DDoS Attacks in Experimental LTE Networks

Jan Feng[1], Bing-Kai Hong[1], and Shin-Ming Cheng[1,2(✉)]

[1] Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan
{m10615033,d10815003,smcheng}@mail.ntust.edu.tw
[2] Research Center for Information Technology Innovation, Academia Sinica, Taipei, Taiwan

Abstract. The infamous distributed denial-of-service (DDoS) cyberattack in which attackers aim to disrupt normal services provided by one or more servers over the Internet based on distributed resources have been deeply investigated. However, the impacts on the recent popular LTE networks remain an open issue and becomes the main target of this paper. We implement the different types of existing DDoS attacks against volume, protocols, and applications in experimental 4G LTE networks. In particular, the attack is developed on the rooted Android mobile phone and the targeted networks build by using OpenAirInterface (OAI) platform. An additional monitoring module is included to capture the packets, payloads, and patterns generated from attacks. The evaluated results show that the existing IP-based DDoS attack can be successfully launched and cause significant amount of traffic volume to the experimental networks.

1 Introduction

With the popularity of heterogeneous mobile devices and ubiquitous cellular connectivity, the 4G communications technology, Long Term Evolution (LTE), has been deeply integrated into our daily life. To offer the public reliable and accountable service, security and privacy issues have been intensively investigated by the operators. The private networks controlled by the operator on the one hand eliminate the possibility of introducing traditional well-known attacks in the public Internet. On the other hand, the expensive equipments and complicated protocols in LTE networks significantly increase the cost of developing experimental platform, thereby burdening the attack design and testing. As a result, no severe vulnerabilities are exposed in LTE networks since it is launched [1].

However, in the recent years, the appearance of Software Defined Radio (SDR) bridged the gap between academic researchers who are interested in cellular security and realistic cellular experimental platform. Consequently, lots of practical attacks are designed and are proved to be feasible in the operational LTE networks [2], such as IMSI catcher [3,4], denial-of-service (DoS) [5–7], Distributed DoS (DDoS) [8–11], information spoofing [12,13], privacy violation [14,15], DNS spoofing [16], and large-scale attack [17]. Typically, such attack

L. Barolli et al. (Eds.): WAINA 2020, AISC 1150, pp. 545–553, 2020.
https://doi.org/10.1007/978-3-030-44038-1_50

is achieved by introducing rogue Base Stations (BSs) implemented by using open-source cellular software (e.g., OpenAirInterface; OAI or srsLTE) with cheap SDR hardware (e.g., Universal Software Radio Peripheral; USRP). In particular, the attacker discovered the design flaws of LTE protocols, such as unencrypted messages exchanged before the mutual authentication, to enforce the victim User Equipment (UE) believe the commands sent from rogue BSs.

In this paper, we are interested in if the current DDoS attacks thrived in Internet could impact the LTE networks. The all-IP architecture of LTE networks gives a chance to those infamous IP-based attacks, such as DNS amplification, Ping of death flooding, SYN flooding, or HTTP GET/POST attacks, where the network elements in LTE core networks could become the attack targets. Some related works [18–20] have explored this research direction, however, no practical attacks on UE side are implemented and thus no feasible experimental results are provided. To evaluate the negative effects caused by DoS attacks launched from the UE side, we build an experimental LTE network as a target by using open-source OAI and USRP B210 from NI. Moreover, we implement existing fifteen IP-based DDoS attacks including volume amplification and protocol flooding attacks on rooted commercial Android phones and SDR UEs. An additional monitoring module is included in the experimental platform to capture the packets, payloads, and patterns generated from attacks as well as to record the attack relation. The evaluated results show that the attack can be successfully launched and cause significant amount of traffic volume to the experimental networks.

2 Background and Related Works

2.1 LTE Network Architecture

Figure 1 depicts a simplified LTE network architecture, which consists of UE, Radio Access Network (RAN), and the Core Network (CN). UE contains an unique International Mobile Subscriber Identity (IMSI) and corresponding authentication materials for mutual authentication between CN. E-UTRAN in LTE represents RAN and is composed of multiple BSs, eNBs, for allocating limited radio resources and encrypting user data. As the CN in LTE, Evolved Packet Core (EPC) consists of multiple important IP-based network elements, such as mobility management entity (MME), home subscriber server (HSS), and serving network gateway (SGW), and packet data network gateway (PGW). MME is responsible for authentication and resource allocation while UE tries connecting to the network. The UEs' identities and authentication material are stored in HSS and SGW and PGW helps data forwarding.

2.2 IP-Based DDoS Attacks

The traditional IP-based DDoS attacks leverage multiple attackers to generate a huge attack traffic volume to the target. We classified the conventional

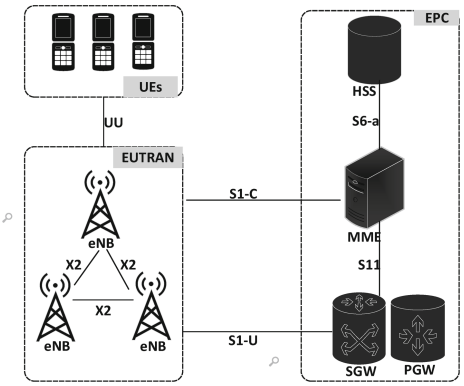

Fig. 1. LTE network architecture

DDoS attacks into direct flooding, volume amplification, and handshake protocol attacks. Attacker could send a high volume of malicious traffic to the victim through the botnet. It can be achieved via ping commands or ICMP broadcast. Amplification attacks set up attacks through making up fake source IP addresses and leverage vulnerable serves to send UDP responses to the target. Amplification attacks can launch through DNS servers, NTP servers, Chargen servers, etc. Protocol attacks focuses on vulnerabilities of TCP/IP protocols and connection procedures, including SYN flood attack, ACK flood attack, etc.

2.3 DoS and DDoS Attacks in LTE Networks

2.3.1 IP-Based DDoS Attacks in LTE Networks

Some IP-Based DDoS attacks have discussed in previous studies [8–10], where multiple attackers are needed to launch this kind of attack. In particular, those attackers with coordinated agents using botnet command and control centers (C&C) can generate massive traffic volume and further launch DDoS attacks.

2.3.2 DoS and DDoS Attacks Designed for LTE Networks

Recently, some novel attacks are proposed to block services of LTE network by leveraging semantic vulnerabilities of LTE protocols [5–7,17,21,22]. Regarding DoS attack, an adversary could simply utilize the plaintext without encryption and integrity protection exchanged between UE and BS before mutual authentication procedure. In this case, a rogue BS is developed to insert a reject message containing some cause among a normal message exchanging between victim UE and operational BS and the victim UE received the malicious information will believe it and enforce itself to carry out the instruction in the message, for example, cannot connect to any surrounding operational BSs, thereby achieving DoS [5–7,17]. On the other hand, attacker could develop malicious UEs to launch novel DDoS attack [21,22]. By continuously

sending RRC_Connection_Request messages to the victim BS without responding RRC_Connection_Complete, the resource for RRC connections will be depleted and the normal RRC_Connection_Request from legal UE will be rejected, thereby achieving DDoS attack. Same trick can be applied in many registration procedure, such as malicious UE sending deregistration requests before or during the registration procedure. Please note that this attack is very similar to that leveraging vulnerabilites in handshaking protocols.

3 System Model

3.1 System Architecture

As shown in Fig. 2, the system architecture including one EPC with one eNB. There are multiple commercial UEs connecting to the eNB and tried to launch DDoS attack to the PGW located in the EPC. In order to monitor the reaction of being attacked, we leverage SDR hardware and opensource LTE software to build an experimental LTE network. We implement various kinds of DDoS attacks as an APP on the malicious UE, where harmful and crafted packets are sent to a particular IP address. A gateway is included in our architecture to separate the interfaces of S1-U, S1-C, and SGI. It is due to that we need to understand the behavior of each interface when attack occurred, especially distinguishing the traffic from intranet and Internet.

3.2 Adversary Model

We assume an active adversary with minimum privilege, that is, the adversary owns valid keys to register with the LTE network but does not have information about other legitimate users' key. Moreover, the adversary knows the IP address

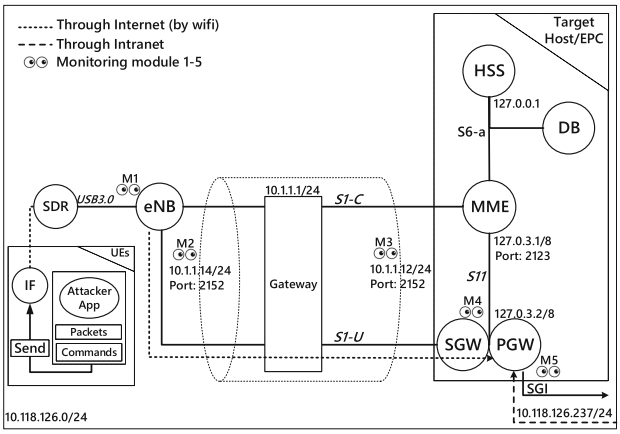

Fig. 2. System architecture

of the elements in the CN and touch them directly. The attack is launched by malicious APPs in adversary's UE. As Fig. 2 shows, two attacks are launched, the first one is targeted at the IP address of PGW and is achieved via WiFi connectivity. The second one is targeted at IP address of SGW via UU and S1-U interfaces (i.e., normal LTE connectivity). By comparing results from two attacks, we could evaluate the attack effects more precisely.

3.3 Monitoring Module

In order to comprehensive understand the effects caused by proposed DDoS attack, we deploy five monitoring modules in different places of the experimental environment. As Fig. 2 and Table 1 show, M1 locating at eNB captures attack packets from malicious UE. M2 and M3 are respectively responsible of outgoing traffic from eNB and incoming traffic to MME/SGW. The difference between M3 and M4 both located in SGW/PGW is that M3 inspects both S1-C and S1-U while M4 investigates tunneling traffic between MME and PGW. M5 is used for monitoring the traffic from Internet via SGI interface.

Table 1. Monitoring modules

Module	Procedure	Interface	Flow tool	Packet tool
M1	UE to eNB	–	`QCSuper`	–
M2	eNB to EPC	eno1	`iftop`	`Wireshark`
M3	S1-C & S1-U	eno1	`iftop`	`Wireshark`
M4	S1-U	gtp0	`iftop`	`Wireshark`
M5	SGI	enx00e04c68008e	`iftop`	`Wireshark`

4 DDoS Attacks in LTE Network

4.1 Direct Flooding

In this category, attackers usually launch flow amplification to increase bandwidth consumption and even congestion. In flow attacks, attackers mainly send a high volume of malicious traffic directly to the victim through ping commands or ICMP broadcast. We implement ① ping of death flood attack, ② malformed IP packet flood attack, and ③ smurf attack. We launch ping of death flood attack through ping commands, and later send the abnormal packet to the target PGW. At another malformed IP packet flood attack, it's also the so-called teardrop attack. It rearranges regular IPv4 packet format, then sends these irregular packets to the target. Little different from the preceding, smurf attack acts attacks through broadcasting. While UEs under the same network receive ICMP requests with the fake source IP as the target IP, they send considerable ICMP

responses to the target together. A particular example of the ping of death flood attack is described as follows. After successfully connecting to the network, these malicious UEs start sending massive ping requests to the eNB presented in step 1. In step 2, the eNB will next forward the packet to corresponded EPC. However, the packet size owns over IPv4 standard 65536 Bytes. Once the target PGW receives a vast amount of traffic, it might cause PGW broken, and the attack succeeds.

4.2 Volume Amplification Attacks

Regarding reflected amplification attacks, weaknesses of web servers and UDP protocol are exploited. Some web servers, such as DNS servers or NTP, are lack of comprehensive authority mechanism and adopt UD protocol for data transmission. Unlike the reliable TCP protocol, UDP packets endure high risk in making up fake packets. We implement amplification attacks, including ④ DNS servers, ⑤ NTP servers, ⑥ Chargen servers, ⑦ SSDP servers, and ⑧ Memcached servers. The key of those attack is to make the servers believe that the victim IP address is the source IP address of the crafted traffic. Vulnerable servers will response to PGW in our attack scenario. After successfully connecting to the network, malicious UEs start sending DNS query packets to unsettled DNS servers with fake source IP, which perform in step 1. By repeating recursive queries, in step 2, DNS servers will respond with large UDP packets to the target PGW. While PGW constantly accepts the enormous traffic pressure, it probably ends with bandwidth overflow. Furthermore, the severity is far from the effort made by attackers.

4.3 Handshake Protocol Attacks

Regarding the handshake protocol attacks, adversary exploits weakness of handshake protocols and we implement ⑨ SYN flooding attack, ⑩ ACK flood attack, ⑪ RST flood attack, and ⑫ TCP connection flood attack. We take the SYN flooding attack as an example. In order to increase the successful possibility of attacking, we build a stable environment where multiple UEs with HTTP services exist. Then those UEs are leveraged to attack targeted CN by sending abnormal packets.

5 Experimental Results

5.1 Experimental Environment Setup

We use Intel mini PC-NUC with ubuntu 16.04 OS and intel i7 CPU as well as USRP hardware to build our experimental networks consisting of eNB and EPC. On the other hand, we choose mobile phones supported LTE, and Android Studio with SDK. Moreover, we use the software `iftop`, `QCSuper`, and `Wireshark` as the monitoring modules. We deploy multiple UEs with malicious apps which

connect to our OAI EPC at the same time through USRP B210. We initiate `Wireshark` and `iftop` in each network interfaces to respectively collect activity information and traffic flow. We also apply `QCSuper` tool to keep an examination on the UE side. Although current DDoS attacks might not touch the elements in the CN (such as MME, SGW, or PGW) directly, the experiment is necessary since the monitoring results such as attack patterns and logs are necessary to the operator for DDoS attack detection and prevention.

5.1.1 Attack Module in the UE Side

We exploit Android NDK in communication with the Linux layer below the Android structure to launch our DDoS attacks. However, we need to make up fake source IP addresses in some attacks such as amplification attacks and to modify raw packets directly. To this end, we developed a generic method that can stay execution without rebuilding Android OS or Linux kernel but act as the root with the authority of `CAP_NET_ADMIN` and `CAP_NET_RAW` in Linux kernel.

5.1.2 Monitoring Module in the CN

As shown in Table 1 and Fig. 2, we choose `Wireshark` and `iftop` to carry out our monitoring modules. The deployment details are described in Sect. 3.3. In particular, M2 is assigned at IP 10.1.1.14 (i.e., eNB) for outgoing traffic tracking while M3 is located at IP 10.1.1.12 (i.e., EPC) for monitoring traffic between eNB and EPC. Moreover, M4 is assigned at IP 127.0.3.2 for inspecting tunneling traffic and M5 is for public IP 10.118.126.237 (i.e., PGW) for Internet traffic investigation.

5.2 Performance Evaluation

We list our detailed attack results in Table 2, including flood type, volume type, and protocol type attacks. Under the consideration of our chiefly OAI experimental environment, the results simply depend on monitoring module M2, M4, and M5 with payload 500. Because of direct attacks, we focus on M2 and M4 in flood type and volume type attacks. In attack ① and ②, their data flow is around 200 MB in one minute with three malicious UEs. However, attack ③ is launch by broadcasting, and it only generated 25 MB. It should be stronger when more attackers exist. In protocol type attacks, ⑩, ⑪ and ⑫ own 100 MB to 200 MB. There was a gap between ④ and the other. It exists lower attack flow because TCP connection requests sent after the whole TCP three-way handshake procedure, which also promoted attack succeed difficulty.

Last, from attack ④ to ⑨ are volume attacks. It mainly depends on reflection responses by remote servers, so we consider the M5 monitoring module rather than M4. Most of them own more 200 MB in M2, but only around 50 KB to 80 KB in M5. It shows that amplification attacks have poor performance than other attacks under the experimental LTE network. Besides, in our investigation, though our attacks aim at crashing the EPC, the eNB may sometimes hit earlier. However, it still requires more tests to draw a definite conclusion.

Table 2. Attack volume of specified attacks from fifteen DDoS attacks with three attackers in 1 min

Attack name	M2	M4	M5	Payload
① Ping of death flood attack	202 MB	198 MB	–	500
② Malformed IP packet flood attack	179 MB	116 MB	–	500
③ Smurf attack	25.2 MB	17.1 KB	–	500
④ DNS amplification attack	287 MB	–	36.7 MB	500
⑤ NTP amplification attack	230 MB	–	78.3 KB	500
⑥ Chargen amplification attack	290 MB	–	56.4 KB	500
⑦ SSDP amplification attack	288 MB	–	58.8 KB	500
⑧ Memcached amplification attack	595 MB	–	275 MB	500
⑨ SYN flood attack	125 MB	121 MB	–	500
⑩ ACK flood attack	484 MB	141 MB	–	500
⑪ RST flood attack	290 MB	208 MB	–	500
⑫ TCP connection flood attack	8.28 MB	4.47 MB	–	500

6 Conclusion

In this paper, we implement different types of DDoS attacks in the experimental LTE networks and investigate the reactions of the LTE. In particular, the attack tools are installed in the commercial UEs, and we successfully launch the attack, and the targeted networks suffer from heavy traffic. The attack tools and monitoring modules are useful to the operators for the testing of future 5G networks. The monitored traffic patterns can be leveraged by the network defenders who could recognize the occurrences of the DDoS attacks.

Acknowledgements. This work was partially supported by the Institute for Information Industry, Taiwan, under Grant 108-EC-17-D-11-1638, by the Ministry of Science and Technology, Taiwan, under Grants 108-2628-E-011-007-MY3, and by Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU).

References

1. Mavoungou, S., Kaddoum, G., Taha, M., Matar, G.: Survey on threats and attacks on mobile networks. IEEE Access **4**, 4543–4572 (2016)
2. Rupprecht, D., Dabrowski, A., Holz, T., Weippl, E., Pöpper, C.: On security research towards future mobile network generations. IEEE Commun. Surv. Tutor. **20**(3), 2518–2542 (2018)
3. Steig, S., Aarnes, A., Van Do, T., Nguyen, H.T.: A network based IMSI catcher detection. In: Proceedings of IEEE ICITCS 2016, September 2016
4. Park, S., Shaik, A., Borgaonkar, R., Martin, A., Seifert, J.-P.: Whitestingray: evaluating IMSI catchers detection applications. In: Proceedings of USENIX WOOT 2017, August 2017

5. Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., Seifert, J.-P.: Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In: Proceedings of NDSS 2016, February 2016
6. Shaik, A., Borgaonkar, R., Park, S., Seifert, J.-P.: On the impact of rogue base stations in 4G/LTE self organizing networks. In: Proceedings of ACM WiSec 2018, pp. 75–86, June 2018
7. Fei, T., Wang, W.: LTE is vulnerable: implementing identity spoofing and denial-of-service attacks in LTE networks. In: Proceedings of IEEE GLOBECOM 2019, December 2019
8. Khosroshahy, M., Qiu, D., Ali, M.K.M.: Botnets in 4G cellular networks: platforms to launch DDoS attacks against the air interface. In: Proceedings of MoWNeT 2013, pp. 30–35, August 2013
9. Henrydoss, J., Boult, T.: Critical security review and study of DDoS attacks on LTE mobile network. In: Proceedings of APWIMOB 2014, pp. 194–200, August 2014
10. Jover, R.P.: Security attacks against the availability of LTE mobility networks: overview and research directions. In: Proceedings of IEEE WPMC 2013, June 2013
11. Gupta, A., Verma, T., Bali, S., Kaul, S.: Detecting MS initiated signaling DDoS attacks in 3G/4G wireless networks. In: Proceedings of COMSNETS 2013, January 2013
12. Shaik, A., Borgaonkar, R., Park, S., Seifert, J.-P.: New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. In: Proceedings of ACM WiSec 2019, pp. 221–231, May 2019
13. Lee, G., Lee, J., Lee, J., Im, Y., Hollingsworth, M., Wustrow, E., Grunwald, D., Ha, S.: This is your president speaking: spoofing alerts in 4G LTE networks. In: Proceedings of ACM MobiSys 2019, pp. 404–416, June 2019
14. Jover, R.P.: LTE security, protocol exploits and location tracking experimentation with low-cost software radio, July 2016. arXiv preprint: arXiv:1607.05171
15. Borgaonkar, R., Hirschi, L., Park, S., Shaik, A.: New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. Proc. Priv. Enhanc. Technol. **3**, 108–127 (2019)
16. Rupprecht, D., Kohls, K., Holz, T., Pöpper, C.: Breaking LTE on layer two. In: Proceedings of IEEE S&P 2019, May 2019
17. Heish, W.-L., Hong, B.-K., Cheng, S.-M.: Toward large-scale rogue base station attacks using container-based virtualization. In: Proceedings of IEEE VTC-Fall 2019, September 2019
18. Farina, P., Cambiaso, E., Papaleo, G., Aiello, M.: Understanding DDoS attacks from mobile devices. In: Proceedings of FiCloud 2015, pp. 614–619, August 2015
19. Kouraogo, Y., Zkik, K., Orhanou, G., et al.: Attacks on Android banking applications. In: Proceedings of ICEMIS 2016, September 2016
20. Tan, Y.-A., Xue, Y., Liang, C., Zheng, J., Zhang, Q., Zheng, J., Li, Y.: A root privilege management scheme with revocable authorization for Android devices. J. Netw. Comput. Appl. **107**, 69–82 (2018)
21. Byrd, T., Marojevic, V., Jover, R.P.: CSAI: open-source cellular radio access network security analysis instrument, May 2019. arXiv:1905.07617
22. Hu, X., Liu, C., Liu, S., You, W., Li, Y., Zhao, Y.: A systematic analysis method for 5G non-access stratum signalling security. IEEE Access **7**, 125424–125441 (2019)