Session-Based Detection of Signaling DoS on LTE Mobile Networks

Woung Jang, Se Kwon Kim, Joo Hyung Oh, and Chae Tae Im

***Abstract*—In recent years, global cellular network service is being changed rapidly to LTE. However, the fast introduction of LTE has been going with not enough research about security threat so it could have many kinds of vulnerability. Therefore, the research about security threat on 4G network is ongoing in many countries. Particularly, in the situation where domestic subscribers are increasing rapidly, the security threats which are hindering stability and usability could make a fatal effect on many users. 4G network should consider the feature of mobile network to keep 4G network stable. Because mobile network has limited radio resources, it releases the radio resource which is not used in selected time and reallocates when requesting the data transmission. Many signaling messages are transferred in the network entities to allocate or release the radio resource. In this paper, it will introduce the technology to detect signaling DoS traffic hindering the stability and usability of network entities managing the radio resources by huge signaling message from the repetitive wireless connection/release message.**

***Index Terms*—Denial of service, LTE, signaling DoS, virtual setup, 4G.**

I. Introduction

Today, smart phone users use various mobile services on the high speed mobile network. Many kinds of mobile services need faster and stable mobile network infrastructure, and because of this, mobile network market has changed rapidly into LTE networks from 3G WCDMA network. In June 2013, the number of LTE networks subscribers passed over the number of 3G WCDMA network subscribers, and continue increasing 1 million per month consistently in Korea [1], [2].

On the other hand, the development speed of mobile security technology for LTE network is not fast enough. Because of closed architecture of legacy cellular network, the demand of security system inside the network or security policy was unmarketable. Therefore, the development of security technology concerning the feature of mobile network is required.

Mobile networks have limited radio resources. For allocating resources effectively, the resource of one UE will be released when detected no use during set time, and reallocate when detected data transfer request. In these processes, many signaling messages for setting radio resource are transferred within mobile network entities. Therefore, if malicious users trigger the allocation and release of the radio resources, it could make the network failure of the entities controlling radio resources. This is Signaling DoS [3]. (See Fig. 1).

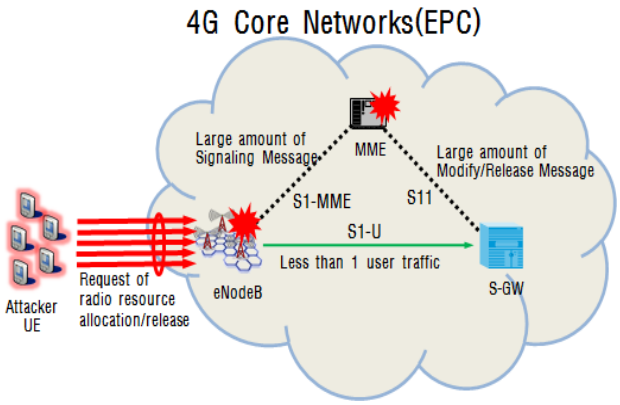


Fig. 1. Signaling DoS in LTE networks.

In 3G WCDMA network, there is low risk of Signaling DoS attack because signaling message and user data traffic use the same route. In LTE networks, however, the route of signaling message and data traffic is different, and the network bandwidth of the signaling message is smaller than that of data traffic. In many cases, mobile network service providers make the bandwidth of data traffic is over 10 times bigger than that of signaling message. For Signaling DoS attack which makes the overflow of signaling message route, this attack could affect the 4G networks signaling entities, like eNodeB, MME.

In this paper, we suggest the algorithm about detecting Signaling DoS caused by repetitive network connection/release.

II. Background: Mobile

Basic mobile networks include UE (User Equipment), BS (Base Station), CN (Core Network) for control and data communication. And until 3G, mobile networks have the hierarchical architecture. The closer it tis to the outside internet, the more integrated the mobile entities are.

As shown in Fig. 2, 3G Networks [4] provide data service through UTRAN (Universal Mobile Telecommunication System Terrestrial Radio Access Network) and PN (Packet Network), an element of core network. And UTRAN consists of many base stations and RNC (Radio Network Controller). UTRAN makes UE to communicate with PN, PN makes UE to communicate with the external networks like the Internet. In the 3G mobile network, they use a unique protocol called GTP (General Packet Radio Service Tunneling Protocol).

Manuscript received December 16, 2013; revised March 17, 2014. This work was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013.

The authors are with Korea Internet & Security Agency, Seoul, Korea (e-mail: jangw2232@kisa.or.kr, heath82@kisa.or.kr, jhoh@kisa.or.kr, chtim@kisa.or.kr).

This protocol is used for controlling data communication in the mobile network and transmitting actual data. The former is GTP-C, and the latter is GTP-U. The IP packets sent from UE are encapsulated with the GTP-U. GTP-C controls the whole data transmitting process.

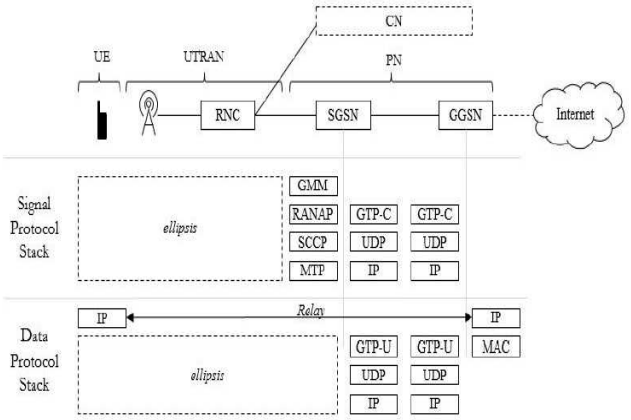


Fig. 2. 3G mobile network structure.

In LTE networks [5], as shown in Fig. 3, UTRAN evolved to E-UTRAN (Evolved UTRAN), and PN also evolved to EPC (Evolved Packet Core). It is a feature of LTE networks that there are two paths each to communicate the control message and data transmission message. S-GW (serving Gateway) and P-GW (PDN gateway) in the LTE networks can be mapped to the SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node) in the 3G networks. And typically, mobile network service providers make the bandwidth of data traffic is over 10 times bigger than that of signaling message. This makes the main cause of LTE Signaling DoS attack.

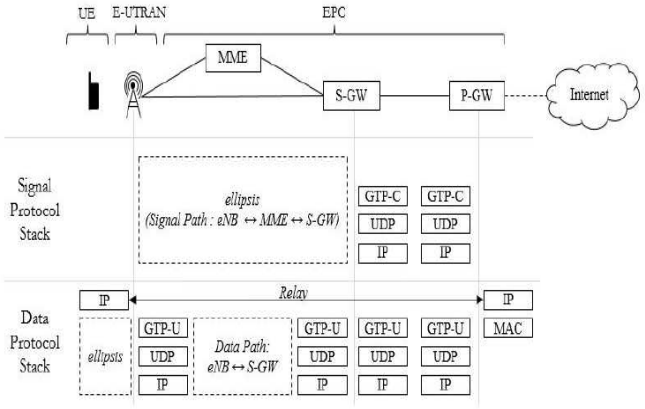


Fig. 3. LTE mobile network structure.

III. Related Research

Security technologies for protecting each vulnerability in mobile network have been developing. Ricciato introduced DoS Attack models in 3G WCDMA network [6]. In his paper, he introduced various DoS attack model like paging, DCH (Dedicated Channel) allocation. Patrick proposed first the theme about Signaling DoS in 3G network [3]. He made the algorithm for detecting the Signaling DoS. Bassil introduced Signaling DoS in LTE networks [7]. His Signaling DoS method is depend on the scenario allocate/release many dedicated radio bearer. But when allocating the dedicated bearer in the LTE networks, PCRF should request the allocation of dedicated bearer. Bassil was not mentioned about the method of the allocating the dedicated bearer from PCRF.

In this paper, we choice the Signaling DoS detection method made by active-idle state change.

IV. Signaling DoS Detection

As shown in Fig. 4, there are three steps to detect the Signaling DoS. First step is classification the radio resource allocation/release of UEs by analyzing GTP-C control messages of each UE. Second step is detection of virtual setup by analyzing the data traffic during allocation time. Final step is detection of Signaling DoS by analyzing the time interval between the virtual setups.

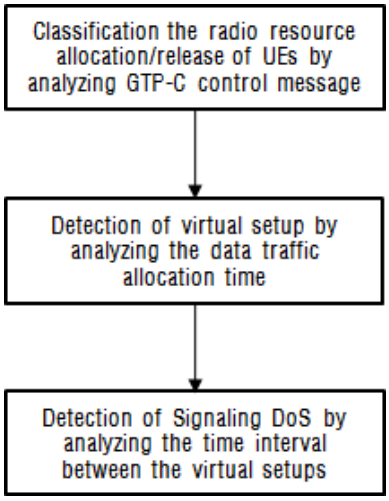


Fig. 4. Signaling DoS detection process.

A. Make Session from Classifying UE

In 4G LTE networks, there are three cases of allocating radio resources to UE. It's Allocation by attach, Allocation by handover, Allocation by idle-active state change. All of three cases could be detect by modify bearer request/response message in S11 interface. As shown in Fig. 5, by monitoring the messages in S11 interface, the allocation of radio resource of each UE could be detected.

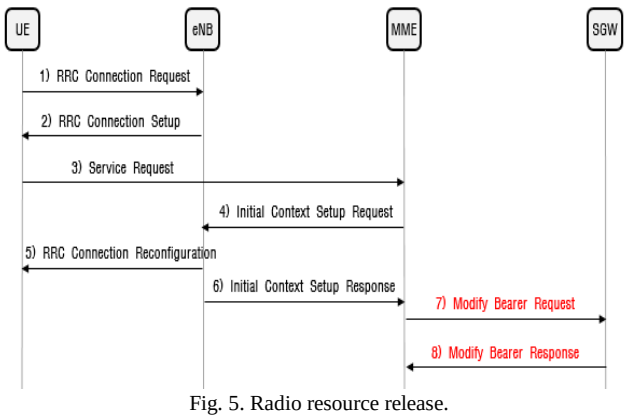


Fig. 5. Radio resource release.

Likewise, there are three cases of releasing radio resources to UE. They are release by detach, release by handover to

another eNodeB, release by idle-active state change. In the three cases, release by detach takes more time than release by idle-active state change, and release by handover is hard to use to Signaling DoS attack. By monitoring release access bearer request/response messages in S11 interface, the release of radio resource of each UE could be detected. (See Fig. 6).

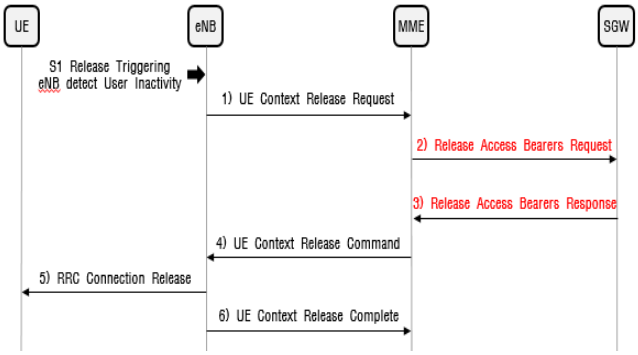


Fig. 6. Radio resource re-allocation.

B. Detection of Virtual Setup

For determining these radio resource allocations by Modify Bearer Request/Response are normal, data traffic of each UE should be recorded. Signaling DoS has a feature that nothing or little data traffic from UE. Therefore, by monitoring S1-U interface, each UE traffic could be classified and the allocation of radio resource of each UE could be determined whether virtual setup or not.

For identifying sender UE from data traffic in S1-U interface, Modify Bearer Request/Response message in S11 interface should be recorded. LTE network entities use TEID (Tunnel Endpoint Identifier) for identify each tunnel of UE. There is S1-U S-GW TEID in modify bearer request message, S1-U eNodeB TEID in modify bearer response message. These TEIDs could be recorded in a database and this database make identification possible.

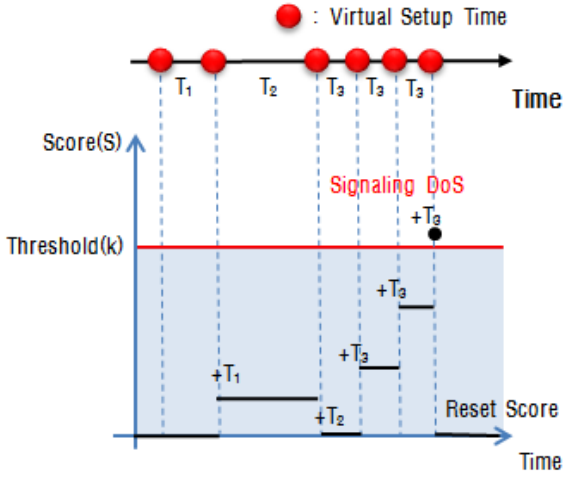


Fig. 7. Signaling DoS detection algorithm.

C. Detection of Signaling DoS

Signaling DoS is caused by repetitive/periodic virtual setup by multiple UE. The detection of Signaling DoS is based on the database of virtual setup time of each UE. As shown in Fig. 7, if cumulative summation score of a specific UE is over than threshold k, it will detected Signaling DoS attack.

$$S_t = \max\{S_{t-1} + (-\frac{T}{\alpha} + 1), 0\}$$

In the upper equation, S is score, t is current virtual setup time, t-1 is previous virtual setup time, T is the time interval between two virtual setups. α is variable to adjust score. If the time interval is short, the score is increased. If the time interval is long, the score is decreased.

V. Conclusions and Future Work

We have presented the 3 Step Signaling DoS detection algorithm. First step is classifying the radio resource allocation/release of UEs by analyzing GTP-C control messages of each UE. Second step is detecting virtual setup by analyzing the data traffic during allocation time. Final step is detection of Signaling DoS by analyzing the time interval between the virtual setup. In future work, we intend to develop and test this algorithm to apply an intrusion detection system as a module on commercial LTE network, or port in the cellular network control system

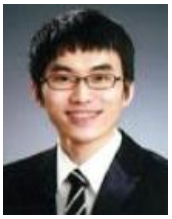
Acknowledgment

This research was funded by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013.

References

[1] *Global Mobile Data Traffic Forecast Update* (*2012~2017*), CISCO VNI (Visual Networking Index), Mobile World Congress, Feb 2013.
[2] (June 2013). Statistics on wired & wireless, *Ministry of Science, ICT & Future Planning*. [Online]. Available: http://www.msip.go.kr/www/brd/m_220/view.do?seq=385
[3] P. Lee, T. Bu, and T. Woo, "On the detection of signaling dos attacks on 3g wireless networks," in *Proc. INFOCOM 2007*, May 2007.
[4] H. Holma, A. Toskala, *WCDMA for UMTS – Radio Access for Third Generation Mobile Communications*: Willey, 2004, ch. 1.
[5] General Packet Radio Service (GPRS); Service description; Stage 2, TS 23.060 V10.3.0, 3GPP, 2011.
[6] F. Ricciato, A. Coluccia, and A. D'Alconzo, "A review of DoS attack models for 3G cellular networks from a system-design perspective," *ACM Computer Comun*, vol. 33, 2010.
[7] R. Bassil, A. Chehab, I. H. Elhajj, and A. Kayssi, "Signaling Oriented Denial of Service on LTE Networks", in *Proc. MobiWac 2012*.

Woung Jang was born on June 13, 1987, Republic of Korea. He has bachelor's degree in computer science & engineering from Korea University in Seoul, Korea. He joined Korea Internet and Security Agency in February 2013, and researches about 4G LTE mobile security include IMS, VoLTE.



Se Kwon Kim was born on February 27, 1982, Republic of Korea. In 2009, he has received master's degree in communication signal processing from Sungsil University. His main interest area is network security (IPS, IDS), malware (Botnet, Behavior based code analysis). He joined Korea Internet and Security Agency in January 2009, and researches about Botnet, 3G mobile security include GTP. In 2011, he became senior research associate and researches for 4G/LTE network security include EPC, Femtocell networks.

Joo Hyung Oh was born on September 5, 1980 at Ulsan, Republic of Korea. In 2005, he has received bachelor's degree in computer science from Inje University. Finally, in 2008, he received master's degree in computer engineering from Sungkyunkwan University. His main interest area is network security (VPN, IPS), malware (Botnet, Behavior based code analysis). He joined Korea Internet and Security Agency in December 2007, and researches about botnet, malware analysys, 3G mobile security include GTP and SS7 on 3G network. In 2010, he became senior research associate and researches for 4G/LTE network security include EPC, Femtocell data network.

Chae Tae Im was born on September 1, 1974 at Daejeon, Republic of Korea. In 2000, he has received bachelor's degree in computer science from Chungnam National University. Finally, in 2003, he received master's degree in computer engineering from Pohang University of Science and Technology. His main interest area is network security (VoIP, mobile network), malware (Botnet, Behavior based code analysis). He joined Korea Internet and Security Agency in January 2003, and led researches about VoIP, Botnet, Malware, 3G mobile security. In 2011, he became director of advanced operation technology team in Korea Internet Security Center and research about 4G/LTE network security and mobile malware detection/prevention.