [5]. The process is triggered by the MME, after the user is successfully identified. Figure 2 shows the sequence diagram.

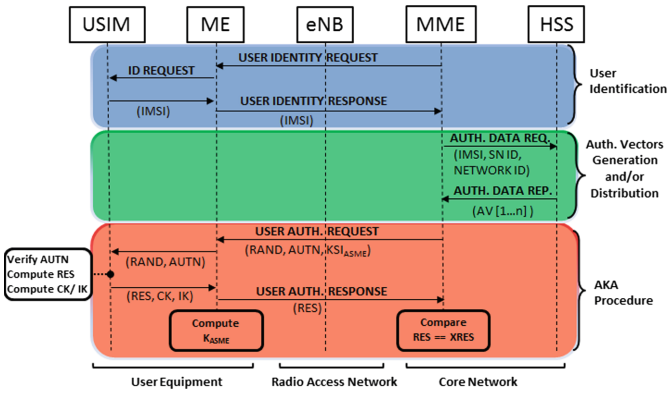

Fig. 2. Authentication sequence during EPS-AKA (Color figure online)

During the *Authentication Vector* (AV) generation phase, i.e. green section of Fig. 2, the MME checks the stored key material and its freshness. If there is any AV available, it will be used to start the authentication process. Otherwise, MME requests new AVs from the *Home Subscriber Server* (HSS). Whenever the HSS has no available AVs, 3GPP specifies [5] that multiple vectors should be computed and stored for future use, increasing the computational load in the core network. Each AV is composed according to the equation

$$AV := RAND \parallel AUTN \parallel XRES \parallel K_{ASME} \tag{1}$$

where:

RAND is the challenge to prove the user authenticity.
AUTN is the parameter to prove freshness of authentication vector and serving network authenticity.
XRES is the expected response to the challenge.
$\mathbf{K_{ASME}}$ is an identifier to derive the same key hierarchy in both end points.

The AKA process starts with a User Authentication Request message, composed of three parameters: RAND, AUTN and KSI_{ASME}, the Key Session Identifier used by the ME to generate the same key value for K_{ASME}.

Once the ME receives the message, it retrieves the KSI_{ASME} parameter and passes the other parameters to the USIM. The USIM verifies the freshness of the authentication vector, deriving the sequence number from the AUTN parameter. If the derived value matches with the expected sequence, a challenge response RES is computed and sent back to the UE. Then, two keys are derived from the master key K, one for integrity (IK) and another for confidentiality (CK).

A User Authentication Response is sent back to the MME, generating on it the same key pairs CK/IK and completing the AKA process. Now, both end points are able to generate the same key material following the scheme of Fig. 3.

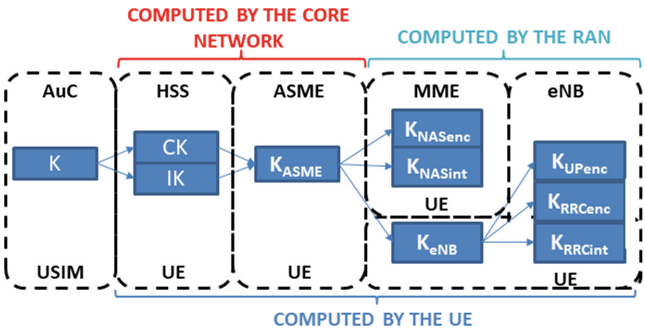

Fig. 3. Key hierarchy for E-UTRAN

Each time an AKA process is called, key material is re-generated based on the new value of K_{ASME}. Master key K is securely stored in the HSS and IMSI, without being transmitted or used directly. It is only used to derive the entire key hierarchy.

2.2 RRC Signalling Attack

The attack exploits a vulnerability in the specifications of the RRC layer [17], which is the third level of the *Open Systems Interconnection* (OSI) model [18], shown in Fig. 5. The attack was originally identified in [2], and subsequently acknowledged in several publications, such as [19–21].

In [2], the authors performed a simulation with the purpose of getting measurements to assess the impact of the attack inside the core network. The results conclude that there is no requirement of having high-computational hardware in order to perform this attack, since it can easily be launched by using a non-sophisticated equipment, such as a normal desktop PC. The attack is able to collapse the system in just 30 s by using a number of previously gathered legitimate IMSI values which are leveraged to send 500 service requests per second, following a Poisson distribution [2].

The aim of this attack is to consume available resources inside the core network by flooding the system with radio service requests which contain previously collected, legitimate IMSIs. Initially, the malicious user retrieves legitimate user identities or IMSI from the radio channel by luring the user to connect to a rogue MME and force the transmission of the IMSI with an *Identity Request* message. The approach to gather all IMSI is widely explained in [23].

Once the attacker has collected enough number of legitimate identities to perform the attack, it is ready to initiate it by sending *RRCConnectionRequest* spoofed messages including one of the eavesdropped IMSIs within each request. MME receives the service request and retrieves an authentication vector from the HSS. Because there is no means to identify the injected messages as illegitimate, the authentication process continues with both MME and HSS validating the user identity by checking the value of the IMSI.

MME sends a *RRCConnectionSetup* message and launches a timer while awaiting for a *RRCConnectionSetupComplete* message, which never arrives. Once the timer is expired, the authentication session is cancelled and all the occupied resources are released. HSS requires to consume hardware resources, such as RAM memory and CPU usage, in order to compute each authentication vector, as well as for storing the derived session keys until the authentication session is completed or fails. The attacker only has to simultaneously initiate a limited number of *RRCConnectionRequest* in order to exhaust the available resources of the HSS and collapse the cell service completely.

In conclusion, this attack has a twofold impact on the system performance. First, legitimate users are unable to connect to the network, since the available resources are depleted by the attacker. Secondly, by serving multiple spoofed service requests, the core network is collapsed. The collapse occurs due to a heavy computing load registered on the HSS to generate and distribute the authentication vectors (Fig. 4).

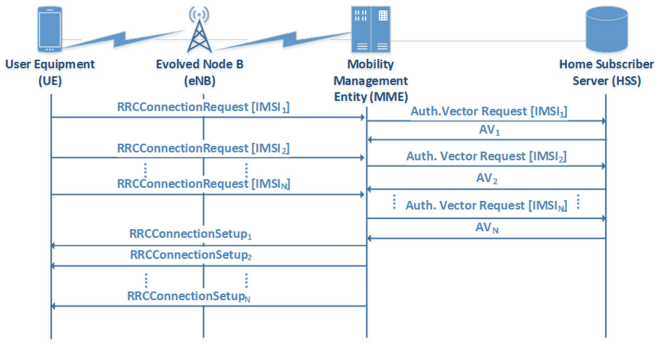

Fig. 4. Data-flow diagram of a DoS attack over the RRC layer.

3 Detection Methodology

3.1 Proposed Metrics

Three metrics are proposed in this work that have been specially designed to expose the characteristics of the examined signalling DoS attack. To the best of the authors' knowledge, this is the first proposed methodology for detecting such attack and the main contribution of the work presented on this paper. All the novel metrics used for detecting the signalling DoS attack are extracted from the same layer, the RRC layer [16] and are presented below.

Connection Release Rate (CRR). Since the attacker will never be able to successfully complete the authentication phase, the RRC connection will be closed with a rrcConnectionRelease message sent by the base station. Because the RRC connectivity remains active, this would never occur under normal circumstances, unless the node is experiencing handover. The CRR is given by

$$CRR(x) = \frac{\#CR_X}{\Delta T} \tag{2}$$

where CR_x is the number of Connection Request messages on the current sliding window, x, and ΔT is the duration of the window.

Average RRC Session Establishment (SMT). A UE is considered to have established an RRC session once it is able to allocate a radio link to initiate the RRC authentication phase. This metric evaluates the frequency of established RRC sessions within a certain period of time, x. During the attack, all the attacking nodes will trigger a new RRC session establishment every time the eNB rejects the previous request due to an incorrect challenge response or due to a master key mismatch. Additionally, legitimate session establishments might be triggered on already established RRC sessions whenever the MME decides to reconfigure the link by reassigning a new bearer or changing any additional parameter previously negotiated. As a result, this negatively impacts

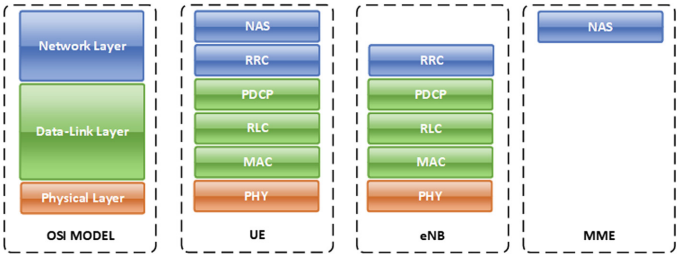

Fig. 5. Protocol stack for LTE control plane traffic [22] against OSI model [18]

the effectiveness of this metric to distinguish between rogue and legitimate node behaviour.

$$ASE(x) = \frac{\sum SE_X}{n^2} \tag{3}$$

where SE_x is the average Session Establishment duration for the sliding window x and n is the number of established sessions within the sliding window.

Session Success Rate (SR). This metric evaluates the number of successful RRC sessions established between each node and the serving eNB. Since the attacker nodes will not be able to complete any RRC session establishment, this metrics is expected to positively characterise the attack and reduce the uncertainty.

$$SSR(x) = \sum_{0}^{x} \frac{\#AA - \#AF}{\#CR} \tag{4}$$

where $\#AA$, $\#AF$, $\#CR$ are the number of Attach Accepted, Attach Failure and total number of Connection Request messages for the current window, x, respectively.

3.2 Dempster-Shafer Theory

The *Dempster-Shafer* (D-S) theory of evidence [9] is used to fuse the evidence collected from the proposed metrics. The D-S theory starts by defining a Frame of Discernment, which is a finite set of all possible, mutually exclusive propositions about a specific problem domain. In our case, a frame in the LTE network might either be normal or malicious (attack) and this is represented as: $\Theta = \{N, A\}$. Θ is also exhaustive, which means that one proposition from the set has to be true.

Given a Frame of Discernment, any hypothesis or proposition, A, is an element of the power set $P(\Theta)$ with $|P(\Theta)| = 2^{\Theta}$. Note that the power set contains all possible subsets of Θ, including the empty set ($\varnothing$) and the universal set, i.e. the Frame of Discernment, Θ, itself. Thus, the formula to represent the power set is as follows: $P(\Theta) = \{N, A, \{N, A\}, \varnothing\}$. In the case where a hypothesis has only one element, i.e. no subsets, it is referred to as a *singleton*. In our case, hypotheses A and N are singletons. However, {A, N} is not singleton as it has A and N as subsets.

In Bayesian probability theory, all hypotheses are singletons. However, this is not necessary in the theory of evidence. As a consequence, in the case of assigning belief towards a non singleton hypothesis, $H \subseteq \Theta$, there is no explicit commitment of belief towards a subset of H, $A \subseteq H$. Thus, the theory of evidence gives the freedom to explicitly assign belief to uncertainty. For example, by assigning a belief value to {A, N}, there is no explicit information on whether A is more probable than N [24]. As a result, the additivity rule is no longer required. In other words, in the theory of evidence framework, the belief in a

hypothesis and its complement can be less than one, i.e. $Bel(H) + Bel(\neg H) \leq 1$ [24].

Each proposition from the Frame of Discernment, $H \subseteq \Theta$, is assigned a belief value within the range [0, 1] through a mass probability function, $m : 2^{\Theta} \rightarrow [0, 1]$.

The mass function, also known as basic probability assignment or basic belief assignment, follows the following three conditions [9]:

$$\sum_{H \subseteq \Theta} m(H) = 1 \tag{5}$$

$$m(H) \geq 0, \forall H \subseteq \Theta \tag{6}$$

$$m(\varnothing) = 0 \tag{7}$$

where:

$m(H)$ is the the amount of belief strictly supporting hypothesis H.
$m(\varnothing)$ is the probability of the empty set, which is equal to zero for a normalised mass function.

Once a mass value has been assigned for all the hypotheses, the rule of combination [9] defines the method to combine evidence from multiple observers about the same hypothesis. The fuse of evidences is only possible whenever all the observers are facing the same problem and set of hypotheses. In essence, this condition requires all the observers to share the same Frame of Discernment.

The rule of combination is applied to fuse the beliefs of two independent observers into a common belief, and it is defined by the following formula:

$$m_{comb}(H) = \frac{\sum_{X \cap Y = H} = m_1(X) * m_2(Y)}{1 - \sum_{X \cap Y = \varnothing} = m_1(X) * m_2(Y)} \forall H \neq \varnothing \tag{8}$$

where:

$m_{comb}(H)$ is the combined belief, by two independent observers, supporting the hypothesis H.
X, Y correspond to any supported hypothesis by observers 1 and 2 respectively.
$m_1(X)$ is the probability supporting hypothesis X as perceived by observer 1.

3.3 Detection Framework

All the necessary information required to detect the signalling DoS attack is extracted from captured traffic by constantly monitoring the network activity. Figure 6 presents the general view of the entire detection process, which is composed of four main phases.

The monitoring phase applies to the OSI model of the protocol stack and is represented in the left most side of Fig. 6. The selected LTE metrics, indicated

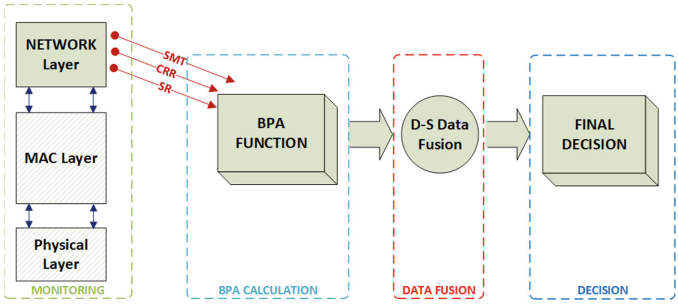

Fig. 6. General view of the detection process (Color figure online)

in red colour, are extracted from the Network layer. The output from this phase is a single buffer containing the individual samples of each monitored metric.

The *Basic Probability Assignment* (BPA) computation phase is responsible for calculating the beliefs for each of the hypotheses composing the power set in the D-S framework. To this end, using a sliding window of an experimentally selected [25], pre-defined size of 30 samples, the statistical BPA parameters are calculated during each time window, as described in [26]. These parameters, along with the actual metric samples extracted from each frame are introduced into the BPA function. The output of this phase is three distinct buffers containing a triplet set of BPA values, one for each hypothesis, per metric.

During the data fusion phase, the individual buffers obtained during the BPA computation phase are iteratively fused, using the D-S rule of combination (E.q. 8), treating each metric as an independent source of information and fusing them in pairs. The final output of this procedure is a triplet of beliefs for each frame, containing the beliefs for the three hypotheses.

Finally, in the decision phase, the resulting, per frame, fused beliefs for Attack, Normal and Uncertainty are received. The hypothesis with the highest probability is selected as the final decision. In the case where the Attack and Normal probabilities are equal, the decision of Normal is chosen. To the best of the authors' knowledge, the work presented on this paper is the first application of D-S theory for detecting DoS attacks on LTE networks.

4 Experimental Environment

4.1 Generating and Collecting the Data

This research project was initially focused on implementing the selected DoS attack within a simulated environment, aiming at verifying its feasibility beyond the theoretical approach, and evaluating its impact on the core-network components. Using OPNET Modeler Suite ver. 17.5, it was possible to confirm the side effects that running the *Radio Resource Control* (RRC) signaling attack could inflict on the *Home Subscriber Server* (HSS). Figure 7 shows the *Central Processing Unit* (CPU) utilisation registered in the HSS, where the attack was able

to saturate the resources in a short period of time. Once the attack was stopped after 4 min, the system quickly recovered back to its normal behavior.

During this simulation, the attacker node was sending 500 RRC Connection Request messages per second using different IMSI values, forcing the MME to compute all the required cryptographic material to challenge the UE and authenticate it. However, OPNET Modeler ver. 17.5 was not able to provide real traffic captures to be used when evaluating the proposed metrics to detect the attack. The LTE modules were in an early stage and there were not plans in the development pipeline to implement the additional traffic information for the lower layers in the protocol stack, which was the main interest of this research project.

Due to the limitations with OPNET, a physical test-bed was designed using hardware-based emulating equipment, as discussed below, to run the required application-level services, and the core components composing a 4G deployment: Evolved Packet Core (EPC) entities, *Mobile Management Entity* (MME), *evolved-Node B* (eNB) and UE/s. The final architecture of the test-bed is displayed in Fig. 8 and includes the following components:

App Traffic Generator. The network traffic was managed in a Lenovo ThinkCentre M73 Tiny Desktop PC, equipped with an Intel Core i3-4130T Processor (2.9 GHz), 8 GB RAM and Windows 7 Pro 64 bits. This host was configured to run an FTP server with Microsoft IIS 6.0, allowing the UEs to perform file downloading via FTP to keep a continuous data flow throughout the duration of the emulation session.

eNode-B. The RAN infrastructure was emulated using an LTE Enterprise Femtocell board, manufactured by Mindspeed with model number M84300, including a Transcend T3310 chipset for implementing all the standard LTE modulation schemes. The femtocell station was configured to have 3 sectors, requiring only one sector to create a single cell for covering all the UEs required for conducting the experiments.

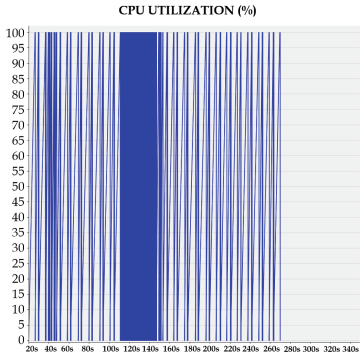

Fig. 7. CPU utilisation registered in the MME with 500 req/s

All the communications between the femtocell and the UE emulator were performed with wired connections and physical signal fading emulators, able to reproduce multiple radio path-loss schemes for signal attenuation. Free-space path-loss scheme was selected for this test-bed, making the UE emulator responsible for implementing the urban path-loss attenuation prediction on the registered radio measurements.

Evolved Packet Core (EPC). A single Aeroflex PXI 3000 modular platform was equipped with the Aeroflex LTE Base Station RF Measurements modules for providing the EPC capabilities to the test-bed. The equipment was configured to use FDD modulation for both downlink and uplink. All the UEs were registered in the HSS with the same master key, to reduce the computational complexity of each experiment.

UE Emulator. The UE emulation was managed in an Aeroflex E500 Network Tester, able to emulate the behaviour of up to 4000 UEs with the configuration used on this test-bed: 4 x Aeroflex TM500 modules interconnected to each other. The attacker's UEs were configured with an incorrect master key, forcing the unsuccessful authentication against the core network in the same manner the attack would occur in real life.

The data traffic load was generated on the UE side using a Spirent C50 TestCenter, model number C50-KIT-04-START, with 4-port 10/1 Gbps Ethernet SFP able to manage a volume of up to 40 Gbps. The TM500 was configured to emulate different groups of malicious and legitimate UE nodes, as described in Table 1.

4.2 Scenario Definition

The proposed LTE scenario complexity is a reduced representation of a commercial deployment. Specifically, the test-bed scenario is mainly composed of an LTE emulated eNB connected to an emulated LTE core network. During the RRC signalling attack implementation, there are two types of UE nodes; legitimate and rogue UEs. Both types of UEs are registered in the HSS as active subscribers. However, legitimate UEs use a valid master key (K) value, while rogue UEs have been configured with an incorrect K value, which forces a failure during the establishment of the RRC session.

In a real-life attack, the attacker would perform exactly the same actions, as the only information under its control would be the IMSI value of legitimate UEs, but it would not be able to compromise the private master key (K) associated to every mobile subscriber. Since the aim of a malicious user is to disrupt the service in the most efficient manner, the attacker's effect was replicated by multiple sets of rogue UEs acting as a single attacker node. Configuring multiple rogue UEs that attempt to establish RRC sessions in parallel, it is possible to reproduce the equivalent network traffic volume that would be produced by a single attacking UE targeting a commercial LTE cell.

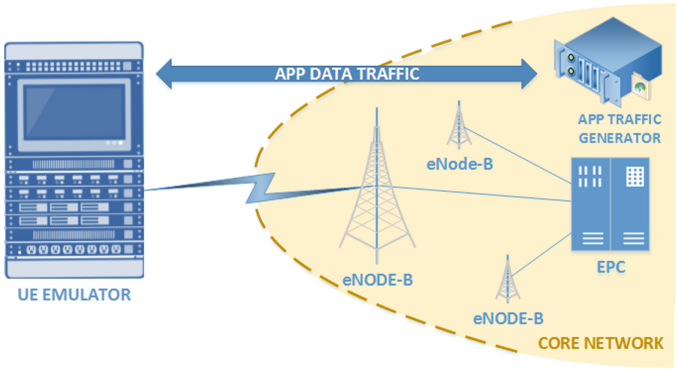

Fig. 8. LTE Test-bed architecture

Table 1. Emulation Scenarios for LTE experiments

Properties	Scenario 1	Scenario 2	Scenario 3
Legitimate UEs	200	50	200
Rogue UEs	200	450	200
Initial, attack phase	30 s	300 s	300 s
Final phase	95 s	221 s	431 s
Total duration	2 min 35 s	13 min 41 s	17 min 11 s

The ratio between legitimate and rogue nodes has been modified across the three scenarios, as described in Table 1 to evaluate the impact on core equipment when the rogue traffic load is equal (Scenarios 1 and 3) and higher (Scenario 2) than the traffic generated by the legitimate UEs. The simulation of the attack is composed by three phases: *initial phase*, where the legitimate nodes are activated; *attacking phase*, when the attacking nodes are activated in parallel to the existing legitimate nodes; and *final phase*, when the attacking nodes are deactivated to recover the normality on the network.

The duration of initial and attacking phases is set to 30 seconds for the Scenario 1, and 5 min for Scenarios 2 and 3; whereas the duration of the final phase varies on each scenario. Moreover, the time allocated to the initial and attacking phases includes the time required for initiating the legitimate and malicious UEs, having a gradual increase in the cellular network traffic received at the eNB.

5 Result Evaluation

The evaluation of the results have been conducted using the evaluation metrics of *Detection Rate* (DR), *False Positive Rate* (FPR) and *False Negative Rate* (FNR). The DR, also known as Recall, indicates the proportion of malicious frames

detected in comparison with the total number of frames emitted by the attacker. This parameter offers a clear indication of how efficient the detection algorithm is. However, this value is not able to provide a fair assessment of the detection performance by itself and could lead to an error when analysed individually, since it does not take into account the negative effects of misclassifying malicious frames as normal (FN), or when a false alarm is raised (FP) as result of applying the detection algorithm.

$$DR = \frac{TP}{TP + FN} \tag{9}$$

$$FPR = \frac{FP}{TotalFrames} = \frac{FP}{TP + FP + TN + FN} \tag{10}$$

$$FNR = \frac{FN}{TP + FN} \tag{11}$$

This information has a direct impact onto the overall detection performance and must be taken into account when analysing the performance. Looking at the test evaluation in pattern recognition theory [27] and *Intrusion Detection System* (IDS) [28], it is possible to judge the performance in a more complete manner by evaluating the *Overall Successful Rate* (OSR), also known as accuracy, which takes into account the correctly classified frames against the total population. In addition, we calculated the *Precision* (P), which evaluates the number of frames correctly classified as malicious among the total number of frames classified as malicious by the algorithm and the F_1-Score, which is the harmonic mean of the DR and Precision, and evaluates the balance between these two parameters.

$$OSR = \frac{TP + TN}{TP + FP + TN + FN} \tag{12}$$

$$P = \frac{TP}{TP + FP} \tag{13}$$

$$F_1 - SCORE = \frac{2 * P * DR}{P + DR} \tag{14}$$

The above parameters are used to evaluate the results and obtain the research findings from the experiments, which are discussed in the section below and presented in Table 2.

5.1 Research Findings

The LTE experiments confirm the accuracy of the proposed metrics to detect the attack, no matter if they are used individually or as part of a set of metric combinations. Notably, if the individual performance of each metric is analysed, the CRR metric performs the strongest in detecting the attack, with a DR higher than 98% for all three scenarios presented in this paper. This is expected because the DoS attack creates an unusually large number of RRC Connection Requests, which might end up with a RRC Connection Release message when the attacker's requests are rejected.

Table 2. Results collected on LTE experiments (in percentage)

Scenario#	DR	OSR	FNR	FPR	Precision	F_1-Score	Metrics
1	98.095	87.227	1.904	11.526	84.774	90.949	CRR
1	97.143	74.143	2.857	23.988	72.598	83.096	CRR, SMT
1	96.190	97.508	3.809	0	100.00	98.058	CRR, SR
1	88.571	80.997	11.429	11.526	83.408	85.912	CRR, SMT, SR
1	84.762	66.044	15.238	23.988	69.804	76.559	SMT
1	83.810	89.408	16.190	0	100.00	91.192	SR
1	82.857	88.785	17.143	0	100.00	90.625	SMT, SR
2	100.00	100.00	0	0	100.00	100.00	CRR, SR
2	98.814	98.862	1.186	0	100.000	99.403	CRR
2	97.536	97.548	2.463	0.087	99.907	98.707	SMT
2	97.536	97.548	2.463	0.087	99.907	98.707	CRR, SMT
2	97.536	97.548	2.463	0.087	99.907	98.707	CRR, SMT, SR
2	96.989	97.023	3.010	0.087	99.906	98.426	SMT, SR
2	95.803	95.972	4.197	0	100.000	97.857	SR
3	99.915	98.011	0.084	1.917	97.765	98.828	CRR
3	99.915	98.011	0.084	1.917	97.765	98.828	CRR, SR
3	93.401	93.608	6.599	0.852	98.925	96.084	SMT
3	93.401	93.608	6.599	0.852	98.925	96.084	CRR, SMT
3	93.401	93.608	6.599	0.852	98.925	96.084	CRR, SMT, SR
3	79.272	81.747	20.728	0.852	98.736	87.940	SMT, SR
3	0.423	16.406	99.577	0	100.00	0.842	SR

However, to provide robustness to the detection algorithm, other metrics should be taken into account because normal network behaviour might also manifest with a high number of RRC Connection Requests. This could happen, for example, in the case of congested LTE cells without enough radio spectrum to cope with the demand. Under such circumstances, the individual analysis of the CRR would feed misleading information into the detection algorithm, necessitating to weigh in additional information captured by the SMT and SR metrics.

The best overall performance is obtained in Scenario 2, with the metric combination (CRR, SR), where every frame is correctly classified and all evaluation metrics reach their highest value. The DR, OSR, Precision and F_1-Score reach 100%. This result is specially important because Scenario 2 was specifically designed to facilitate the detection, with only 50 legitimate *User Equipments* (UEs) and 5 times more rogue UEs.

If the same metric combination is evaluated in the Scenario 1 and 3, where the legitimate to rogue UE ratio is equal to 1, the DR decreases down to 96.19% when the emulation duration is short, or 99.92% when the simulation duration

is similar to Scenario 2. In both cases, the OSR and F_1-Score perform very well, remaining above 97.5% due to the accuracy on the classification of the collected network traffic.

The *Session Mean Time* (SMT) metric is the second best metric, bute requires a long duration (Scenario 3) for the emulation to guarantee the best performance. This metric is able to detect the attack with a DR of 97.54% and 93.4% for Scenarios 2 and 3, respectively. On the contrary, the OSR obtains a better result in Scenario 2, with a 97.55% against the 93.62% evaluated for Scenario 3 due to a 6.6% FNR. The reason for this minor difference is again the ratio between legitimate to rogue UEs, as only the legitimate UEs are able to successfully complete an RRC session and modify the average RRC session monitored by the SMT metric.

If the *Success Rate* (SR) or the CRR metrics are combined with the SMT metric, the individual detection performance suffers an important decrease of the DR and increase of the FNR. Scenario 1 registers the worse case, when the (SMT, SR) metric combination manages to obtain a decent 82.86% DR. This value implies a reduction of almost 15% on the DR if it is evaluated against its highest detection performance, when this metric is individually used in Scenario 2. However, even in this case, this metric combination is able to provide a high level of accuracy, with a 100% Precision and F_1-Score of 90.63%

The lowest result across all the conducted experiments is registered for the SR metric in Scenario 3, with an unacceptable 0.42% DR and FNR of 99.58%. The registered Precision is 100% due to the absence of FP cases, which boosts the OSR to a minimal 16.41%.

Although the SR is present in all low DR results across all scenarios, it adds value when combined with the CRR metric, as previously mentioned at the beginning of this section. The (CRR, SR) metric combination provides very good results for all three Scenarios. Besides the excellent performance in Scenario 2, it obtains a DR higher than 96% in both scenarios 1 and 3, which is accompanied with an OSR of 97.51% in Scenario 1, and 98.01% in Scenario 3.

Looking at the obtained results, it is possible to conclude that an attacker attempting to execute the signalling DoS attack should inject a similar number of RRC Connection Request messages equivalent to the actual number of legitimate requests registered on the network, reducing the attack duration to short periods of time. The optimisation of the attack implies a period of monitoring the channel, in an attempt to match the average legitimate RRC Connection Request messages registered within a certain time. Only by carefully tailoring the attack duration and injection rate, may the attacker be able to reduce the chances of being detected by the proposed algorithm.

6 Conclusions

This paper has presented three new metrics to detect DoS attacks over the RRC layer in LTE networks. The proposed solution has been experimentally validated using an emulated LTE test-bed, obtaining a sample data-set to evaluate the detection performance.

The detection mechanism is able to detect the attack with a DR higher than 98.81% and Precision higher than 88.77% using a single metric, the CRR. Furthermore, robustness has been added by combining the use of the CRR metric with two additional metrics, the SR and SMT, which are able to perform equally well in terms of DR or even improve the DR by 1.2% in specific cases.

The results have revealed how the attacker could optimise the attack, by adapting the average RRC connection Requests within the targeted network and reducing the attack's duration to short periods. Further research to improve this work should be focused on evaluating the algorithm in more congested networks, where the data fusion results have proven to be more successful to reduce the false positives.

References

1. Vintila, C., Patriciu, V.: Security analysis of LTE access network. In: Proceedings 10th International Conference Networks (ICN 2011), pp. 29–34 (2011)
2. Yu, D., Wen, W.: Non-access-stratum request attack in E-UTRAN. In: Computing, Communications and Applications, pp. 48–53 (2012)
3. Bilogrevic, I., Jadliwala, M., Hubaux, J.: Security issues in next generation mobile networks: LTE and femtocells. In: 2nd International Femtocell Workshop, pp. 1–3, Luton, UK (2010)
4. Purkhiabani, M., Salahi, A.: Enhanced authentication and key agreement procedure of next generation evolved mobile networks. In: 2011 IEEE 3rd International Conference on Communication Software and Networks, May 2011, pp. 557–563 (2011)
5. 3GPP TS 33.401: Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture, vol. 1, no. v.15.6.0 - Release 15, pp. 1–79 (2018)
6. Vintilă, C.-E., Patriciu, V.-V., Bica, I.: An analysis of secure interoperation of EPC and mobile equipments. In: 6th International Conference on Digital Telecommunications, pp. 1–6 (2011)
7. 3GPP TS 33.501: Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system, vol. 1, no. v.15.3.1 - Release 15, pp. 1–181 (2018)
8. 3GPP TS 38.300: Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description; Stage 2. vol. 0, no. v.15.4.0 - Release 15, pp. 1–97 (2018)
9. Shafer, G.: A Mathematical Theory of Evidence. Princeton University Press, Princeton (1976)
10. Bassil, R., Chehab, A., Elhajj, I., Kayssi, A.: Signaling oriented denial of service on LTE networks. In: Proceedings of the 10th ACM International Symposium on Mobility Management and Wireless Access, Ser. MobiWac 2012, pp. 153–158. ACM, New York (2012)
11. Jover, R.P., Lackey, J., Raghavan, A.: Enhancing the security of LTE networks against jamming attacks. EURASIP J. Inf. Secur. 1–14 (2014)
12. Li, X., Wang, Y.: Security enhanced authentication and key agreement protocol for LTE/SAE network. In: 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing, September 2011, pp. 1–4 (2011)

13. Køien, G.M.: Mutual entity authentication for LTE. In: 2011 7th International Wireless Communications and Mobile Computing Conference, July 2011, pp. 689–694 (2011)
14. Zheng, Y., He, D., Yu, W., Tang, X.: Trusted computing-based security architecture for 4G mobile networks. In: Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT 2005), pp. 251–255 (2005)
15. Zheng, Y., He, D., Tang, X., Wang, H.: AKA and authorization scheme for 4G mobile networks based on trusted mobile platform. In: 2005 5th International Conference on Information Communications Signal Processing, December 2005, pp. 976–980 (2005)
16. 3GPP TS 22.278: Technical Specification Group Services and System Aspects; Service requirements for the Evolved Packet System (EPS), Network, vol. 0, no. v.16.1.0 - Release 16, pp. 1–50 (2018)
17. 3GPP TS 36.331: Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification, no. v.15.4.0 - Release 15 (2018)
18. Wetteroth, D.: OSI Reference Model for Telecommunications. McGraw-Hill Professional, New York (2001)
19. Cao, J., Ma, M., Li, H., Zhang, Y., Luo, Z.: A Survey on security aspects for LTE and LTE-A networks. IEEE Commun. Surv. Tutor. **16**(1), 283–302 (2014)
20. Lichtman, M., Reed, J.H., Clancy, T.C., Norton, M.: Vulnerability of LTE to hostile interference. In: 2013 IEEE Global Conference on Signal and Information Processing, December 2013, pp. 285–288 (2013)
21. Cho, J.-S., Kang, D., Kim, S., Oh, J., Im, C.: Secure UMTS/EPS authentication and key agreement. In: Park, J., Leung, V., Wang, C.L., Shon, T. (eds.) Future Information Technology. Application, and Service, pp. 75–82. Springer, Dordrecht (2012). https://doi.org/10.1007/978-94-007-5064-7_11
22. 3GPP TS 36.300: 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, no. v.14.0.2 - Release 14, 2017
23. Khan, M., Ahmed, A., Cheema, A.R.: Vulnerabilities of UMTS access domain security architecture. In: Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008, SNPD 2008, pp. 350–355 IEEE (2008)
24. Reineking, T.: Belief functions: theory and algorithms. Ph.D. dissertation, Mathematics and Informatics, University of Bremen (2014)
25. Escudero-Andreu, G.: Protection of Mobile and Wireless Networks Against Service Availability Attacks. Ph.D. dissertation, Loughborough University (2018)
26. Kyriakopoulos, K.G., Aparicio-Navarro, F.J., Parish, D.J.: Manual and automatic assigned thresholds in multi-layer data fusion intrusion detection system for 802.11 attacks. IET Inf. Secur. **8**(1), 42–50 (2014)
27. Olson, D.L., Delen, D.: Advanced Data Mining Techniques, 1st edn. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-76917-0
28. Elhamahmy, M.E., Elmahdy, H.N., Saroit, I.A.: A new approach for evaluating intrusion detection system. Artif. Intell. Syst. Mach. Learn. **2**(11), 290–298 (2010)