Security Analysis of DoS Attack against the LTE-A System

Wei Cao, Nan Ma, Ping Zhang
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing, P.R.China, 100876
e-mail: {caowei,manan,pzhang}@bupt.edu.cn

***Abstract*—LTE-Advanced (LTE-A) has become a mature communication system in the world, and its security is attracting more and more attention. Although the LTE-A is significantly improved in functionality and security. However, there are also attacks against the LTE-A network. This paper first studies the specifications of non-access-stratum (NAS) of Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) and uncovers two new denial of service (DoS) vulnerabilities about Tracking Area Update (TAU) procedure. Then we construct the attack scenarios based on the previous analysis. Finally using related devices including mobile phones and eNodeB simulator, we demonstrate the attacks about these vulnerabilities and obtain the corresponding results.**

Keywords-LTE-A; security; tracking area update; DoS

I. INTRODUCTION

With the growing demand for data business development the 3rd Generation Partnership Project (3GPP) has been exploring how to meet new requirements for mobile networks since 2004. Release 8 of the 3GPP standards resulted in the deployment of Long Term Evolution (LTE). Moreover, LTE-A is the evolution of LTE standards, LTE-A is the latest cellular network technology to offer wireless access to mobile phones. This new technology is great enhancements in the Radio Access Network (RAN) as well as the cellular core network, moving towards an all-IP system.

As mobile operators have constructed LTE-A networks around the world, the security of LTE-A network is attracting more and more attention. People are reliant on LTE-A for their voice and data services; meanwhile, with the rising of the Internet of Things (IoT), LTE-A also plays an important role in Machine-to-Machine communication. According to Gartner, there will be 26 billion devices on the IoT by 2020 [1]. Therefore, any impact on the security of LTE-A system could cause serious impact on the great number of devices that rely on it.

According to the many past researches, mobile phones remain vulnerable to many kinds of attacks. Especially, it is known to have several vulnerabilities in early 2G system. For example, the lack of mutual authentication in 2G system makes it possible to attack by fake base stations.

Even though the encryption and authentication algorithms are appropriately enhanced in LTE-A system. However, it is also vulnerable to attackers. For example, Jill Jermyn summarized previous DoS attack models and demonstrated botnets can cause a DoS by exhausting user traffic capacity over the air interface. In addition, the results of the paper show that a single attacker can drastically reduce the QoS of legitimate devices in the same cell [2].

However, different from previous research efforts, there are also existing potential security problems. In particular, femtocells are rapidly becoming a popular and low cost solution to enhance the coverage and capacity of mobile systems, illegal deployment of unproven fake base stations can have a serious impact on mobile phones within coverage.

In this paper, unlike the most papers attacking the network, we focus on the attack on cellphones. We demonstrate two new practical DoS attacks against LTE-A access network based on vulnerabilities through a careful analysis of LTE-A access network protocol specifications, which mainly impact on the User Equipment (UE).

To be specific, in LTE-A, the air interface of access network is called E-UTRAN. Our attack is based on the air interface, first we analyze the security of Tracking Area Update (TAU) procedure, then we construct the attack scenarios based on the previous analysis, finally the analysis is verified by using the eNodeB simulator and the actual UE and get the corresponding attack results.

The rest of this paper is organized as follows. In section Ⅱ, we review the LTE-A network architecture and some important background details are briefly discussed. In section Ⅲ we analyze the security of TAU procedures and describe the possibility of DoS attack on UEs. In section Ⅳ we will carry out some practical verification work. In section Ⅴ concluding the paper.

II. BACKGROUND KNOWLEDGE

A. LTE-A Network Architecture

As shown in Fig. 1, the LTE-A network consists of the Evolved Packet Core (EPC) and the E-UTRAN. The EPC is an all-IP network in the LTE-A systems and consists of a Mobility Management Entity (MME) and a Serving Gateway (SGW), E-UTRAN includes the Evolved Universal Terrestrial Radio Access Network Base Stations, called eNodeB (eNB), which communicates with UEs directly. The access network and the core network are connected through the S1 interface, and the eNodeBs is connected via the X2 interface [3], [4].

Fig. 2 shows the protocol stack of control plane. In E-UTRAN, the data link layer and the physical layer provide the data transmission function for the Radio Resource Control (RRC) protocol message, NAS signals terminate in

978-1-5090-6352-9/17/$31.00 ©2017 IEEE

MME and UE. NAS signals are in RRC messages between UEs and eNodeBs [5], [6]. We will focus on NAS layer and RRC layer and control-plane signals in this paper.

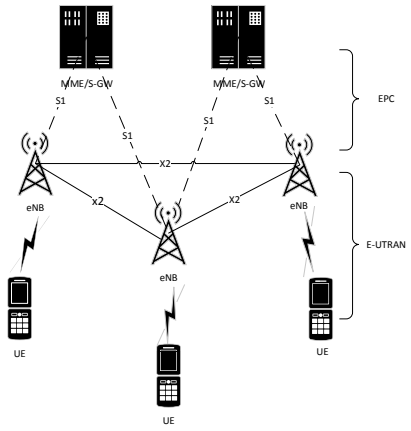

Figure 1. Network architecture of LTE-A

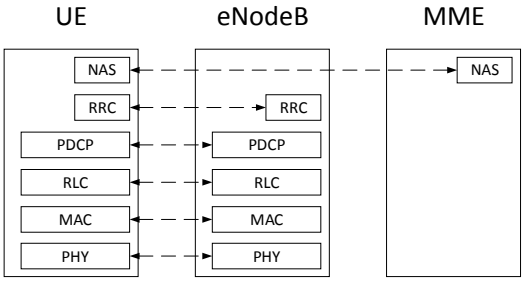

Figure 2. Control plane protocol stacks

B. *Related Technical Terms*

We will mainly analyze the security of TAU procedures, the following terms are used throughout the whole study.

Tracking Area (TA) is defined as an area in which a user may move freely without updating the MME, the main function of the TA is to manage and represent the locations of UEs, the network allocates a list with one or more TAs to the user. Tracking Area List (TAL) is a scheme introduced by the LTE-A system, the UE receives a TA list from a cell, and keeps the list until it moves to a cell that isn't included in its list. Tracking Area Identity (TAI) is the identity used to identify tracking areas, the TAI is constructed from the Mobile Country Code (MCC), Mobile Network Code (MNC) and Tracking Area Code (TAC).Tracking Area Update (TAU) can inform EPC the mobile phone is available. The EPC manages TAs which are registered by UEs in idle and connection state [7][8].

III. VULNERABILITIES ANALYSIS OF TAU

A. *Triggers of TAU Procedures*

According to 3GPP TS 24.301 [8], a stand-alone tracking area update occurs when a UE experiences any of the following conditions.

- UE detects it has entered a new TA that is not in the list of TAIs that the UE registered with the network.
- The periodic TA update timer has expired.
- UE is in UTRAN PMM-Connected state when it reselects to E-UTRAN.
- UE is in GPRS READY state when it reselects to E-UTRAN.
- The TIN indicates "P-TMSI" when the UE reselects to E-UTRAN.
- The RRC connection was released with release cause "load re-balancing TAU required".
- The RRC layer in the UE informs the UE's NAS layer that an RRC connection failure (in either E-UTRAN or UTRAN) has occurred.
- A change of the UE Network Capability and/or MS Network Capability and/or UE Specific DRX Parameters and/or TS 24.008 MS Radio Access capability information of the UE.
- A change in conditions in the UE requires a change in the extended idle mode DRX parameters previously provided by the MME.
- For a UE supporting CS fallback, or configured to support IMS voice, or both, a change of the UE's usage setting or voice domain preference for E-UTRAN.
- For a SR-VCC capable UE, a change of MS Classmark 2 and/or MS Classmark 3 and/or Supported Codecs.
- UE manually selects a CSG cell whose CSG ID and associated PLMN is absent from both the UE's Allowed CSG list and the UE's Operator CSG list.
- UE receives a paging request from the MME while the Mobility Management back off timer is running and the UE's TIN indicates "P-TMSI".
- A change in any of the values of information included in Preferred Network Behavior that would create incompatibility with the Supported Network Behavior provided by the serving MME.

As the first case is the most common case, and the DoS attack is carried out using eNodeB simulator in this paper, so the first trigger condition is the most easy to implement. Therefore we will use the first trigger condition in the following content.

B. *Tracking Area Update Procedures*

The UE will stay in the idle state after the attachment on EPC. When the TAU process initiates, the RCC connection completes first. There are many reasons of TAU but the first two reasons account for more than eighty percent. Moreover, the DoS attack presented in this paper belongs to the first reason. According to [9], the TAU procedures is as follows, since the next section will be based on the analysis of first six steps to construct the attack scenario, so we will focus on the first six steps of the TAU process.

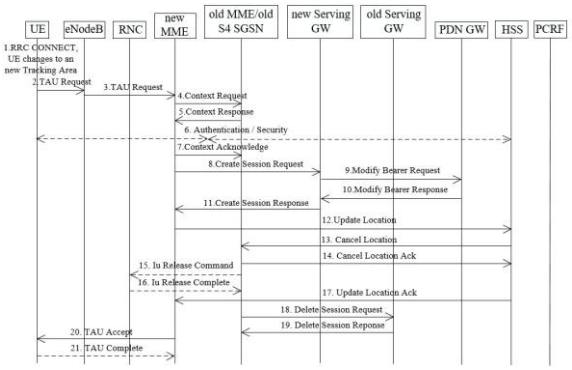

Figure 3. Procedures of TAU

1) UE enters a new TA which is not in the list of TAIs that the UE registered with the network, completing the RRC procedure and starting the TAU procedure.
2) The UE initiates the TAU procedure by sending a TAU Request message together with RRC parameters indicating the Selected Network and the old Globally Unique MME Identity (GUMMEI) to the eNodeB.
3) The eNodeB derives the MME address from the RRC parameters carrying the old GUMMEI, the indicated Selected Network and the RAT. If that MME is not associated with that eNodeB or the GUMMEI is not available or the UE indicates that the TAU procedure was triggered by load re-balancing, the eNodeB selects an MME through MME Selection Function.
4) The new MME differentiates the type of the old node, uses the Globally Unique Temporary UE Identity (GUTI) received from the UE to derive the old MME address, and sends a context request message to the old MME to retrieve user information.
5) If the Context Request is sent to an old MME the old MME responds with a Context Response message.
6) If the integrity check of TAU Request message (sent in step 2) failed, then authentication is mandatory.

C. *Vulnerabilities Analysis and Scenarios Construction*

Since the authentication is performed by mutual authentication in step 6, the UE can recognize the fake base station, so that the fake base station can only attack the UE by issuing an abnormal signaling message before the authentication step.

TABLE I. TAU REJECT MESSAGE CONTENT

Information Element
Protocol discriminator
Security header type
Tracking area update reject
message identity
EMM cause
T3346 value
Extended EMM cause

The attack scenario is mainly for the first TAU trigger condition, since the eNodeB simulator (fake base station) is not in the TAI list of the UE, so the TAU procedure initiates after the UE enters the range of the eNodeB simulator. In this case, the fake base station can operate the TAU Reject message intentionally.

The contents of the TAU Reject message are shown in the Table I, and the detail of EMM cause is shown in table Ⅱ, the left side is the eight binary numbers, and the right side is the corresponding content. In the EMM cause can be set to No. 8 (00001000) rejection reason, the meaning is Evolved Packet System (EPS) services and non-EPS services not allowed, because the process of the message is not encrypted, the UE will update its status to EU3: ROAMING NOT ALLOWED after receiving the fake base station's abnormal air interface signaling. At this point, the UE will no longer attempt to access the normal LTE, 3G, GSM network, and remain in the EMM-DEREGISTERED state, it can cause lasting DoS impact.

TABLE II. EMM CAUSE INFORMATION ELEMENT

0 0 0 0 0 0 1 0	IMSI unknown in HSS Information Element
0 0 0 0 0 0 1 1	Illegal UE
0 0 0 0 0 1 0 1	IMEI not accepted
0 0 0 0 0 1 1 0	Illegal ME
0 0 0 0 0 1 1 1	EPS services not allowed
0 0 0 0 1 0 0 0	EPS services and non-EPS services not allowed
0 0 0 0 1 0 0 1	UE identity cannot be derived by the network

Moreover, the EMM cause can be also set to No. 7 (00000111) rejection reason (EPS services not allowed) as shown in Table Ⅱ, then the UE will be driven from the 4G network to 2G network as a consequence, thus in the 2G network for further attacks.

According to the above analysis, we can construct the corresponding signaling flow chart as shown in Fig. 4.

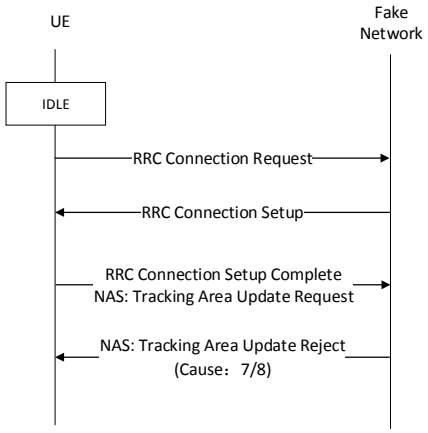

Figure 4. DoS attack procedures.

IV. VERIFICATION AND RESULTS

In this section, we will use Testing and Test Control Notation version 3 (TTCN-3) to write the implementation code of the above process, then obtain the corresponding

results in the supporting hardware and software environment for attack verification.

According to the previous analysis and 3GPP TS 27.007, we can design the following program flow chart.

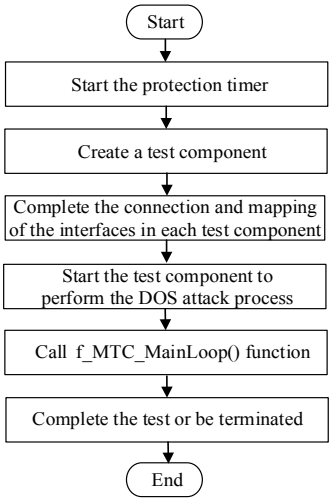

Figure 5. Attack process procedures.

To complete the definition of the DoS attack test case, we first create the EUTRA_PTC parallel test component, and define the main part of the DoS attack test instance. Then we need to call the function f_MTC_ConnectPTCs _LTEA_IRAT() to create the test component of NASEMU _PTC, complete the connection and map of the interfaces in each test component, and realize the communication between MTC and PTC module. After that starting the test component NASEMU_PTC to perform the DoS attack procedure flow. Next calling the f_MTC_MainLoop () function, waiting for the completion of the test behavior on the EUTRA_PTC or the test component is terminated. Finally, the EUTRA_PTC ends the test behavior or is terminated, completing the whole DoS attack test process [10].

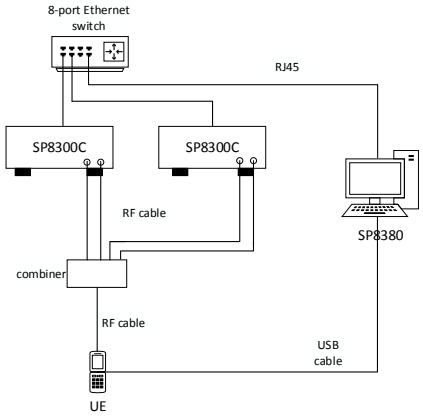

Figure 6. Hardware connection diagram.

In the following, we will build the actual hardware and software environment for testing and verification. The hardware connection environment is as shown in Fig. 6 and Fig. 7, computer system management (SP8380) is the control core of the hardware system, controlling the equipment operation, system self-check, executing TTCN - 3 executable test sets. SP8300C is multimode system simulator, each SP8300C can support one or two LTE/GSM cells.

Figure 7. Actual test environment

The IP configuration of the hardware connection and the main software list of the system is as shown in Tab. Ⅲ and Tab. Ⅳ.

TABLE III. HARDWARE IP CONFIGURATION

Hardware	IP
SP8300C-1	10.0.0.1
SP8300C-2	10.0.0.2
SP8380 server	10.0.0.3

TABLE IV. SOFTWARE LIST OF THE SYSTEM

Software	Description
TS Manager	The interaction interface, used to manage system and execute the test cases
Test Case Software	Provide the DoS test cases for the corresponding scenario
UE Controller	Control terminal status automatically
SP8300C	Simulate one or two LTE / GSM cells
Log Tracer	Receive and store logs in real time

TS Manager, Log Tracer and UE Controller running on SP8380 master server, SP8300C software running on SP8300C instruments. TTCN-3 based Layer 3 test set executable files are integrated in the TS Manager software.

TS Manager provides a concise and convenient interface to manage the execution of test cases, real-time output of logs, and simple and clear results. TS Manager interface including: menu bar, shortcut bar, test suite and test plan window, test case window, output window, MSC window, signaling information window.

After the starting of TS Manager and connection of the instruments and test sets configuration, we can operate the TS Manager test case suite.

The Fig. 8 shows the interface display of the DoS attack of rejecting the 4G network test case. The MSC is the Message Sequence Charts, a formal language used to describe the order in which messages interact between entities and the environment, and the Message Info is the

specific message content signaling contains. In this figure we can see that the reason for the refuse carried in "TRACKINGAREAUPDATEREJECT" signaling is 0000-0111B, as mentioned in table Ⅱ. The comparison of the attack effect on the UE is shown in the Fig. 9, the left side is the state before the attack, the right side is the state after the attack and the small graph above is the partial magnification. we can see that the UE is expelled from the 4G network after the attack, and can only access 3G or GSM network. Moreover, the mobile phone will remain in this state until the restart or even re-plug the SIM card to recover from the attack.

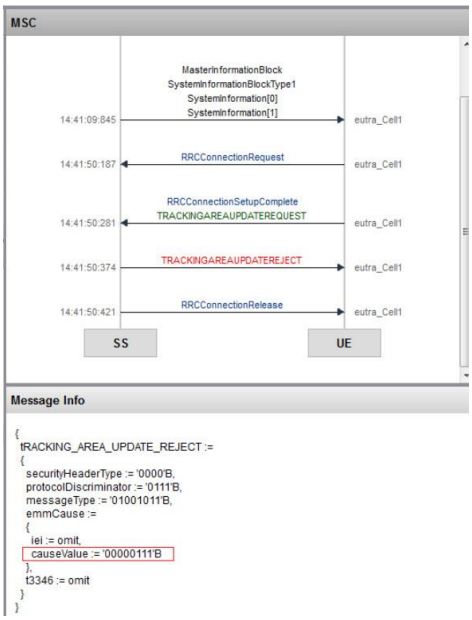

Figure 8. The output of reject 4G case

Figure 9. The UE expelled from 4G.

The Fig. 10 shows the interface display of the test case execution result of the DoS attack of rejecting all standard network. In the figure we can see that the reason for the refuse carried in "TRACKINGAREAUPDATEREJECT" signaling is 00001000B, as mentioned before. The comparison of the attack effect on the UE is shown in the Fig. 11, we can see that the UE is expelled from the all-standards network after the attack, including the 4G, 3G and GSM network. Similar to the previous case, the mobile phone will remain in this state until the restart or even re-plug the SIM card to recover from the attack.

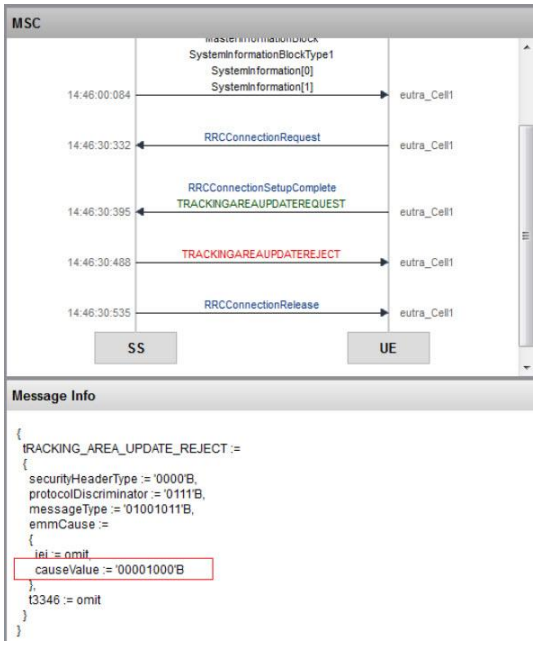

Figure 10. The output of reject all case

Figure 11. The UE expelled from all networks

After the actual verification, we can see that the actual system results and the theoretical analysis is consistent. As for anti-attack schemes, the users can restart or re-plug the SIM card to recover from the attack. In addition, a timer can be used to recover from the DoS attacks, if the UE is detached from the network for a long time because of the TAU reject message until the timer times out, the UE can re-attach itself to the network again without bothering the users, this may be a relatively easy solution to solve the problem in the future.

V. CONCLUSION

We have analyzed some vulnerabilities about E-UTRAN and TAU procedure in this article. Although LTE-A provides

some mechanisms to make mobile system more security, we found out that some vulnerabilities in such networks still exist, unprotected transmission of messages were used to launch DoS attacks, then we proved the existence of defects in theory and practical system of the experiment respectively.

Since all commercial phones have to follow the relevant 3GPP protocol, such attacks are of general applicability, so our work is of great important. Finally our work can provides a basis for the improvement and updating of related processes in the future.

ACKNOWLEDGEMENT

This work was sponsored by Huawei Innovation Research Program, the National Natural Science Foundation of China (61421061) and Hisense Co.Ltd.

REFERENCES

[1] Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. http://www.gartner.com/technology/site-index.jsp

[2] Jill Jermyn, Gabriel Salles-Loustau, and Saman Zonouz "An Analysis of DoS Attack Strategies Against the LTE RAN," Journal of Cyber Security, Vol.3 No.2, 159–180.

[3] 3GPP TS 36.401, "Evolved Universal Terrestrial Radio Access Network (EUTRAN), architecture description," Release 14, v14.0.0, 2017.

[4] S. Bhattarai, S. Rook, L. Ge, S. Wei, W. Yu and X. Fu, "On simulation studies of cyber attacks against LTE networks," 2014 23rd International Conference on Computer Communication and Networks (ICCCN), Shanghai, 2014, pp. 1-8.

[5] 3GPP TS33.401, "3GPP System Architecture Evolution (SAE); security architecture," Release 14, v14.2.0, 2017.

[6] D. Yu and W. Wen, "Non-access-stratum request attack in E-UTRAN," 2012 Computing, Communications and Applications Conference, Hong Kong, 2012, pp. 48-53.

[7] L. Qiang, W. Zhou, B. Cui and L. Na, "Security Analysis of TAU Procedure in LTE Network," 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Guangdong, 2014, pp. 372-376.

[8] 3GPP TS 24.301, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)," Release 14, v14.2.0, 2016.

[9] 3GPP TS 23.401, "General Packet Radio Service (GPRS) enhancement for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access," Release 14, v14.3.0, 2017.

[10] 3GPP TS 27.007, "AT command set for User Equipment (UE)," Release 14, v14.3.0, 2017.