Security Analysis of TAU Procedure in LTE Network

Li Qiang
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, P.R.China
yunwu753@163.com

Zhou wen'an
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, P.R.China
zhouwa@bupt.edu.cn

Cui Baojiang
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, P.R.China
cuibj@bupt.edu.cn

Liu Na
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, P.R.China

Abstract—**LTE has become a commercial communication technology worldwide, and its security issues are attracting more and more attention. Tracking Area Update (TAU) is a series of procedures performed by LTE system when users update Tracking Area (TA). The security of TAU procedure directly affects the whole system. This paper first analyzes the security of LTE core networks when the TA updates, then it puts forward a security enhancement scheme by borrowing the thoughts of denial of service (DoS). Therefore, it is important to protect Serving Gateway from overload problems. The proposed scheme is simple, and it also can prevent Serving Gateway from being attacked by malicious requests.**

Keywords—LTE; Security; Tracking Area; Tracking Area Update; Security Enhancement

I. INTRODUCTION

As mobile operators have constructed their own LTE networks around the world, more and more experts put their attention to the security of LTE network. Designers of LTE network aim at simplifying the architecture of the system, as it transits from the existing UMTS circuit plus packet switching combined network to an all-IP flat architecture system[1][2]. In the core network, original function entities are merged into two new logic elements: Mobility management Entity (MME) and Serving Gateway. This change leads to the assignment of most security work to MME by the system, including authentication, key agreement and session management. Most expert, who interest in the security of LTE mostly focus on the MME working procedure. This research mainly contains the authentication scheme under different conditions , key agreement mechanism, etc.

In the LTE system, paging and location update are based on the TAL (Tracking Area List) which composed of Tracking Areas. It is reasonable to suppose that the execution of TA procedure directly related to the quality of experience and has a significant impact on the whole system. The LTE system also assigns the security work of TA procedure to MME, mainly including the authentication of users and the integrity check of signalling. With the development of network and internet, the DoS attack has become the most popular attack in the network security. Many tools and DoS attack detection technologies have been discovered, including network traffic detection and packet content detection to defend DoS [3]. Some people present novel techniques to protect specific systems from DoS [4]. This paper first analyzes the security of Tracking Area Update (TAU) procedure, and a security enhancement scheme aiming at the lack of overload protection mechanism in the Serving Gateway. Also, the reliability of the proposed scheme is analyzed.

The rest of this paper is organized as follows: Chapter II introduces the background knowledge. In Chapter III, it analyzes the security of TAU procedures and describe the possibility of overload in the Serving Gateway. In Chapter IV, a security enhancement scheme is designed. Chapter V mainly analyzes the reliability of the new scheme. Finally, the last part is the conclusion part in Chapter VI.

II. BACKGROUND KNOWLEDGE

A. *Basic Technical Terms*

The following terms are used throughout the thesis and we bring them here as a background to the whole study.

- *MME* is the control plane entity which supports many functions including tracking area list management
- *Tracking Area (TA)* is defined as an area in which a user may move freely without updating the MME. TA is a term used in LTE networks. TA is almost the same concept as the Location Area (LA) in the circuit-switched (CS) domain and the Routing Area (RA) in the packet-switched (PS) domain in GSM and UMTS. 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. In certain operation modes, the UE may move freely in all TAs of the list without updating the MME[5].
- *Tracking Area List (TAL)* is a scheme introduced by the LTE system. In this scheme, instead of assigning

978-1-4799-4171-1/14 $31.00 © 2014 IEEE
DOI 10.1109/3PGCIC.2014.124

one TA to each UE, one UE can have a list of TAs. The UE receives a TA list from a cell, and keeps the list, until it moves to a cell that is not included in its list. In LTE standards, a cell is also able to give

- *Tracking Area Identity (TAI)* is the identity used to identify tracking areas. The Tracking Area Identity is constructed from the MCC (Mobile Country Code), MNC (Mobile Network Code) and TAC (Tracking Area Code).
- *Tracking Area Update (TAU)* can inform EPC the UE is available. The EPC (Evolved Packet Core) manages TAs which are registered by UEs in idle state and in connection state.

B. *Triggers Of TAU Procedures*

A standalone tracking area update occurs when a GPRS-attached or E-UTRAN-attached 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 (except for the case of a UE configured to perform Attach with IMSI when entering a TA in a new non-equivalent PLMN in RRC-IDLE mode);
- the periodic TA update timer has expired;
- UE was in UTRAN PMM_Connected state (e.g. URA_PCH) when it reselects to E-UTRAN;
- UE was in GPRS READY state when it reselects to E-UTRAN;
- the TIN indicates "P-TMSI" when the UE reselects to E-UTRAN (e.g. due to bearer configuration modifications performed on GERAN/UTRAN);
- the RRC connection was released with release cause "load re-balancing TAU required";

different lists to different UEs. The UE location is known in the MME to at least the accuracy of the TAL allocated to that UE[3].

- 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 (e.g. due to GERAN radio capability change or CDMA 2000 Radio Access Technology Capability change) information of the UE.
- 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".

C. *Tracking Area Update Procedures*

There are different Tracking Area Update procedures corresponding to different situations, we only study the first situation that UE enters a new TA here. All TAU procedures are presented in the figure 1[6], but we just analyze procedures from the trigger of TAU to updating bearer context by Serving Gateway.

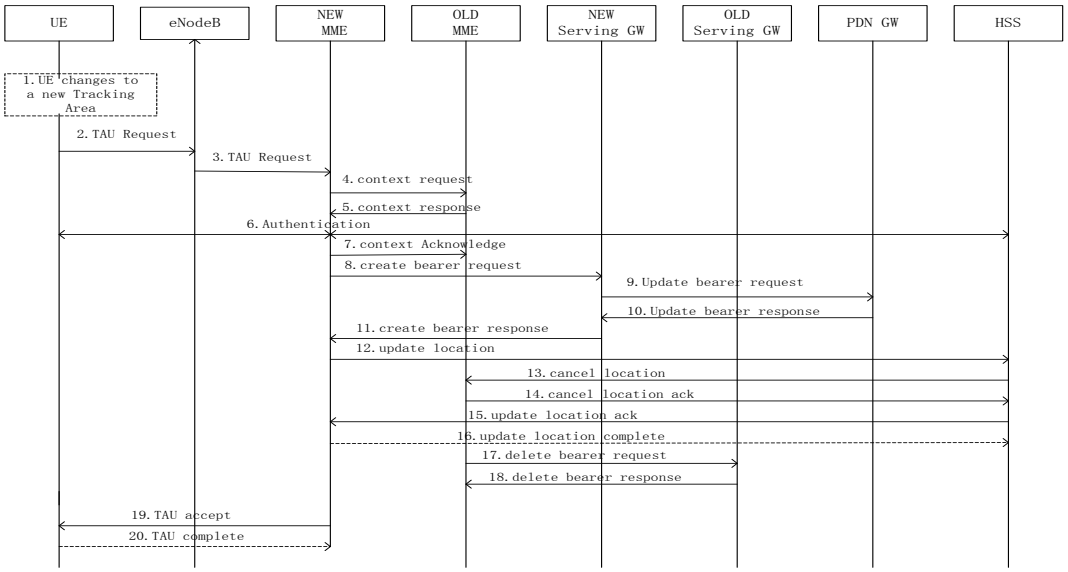

Fig.1 procedures of TAU

1) UE detects it has entered a new TA that is not in the list of TAIs that the UE registered with the network.

2) UE detects it has entered a new TA that is not in the list of TAIs that the UE registered with the network message together with RRC parameters indicating the Selected Network and the old GUMMEI. An exception is that, if the TAU was triggered for load re-balancing purposes, the old GUMMEI is not included in the RRC parameters.

3) The eNodeB derives the MME from the RRC parameters carrying the old GUMMEI and the indicated Selected Network. 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 a new MME with "MME Selection Function". The eNodeB forwards the TAU Request message together with the CSG access mode, CSG ID, TAI+ECGI of the cell from where it received the message and with the Selected Network to the new MME. In case of Tracking Area Update without MME change the signalling in steps 4, 5, 7 and steps 12-17 are skipped.

4) The new MME sends a Context Request message to the old MME to retrieve user information. UE Validated indicates that the new MME has validated the integrity protection of the TAU message, e.g. based on native EPS security context for the UE. To validate the Context Request the old MME uses the complete TAU Request message and responds with an appropriate error if integrity check fails in old MME. This shall initiate the security functions in the new MME. If the security functions authenticate the UE correctly, the new MME shall send a Context Request to the old MME with the UE Validated set. If the new MME indicates that it has authenticated the UE or if the old MME correctly validates the UE, then the old MME starts a timer.

5) If the Context Request is sent to an old MME the old MME responds with a Context Response.

6) If the integrity check of TAU Request message (sent in step 2) failed, then authentication is mandatory.

7) The MME (if the MME has changed then it is the new MME) determines to relocate the Serving GW. The Serving GW is relocated when the old Serving GW cannot continue to serve the UE. The MME (if the MME has changed then it is the new MME) may also decide to relocate the Serving GW if a new Serving GW is expected to serve the UE longer and/or with a more optimal UE to PDN GW path, or if a new Serving GW can be collocated with the PDN GW.

8) If the MME has changed the new MME verifies the EPS bearer status received from the UE with the bearer contexts received from the old MME. If the MME has not changed the MME verifies EPS bearer status from the UE with the bearer contexts available in the MM context. If the MME selected a new Serving GW it sends a Create Session Request message per PDN connection to the selected new Serving GW.

9) The Serving GW informs the PDN GW(s) about the change of for example the RAT type that e.g. can be used for charging, by sending the message Modify Bearer Request per PDN connection to the PDN GW(s) concerned. User Location Information IE and/or UE Time Zone IE and/or User CSG Information IE are also included if they are present in step 8.

10) The PDN GW updates its bearer contexts and returns a Modify Bearer Response message. The MSISDN is included if the PDN GW has it stored in its UE context.

11) The Serving GW updates its bearer context. This allows the Serving GW to route bearer PDUs to the PDN GW when received from eNodeB.

III.SECURITY ANALYSIS OF TAU

A. Overall Analysis

From the signalling procedures, we can see that the security mechanism of TAU is implemented in MME, including the integrity check of Context Request message in step 4 and the authentication in step 6. These two steps ensure the legitimacy of the signaling and the user, but the LTE system puts the integrity of the signalling prior to the authentication of users. The LTE system probably may assume the default initiator as a validated user, and does not authenticate users until the integrity of signaling has been broken. Therefore, it offers the premise for illegal users to attack MME. However, with an abnormal state of MME, no protection mechanism is found in the following procedures. That is to say, the security of TAU procedure completely depends on MME. Although MME is located in the core network, where is relatively safe and with absolutely strong processing ability, the lack of protection mechanism in Serving Gateway is a security vulnerability for networks, demanding strong secure protections.

B. Overload Of Serving Gateway

To analyze the security vulnerability of Serving Gateway in the TAU procedures, we refer to the thoughts called denial of service attacks. Once new MME achieves the context of users, it sends Create Bearer Request to the new Serving Gateway. Except for the request timeout mechanism in the MME, Serving Gateway does not have any security mechanism for this procedure. Serving Gateway may have overload problems if any of the following cases occur in the network.

1) The whole network is in normal working state, but UE switches to a new TA with exceptions. Even though the authentication procedure execute normally, new MME has already accepted exception messages from UE. If the MME is attacked, it may send a large

number of Create Bearer Request messages to the new Serving Gateway in a short period of time.

2) If there is a programmable mobile phone, which can continuously trigger the TAU requests through a program in a short time, these requests are forwarded to the MME from eNodeB and requests from step 1 to step 7 are sent to every node including the new Serving Gateway.

3) Someone falsifies a large number of users malicious, and sends TAU requests with other validate users. The large amount of requests can lead to a new Serving Gateway overload.

Although MME is located in the safe core network, and has a perfect security mechanism, it can not rule out the possibility of MME working improperly in case 1. By contrast, the attackers are willing to falsify the validate user and program on a terminal in an easier way. If these situations occur without any effective security mechanism in the Serving Gateway, the Serving Gateway is likely to overload. Therefore, a security enhancement scheme for Serving Gateway is proposed in the following sections.

IV.A SECURITY ENHANCEMENT SCHEME

In this section, a security enhancement scheme to prevent overload of Serving Gateway is proposed.

Figure 2 shows procedures of the security enhancement scheme.

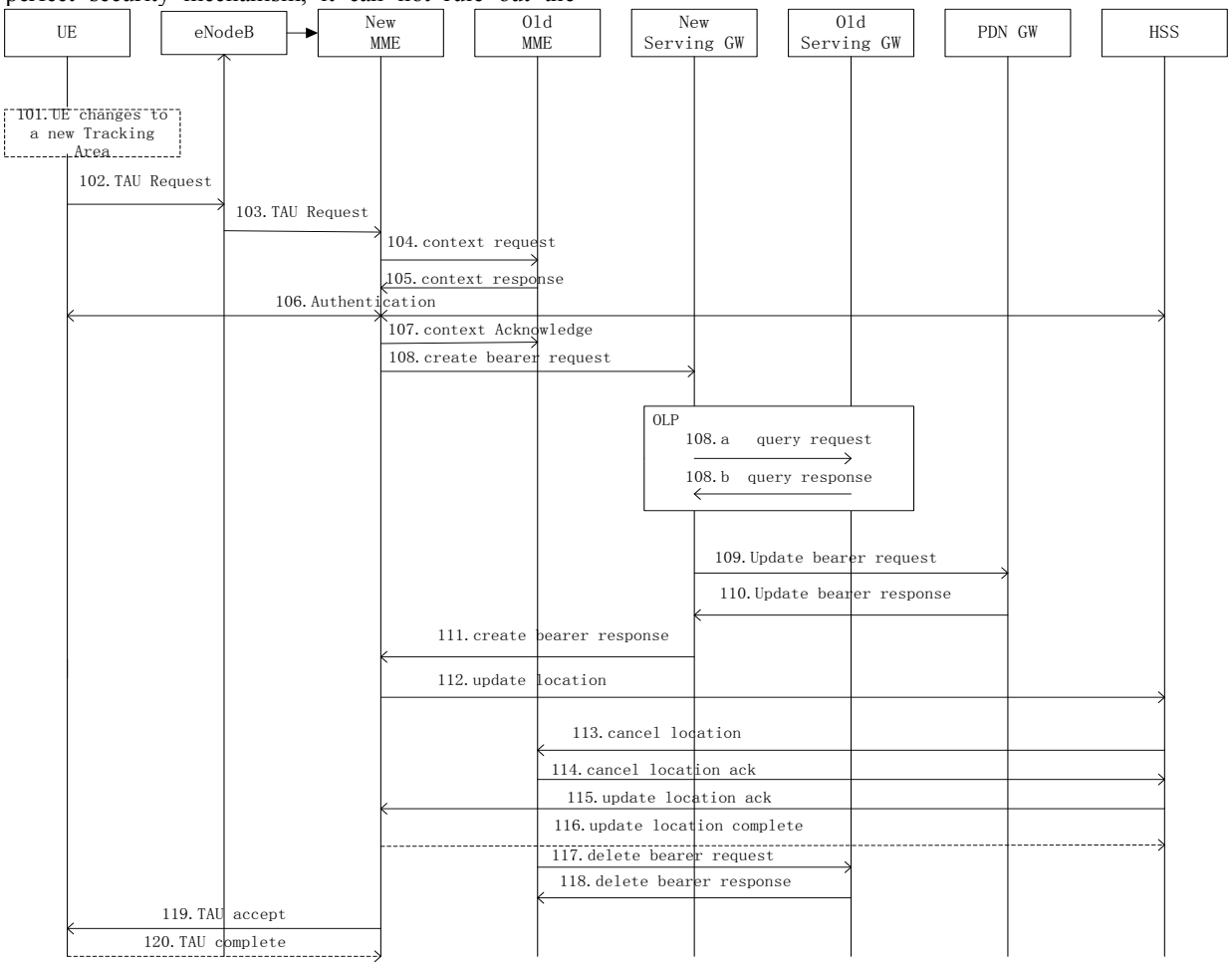

Fig.2 procedures of security enhancement scheme

Every TAU Request message contains the IMSI（international Mobile Subscriber Identification Number）, which is a unique number to identify a subscriber. It can be sent to the Serving Gateway with Create Bearer Request messages. Once the Serving Gateway receives Create Bearer Request from MME, it will check the amount of Create Bearer Request with the same IMSI. If Serving Gateway checks out the amount of Create Bearer Request messages that belong to one user is greater than one, it discards the packets and refuses the request. Although the Serving Gateway has detected the fact that one user corresponds to one Create Bearer Request packet, the Serving Gateway does not proceed to the next step immediately. The Query Request message (108.a) is sent to the old Serving Gateway to verify the authenticity of users, which is performed a by comparing IMSI. Then the Query

Response message (108.b) is sent to the new Serving Gateway with the authentication information. With the authentication information, the legitimate users can be distinguished from illegal users. The packets of illegal users are discarded but the legitimate users can continue the next TAU procedure.

V. RELIABILITY ANALYSIS OF SECURITY ENHANCEMENT SCHEME

The scheme can prevent Serving Gateway from overload in the following situations.

1) When one user triggers TAU procedures under normal or abnormal circumstance, the TAU Request message will lead to an improper working of MME, which is that MME will send more than one Create Bearer Request to new Serving Gateway in a short time.

2) If attackers falsify a large number of users to trigger TAU procedures, the large amount of Create Bearer Request can lead to the overload of Serving Gateway even though MME works properly.

If Create Bearer Request has timed out, the core network refuses the request due to the timeout mechanism. The proposed new scheme is designed to prevent Serving Gateway from being attacked by large amounts of Create Bearer Request messages in a short time. If the same user sends more than one TAU requests, the Serving Gateway discards the request packets and refuses the TAU request. If unauthenticated users attack the core network by sending TAU requests, new Serving Gateway sends Query Request to verify the authenticity of users. The core network continues the procedures after Serving Gateway receives the response that indicates the user is authenticated

VI.CONCLUSIONS.

Because of the simplified network architecture of LTE, most of security work is assigned to MME. However, LTE system lacks essential security protections for other entities. This paper analyzes the security mechanism of TAU procedures, pointing out the security vulnerability is lack of the protection for overload in Serving Gateway and designing a security enhancement scheme. The scheme is simple and of great importance to LTE systems, especially when a high security standard is required.

REFERENCES

[1] 3GPP, Evolved Universal Terrestrial Radio Access Network(E-UTRAN), architecture description, 3GPP TS 36.401 v9.2.0, 2010.

[2] 3GPP, 3GPP System Architecture Evolution (SAE); security architecture, 3GPP TS33.401 v12.9.0, 2013.

[3] Wentao Liu, “Research on DoS Attack and Detection Programming”, in Intelligent Information Technology Application, 2009. IITA 2009. Third International Symposium on (Volume:1), 21-22 Nov. 2009: pp 207-201.

[4] Tagra D,Rahman M,Sampalli S,”Technique for preventing DoS attacks on RFID systems”,in Software, Telecommunications and Computer Networks (SoftCOM), 2010 International Conference on 23-25 Sept. 2010:pp 6-10.

[5] Sara Modarres Razavi, “Tracking Area Planning in Cellular Networks” Link ¨ oping Studies in Science and Technology Licentiate Thesis No. 1473.

[6] 3GPP,General Packet Radio Service (GPRS) enhancement for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, 3GPP TS 23.401 v11.9.0, 2014.