Security Review and Study of DoS Attack on DNS in the International Roaming EPC_LTE Network

Ya'nan Tian(✉), Wen'an Zhou, and Wenlong Liu

School of Computer Science,
Beijing University of Posts and Telecommunications, Beijing 100000, China
tianyanan7080321@163.com, fans656@163.com,
zhouwa@bupt.edu.cn

Abstract. The communication standard Long Term Evolution (LTE) developed by 3GPP is becoming the mainstream technology of the next generation mobile communication, the new features meet the business needs and improve the user experience, but also bring some security threats. In this paper, we introduce the LTE roaming architecture, the attach procedure and the DNS resolution procedure. Then we analyze that MME initiate the DNS request before the authentication is completed based on the procedures and OpenAirInterface (OAI) code, which will lead to a large load on DNS server, this scheme is very vulnerable to DoS/DDoS attacks on DNS server. Finally, according to the characteristics of LTE, we propose a enhancement scheme in MME and analyze the feasibility.

Keywords: LTE · DNS · DoS/DDoS · OAI

1 Introduction

With more and more operators began to deploy LTE networks, LTE based international roaming is also being gradually promoted. According to China Mobile Communications Corporation (CMCC) news reports, by the end of April 2015, China Mobile and the United States, South Korea and other 73 countries and regions launched 4G roaming service, and has launched 4G network testing in many countries and regions, 4G roaming service in these countries and regions will be gradually opened with the completion of the test [1]. The GSMA developed IPX for operators to enable their subscribers to roam globally and to interconnect its full suite of voice and data services through a secure IPX connection. It defined standards to enable interoperability from technical and commercial perspectives.

LTE network has many features compared with UMTS, it uses more flat, all IP network architecture and has fewer network nodes, faster data transmission rate, more flexible bandwidth, lower transmission delay and seamless connection with other existing wireless communication system etc. These new features meet the business needs and improve the user experience but also bring some security threats.

G. Wang et al. (Eds.): SpaCCS 2017 Workshops, LNCS 10658, pp. 64–73, 2017.
https://doi.org/10.1007/978-3-319-72395-2_7

LTE system is a mobile Internet system based on IP, which means that the LTE will face the challenge of traditional IP Internet security threats too. In the recent past, there have been many instances of flooding attacks on the Domain Name System (DNS) aimed at preventing clients from resolving resource records belonging to the zone under attack [2–4]. At the 2016 European black hat conference [5], researchers at NOKIA's Baer lab tested the simulation on a test network: an attack on an unnamed British mobile operator in Finland. The research team found that the Diameter framework can be used in different ways to interrupt the connection of specific users and nodes. The experiment proves that it can successfully launch Denial of Service (DoS) attacks.

The rest of this paper is organized as follows: Sect. 2 introduces the background knowledge. In Sect. 3, we analyze the security of DNS resolution procedures and describe the possibility of overload in the local DNS and the root DNS. In Sect. 4, a security enhancement scheme is designed, meanwhile we analyze the reliability of the new scheme. the last part is the conclusion part in Sect. 5.

2 Background Knowledge

DNS procedures take place in lots of mobile procedures [6–8]: attach procedure (the data session establishment procedure), inter-MME Tracking Area Update procedure, inter-MME S1-based Handover procedure. Because the first attachment request procedure includes the authentication procedure and the DNS resolution procedure, so this paper will describe the attach procedure in detail as an example. In addition, we will also describe LTE roaming architecture and the DNS resolution procedure.

2.1 LTE Roaming Architecture

Figure 1 represents the roaming with Home routed case. In addition, LTE roaming architecture consists of local breakout case with Application Function (AF) in the Home Network and in the Visited Network, due to space limitation, more information can be viewed in documentation [6].

Home Subscriber Server (HSS) stores subscription and profile information of every user registered in a Home Public Land Mobile Network (HPLMN). In the Visiting Public Land Mobile Network (VPLMN), each User Equipment (UE) connects with an evolved NodeB (eNB) through the Uu interface. eNB is the new enhanced Base Transceiver Station (BTS), provides the LTE air interface and implementation of radio resource management for the evolved access system. An eNB is connected with one or more Mobility Management Entities (MME) through the S1-MME interface. eNB connects Serving Gateway (SGW) through S1-U interface. The MME interacted with the HSS is the key control node for the LTE access network which is responsible for authenticating the user. For obtaining authentication data, the MME communicates with the HSS through the S6a interface. For obtaining the IP address of SGW/PGW, MME communicates with one or more Domain Name Server (DNS). SGW conveys user-plane traffic which connects PDN Gateway through S5/S8 interface, When the roaming network model is Home routed case, S8 interface is used.

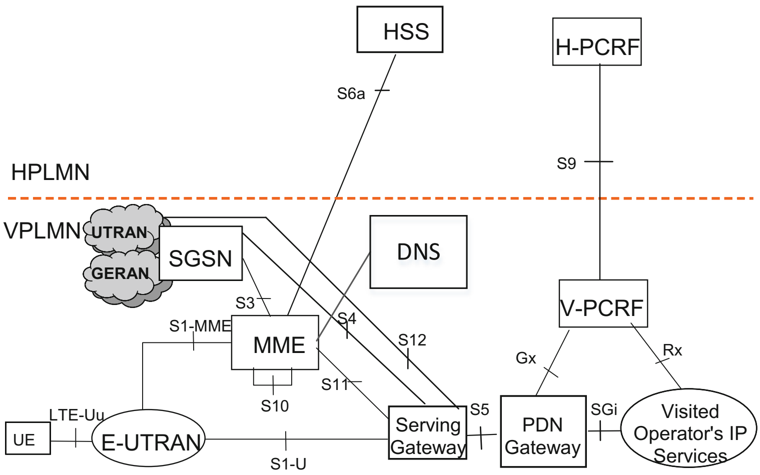


Fig. 1. LTE roaming architecture

2.2 The Attach Procedure

Figure 2 represents the attach procedure lunched by UE (For example, when the phone is turned on), this paper will introduce the key steps related to this topic in detail.

Step 1: The EPS Session Management (ESM) sub-layer of UE-NAS triggers the default PDN connection establishment process, sending the PDN connection request to the EPS Mobility Management (EMM) sub-layer of UE-NAS.
Step 2: The EMM sub-layer of UE triggers the attachment process after receiving the PDN connection request, and the EMM sub-layer of UE sends the Attach Request & PDN connection request to the UE-RRC layer.
Step 3: The RRC layer of UE trigger the RRC connection process after receiving the upper NAS message, send RRC connection request to eNB.
Step 4: eNB sends RRC connection setup response.
Step 5: The UE receives the RRC Connection Setup message, sent to the eNB RRC connection setup complete message which contains NAS information: Attach Request and PDN Connection Request.
Step 6: eNB receives the message, then selects a MME according to selected PLMN-Identity and Globally Unique MME Identifier (GUMMEI). The Initial UE message contain NAS message to MME: Attach Request and PDN Connection Request.
Step 7: After the EMM sub-layer of MME receives the message, the PDN Connection Request is passed to the ESM sub-layer of MME and the EMM of MME sub-layer handles only Attach Request, during the process of attaching the request, EMM of MME requests to the visited DNS for the IP of PGW. The detailed analysis of DNS is in the 2.3 part.
Step 8: EMM sub-layer of MME performs NAS authentication process.
Step 9: The ESM sub-layer of MME receives the PDN Connection Request message and sends the Diameter message to HSS: Location Update Acknowledge, HSS provide the data (PDN signing context, APN-AMBR) to MME.

Step 10: MME sends Create Session Request message to the SGW, which includes the GTP-C tunnel identifier for the down-link MME and the relevant information about the default bearer to be established.

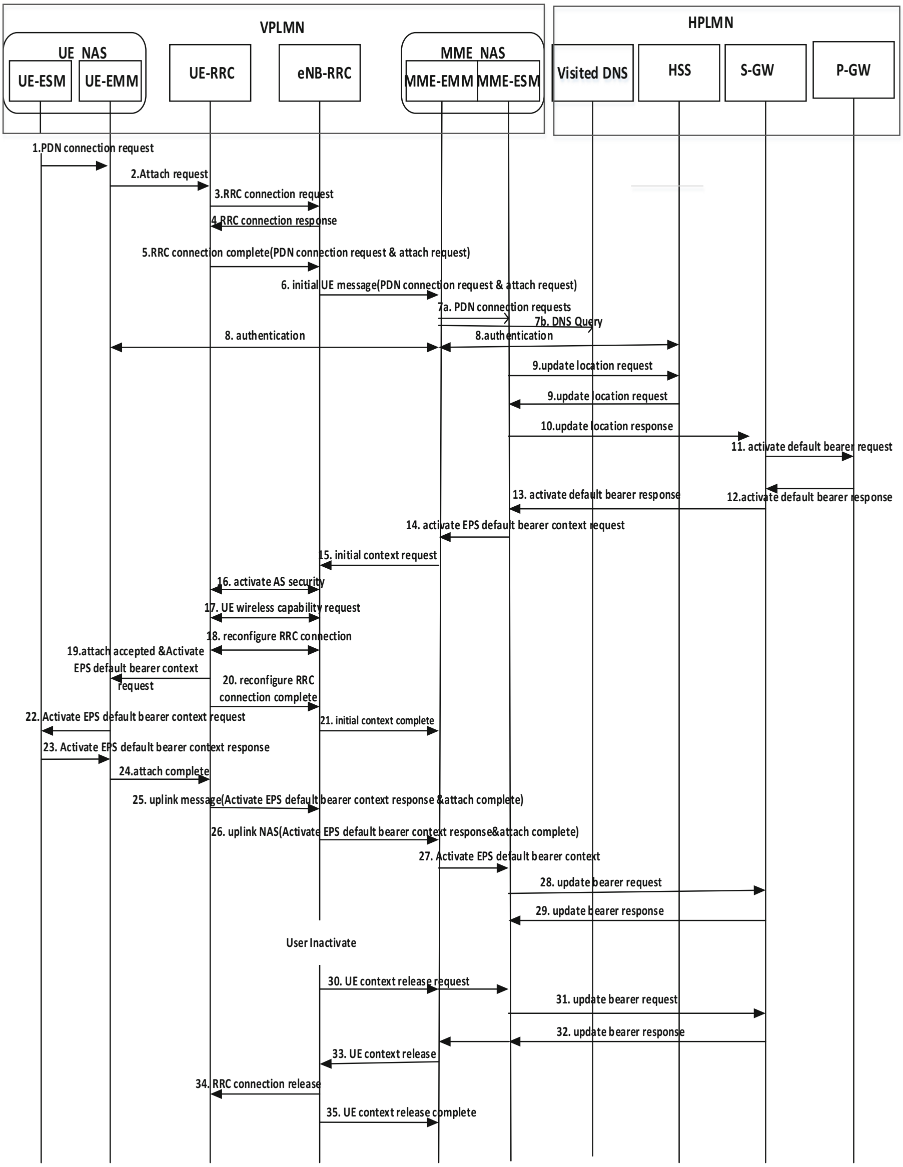

VPLMN
HPLMN
UE NAS
UE-ESM
UE-EMM
UE-RRC
eNB-RRC
MME NAS
MME-EMM
MME-ESM
Visited DNS
HSS
S-GW
P-GW
1.PDN connection request
2.Attach request
3.RRC connection request
4.RRC connection response
5.RRC connection complete(PDN connection request & attach request)
6. initial UE message(PDN connection request & attach request)
7a. PDN connection requests
7b. DNS Query
8. authentication
8.authentication
9.update location request
9.update location request
10.update location response
11. activate default bearer request
12.activate default bearer response
13. activate default bearer response
14. activate EPS default bearer context request
15. initial context request
16. activate AS security
17. UE wireless capability request
18. reconfigure RRC connection
19.attach accepted &Activate EPS default bearer context request
20. reconfigure RRC connection complete
21. initial context complete
22. Activate EPS default bearer context request
23. Activate EPS default bearer context response
24.attach complete
25. uplink message(Activate EPS default bearer context response &attach complete)
26. uplink NAS(Activate EPS default bearer context response&attach complete)
27. Activate EPS default bearer context
28. update bearer request
29. update bearer response
User Inactivate
30. UE context release request
31. update bearer request
32. update bearer response
33. UE context release
34. RRC connection release
35. UE context release complete

Fig. 2. Attach procedure

2.3 DNS Resolution Procedure

DNS is critical to such services as LTE roaming. The DNS call flow mechanism is based on the 3GPP standards defined in the following:

TS 23.401 [6], TS 23.060 [7] for node selection principles
TS 29.303 [8] for DNS procedures
TS 23.003 [9] for node identifiers

Figure 3 shows the typical call-flow for DNS interrogation on the IPX for one operator to resolve a domain name of another operator.

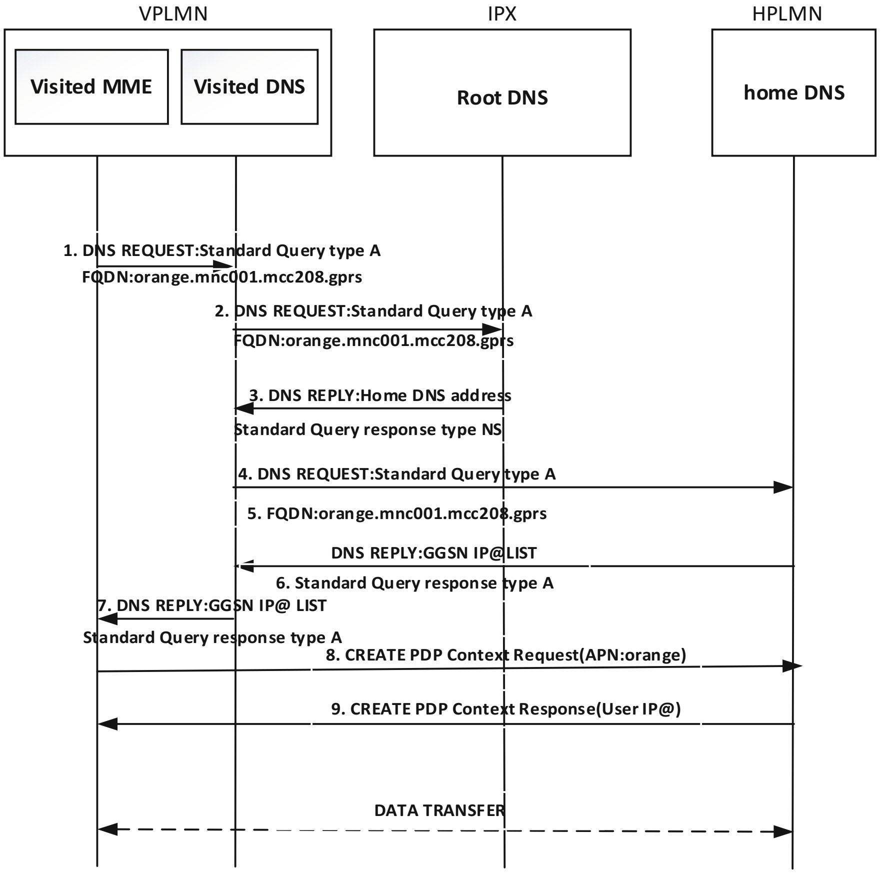

VPLMN
IPX
HPLMN
Visited MME
Visited DNS
Root DNS
home DNS
1. DNS REQUEST:Standard Query type A
FQDN:orange.mnc001.mcc208.gprs
2. DNS REQUEST:Standard Query type A
FQDN:orange.mnc001.mcc208.gprs
3. DNS REPLY:Home DNS address
Standard Query response type NS
4. DNS REQUEST:Standard Query type A
5. FQDN:orange.mnc001.mcc208.gprs
DNS REPLY:GGSN IP@LIST
6. Standard Query response type A
7. DNS REPLY:GGSN IP@ LIST
Standard Query response type A
8. CREATE PDP Context Request(APN:orange)
9. CREATE PDP Context Response(User IP@)
DATA TRANSFER

Fig. 3. DNS resolution procedure

Step 1: MME in VPLMN sends a query for the hostname for which it wants the IP address, to its Local Caching DNS server which is in VPLMN.
Step 2: The visited DNS server checks to see if it has the answer to the query in its cache. If it hit, it answers the visited MME immediately. If it does not hit, it

forwards the query on to the Root DNS server (in IPX). The addresses of the Root DNS server may be statically configured in the Local Caching DNS server.
Step 3: The Root DNS server (in IPX) returns a referral to the visited DNS server which is authoritative for the queried domain name of the host-name.
Step 4: The visited DNS server firstly caches the response for a specified amount of time and then re-sends the query to the Authoritative DNS server which is in HPLMN.
Step 5: The Authoritative DNS server responds to the query with the address of the host-name to the visited DNS server in the requesting network.
Step 6: The visited DNS server caches the response for a specified amount of time and forwards it on to MME.

3 Security Analysis

This paper analyzes the security of DNS server from two aspects: procedure and code of OAI.

3.1 Analysis the Attach Procedure

Some inter-relationship between the NAS and AS protocols is intentionally used to allow procedures to run simultaneously, rather than sequentially as in UMTS. For example, the bearer establishment procedure can be executed by the network without waiting for the completion of the security procedure [11].

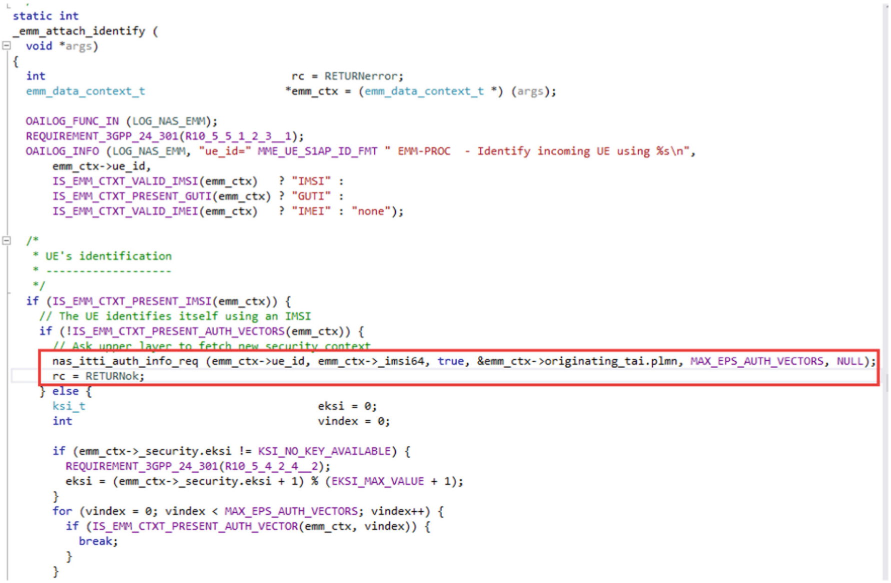
So from the Fig. 2, we can see that step 7 and step 8 are respectively triggered by the EMM sub-layer of MME and the ESM sub-layer of MME. The two sub-layers have a parallel relationship. Step 9 is not obliged to wait for step 8, in other words the ESM sublayer of MME can launch a PDN connection request before the completion of the authentication request, this will lead to some malicious users or malicious software to launch a large number of continuous requests to the MME, resulting in excessive load on the local DNS server, this scheme is very vulnerable to DoS/DDoS attacks on the local DNS server. In addition if the local DNS server does not hit these requests, the local DNS server will send DNS requests to the root DNS server in IPX, which will cause excessive load on the root DNS server. In this scenario, the root DNS server in IPX is vulnerable to DoS/DDoS attack, which will exert a great influence on the international roaming service. The root server can serve a user that does not pass authentication, which is one of the weaknesses of IPX.

3.2 Analysis the Attach Code in OpenAirInterface (OAI)

(OpenAirInterface) OAI [10] is an open source software, and it can run in the traditional Linux system without extra configuration, more and more academic organizations, equipment manufacturers and operators are using and joining the design and development process of OAI open source software, it is gradually applied in the research work and production environment.

In addition to call-flow analysis, this paper also analyzes the security risks faced by DNS according to the OAI code.

Figure 4 is the _emm_attach_identify function which is in \openair-cn\SRC\NAS\ nas_itti_messaging.c, the function execute the attach procedure requested by the UE. It checkes the IMSI firstly, then it sends authentication request to s6a_task.c.



```
static int
_emm_attach_identify (
  void *args)
{
  int                                     rc = RETURNerror;
  emm_data_context_t                     *emm_ctx = (emm_data_context_t *) (args);

  OAILOG_FUNC_IN (LOG_NAS_EMM);
  REQUIREMENT_3GPP_24_301(R10_5_5_1_2_3__1);
  OAILOG_INFO (LOG_NAS_EMM, "ue_id=" MME_UE_S1AP_ID_FMT " EMM-PROC  - Identify incoming UE using %s\n",
      emm_ctx->ue_id,
      IS_EMM_CTXT_VALID_IMSI(emm_ctx)   ? "IMSI" :
      IS_EMM_CTXT_PRESENT_GUTI(emm_ctx) ? "GUTI" :
      IS_EMM_CTXT_VALID_IMEI(emm_ctx)   ? "IMEI" : "none");

  /*
   * UE's identification
   * -------------------
   */
  if (IS_EMM_CTXT_PRESENT_IMSI(emm_ctx)) {
    // The UE identifies itself using an IMSI
    if (!IS_EMM_CTXT_PRESENT_AUTH_VECTORS(emm_ctx)) {
      // Ask upper layer to fetch new security context
      nas_itti_auth_info_req (emm_ctx->ue_id, emm_ctx->_imsi64, true, &emm_ctx->originating_tai.plmn, MAX_EPS_AUTH_VECTORS, NULL);
      rc = RETURNok;
    } else {
      ksi_t                                   eksi = 0;
      int                                     vindex = 0;

      if (emm_ctx->_security.eksi != KSI_NO_KEY_AVAILABLE) {
        REQUIREMENT_3GPP_24_301(R10_5_4_2_4__2);
        eksi = (emm_ctx->_security.eksi + 1) % (EKSI_MAX_VALUE + 1);
      }
      for (vindex = 0; vindex < MAX_EPS_AUTH_VECTORS; vindex++) {
        if (IS_EMM_CTXT_PRESENT_AUTH_VECTOR(emm_ctx, vindex)) {
          break;
        }
      }
```

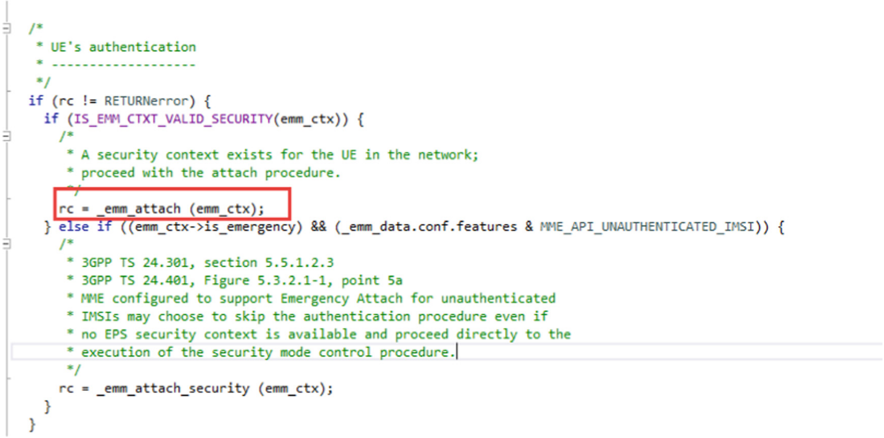
Fig. 4. Flow chart of _emm_cn_pdn_connectivity_res

Figure 5 presents another part of the _emm_attach_identify function which is in \openair-cn\SRC\NAS\ nas_itti_messaging.c. It checkes the return value firstly, if the return value is not error, then it trigger the attachment request.

From the Fig. 4, we can see that the rc is directly assigned to RETURNok, which dose not wait for the result of the authentication and does not have any nothing with the authentication result, because rc is assigned to RETURNok, so the attachment request judgment can be directly executed, and did not have any relationship with the authentication result.

4 Security Enhancement Scheme and Reliability Analysis

The smart-phone is increasing gradually, Mobile phone virus is also growing. Mobile malware can create smart-phone botnets in which a large number of mobile devices conspire to perform malicious activities on the cellular network. Smart-phone botnets will be a major security threat faced by LTE networks, criminals can use its control of the botnets to launch a massive attack on DoS/DDoS mobile communication network. The authors in [12, 13] studied the feasibility of DoS attack and analyzes its impact on



```
/*
 * UE's authentication
 * ------------------
 */
if (rc != RETURNerror) {
  if (IS_EMM_CTXT_VALID_SECURITY(emm_ctx)) {
    /*
     * A security context exists for the UE in the network;
     * proceed with the attach procedure.
     */
    rc = _emm_attach (emm_ctx);
  } else if ((emm_ctx->is_emergency) && (_emm_data.conf.features & MME_API_UNAUTHENTICATED_IMSI)) {
    /*
     * 3GPP TS 24.301, section 5.5.1.2.3
     * 3GPP TS 24.401, Figure 5.3.2.1-1, point 5a
     * MME configured to support Emergency Attach for unauthenticated
     * IMSIs may choose to skip the authentication procedure even if
     * no EPS security context is available and proceed directly to the
     * execution of the security mode control procedure.
     */
    rc = _emm_attach_security (emm_ctx);
  }
}
```

Fig. 5. Code of emm_attach

QoS. Lain et al. in [14], in the roaming LTE network, realize a pulse DoS using the lack of coordination between local and remote components of the LTE network during the roaming authentication process.

Figure 6 shows the percentage of response of the DNS server with different configurations to the request packet. From the diagram, the percentage of the response will drop suddenly when the requested data reaches 1600.

In the Internet, although it is difficult to distinguish normal traffic and DoS attack traffic because the DoS attackers generally hide their true identities/origins, there have been many solutions for DoS/DDoS attack on DNS.

Ayyaz et al. in [15] proposed a security system which keeps track of every IP address of connecting device and provide services to each host based on the set threshold. by implementing a firewall in the network. Chiba et al. in [16] have proposed a new filtering scheme to mitigate the effect of DDoS attack by registering the correspondence DNS query and responsed to the ingress filtering rule of the firewall. The authors in [17, 18] monitor the traffic flow using the CUSUM algorithm. The authors in [19, 20] prevent DoS attacks by improving cache structure, according to the characteristics of TTL.

In this paper, we can set the cache in MME according to the characteristics of LTE. When there is a DNS query request, MME first query in its own cache, if the cache records this information, it is not necessary to initiate DNS request, only when records in the MME cache do not contain this information, it initiates the DNS request. This can reduce the load on the DNS server.

Because the hardware conditions can be easily upgraded, and the cost is lower and lower. If the MME cache hit, due to the omission of the DNS request, it can reduce the delay. If the MME cache does not hit, it can complete the local query in a very short time by adding fast cache in MME. For MME, because the cache is running very fast, the delay caused by it can not have a great impact on the overall efficiency, so on the whole, the quality of service (QoS) will not be reduced.

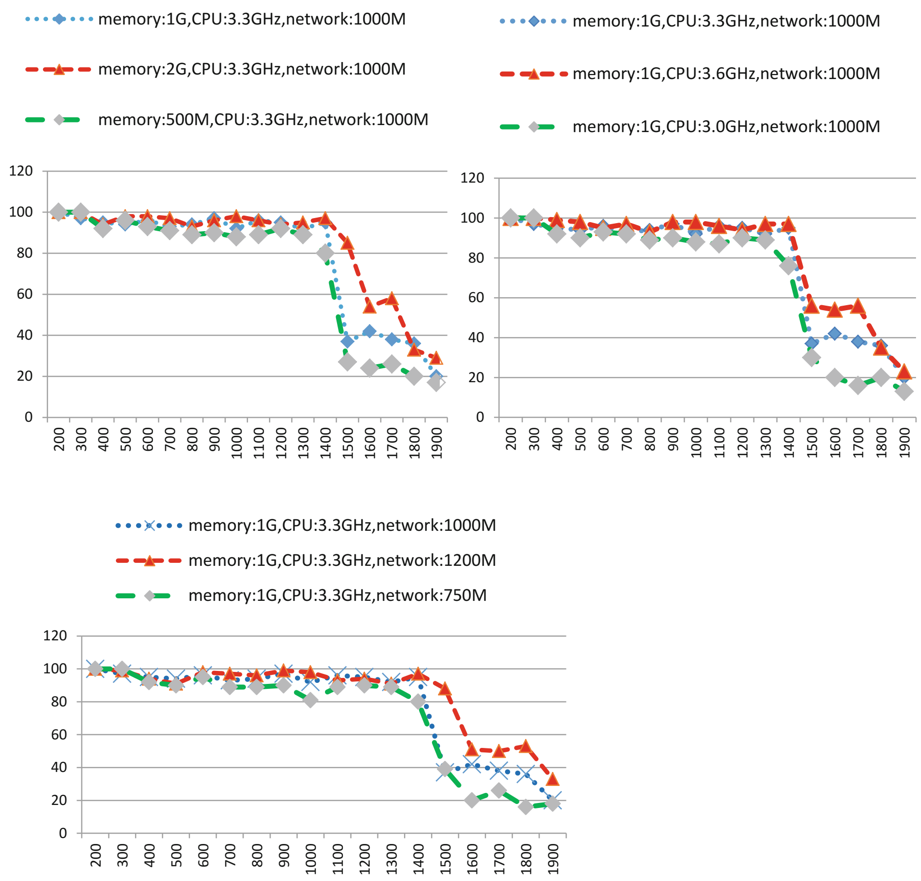


Fig. 6. Percentage of response packets

5 Conclusions

In this paper, we first introduced the LTE roaming architecture, the attach procedure and the DNS resolution procedure. By analyzing the procedure and OAI code, we reveal that MME initiated the DNS request before the authentication was completed, which will likely lead to DoS/DDoS attacks on DNS. Finally, according to the characteristics of LTE, we propose a enhancement scheme in MME and analyze the feasibility.

References

1. http://www.10086.cn/aboutus/news/GroupNews/201504/t20150429_58803.htm
2. Microsoft DDoS Attack, NetworkWorld, January 2001. http://www.networkworld.com/news/2001/0125mshacked.html

3. UltrDNS DDoS Attack, Washington Post, May 2005. http://blog.washingtonpost.com/securityfix/2006/05/blue_security_surrenders_but_s.html
4. http://it.sohu.com/20161025/n471217376.shtml
5. http://www.blackhat.com/eu-16
6. 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
7. 3GPP TS 23.060: General Packet Radio Service (GPRS) service description
8. 3GPP TS 29.303: Domain Name System Procedures
9. 3GPP TS 23.003: Numbering, addressing and identification
10. http://www.openairinterface.org/
11. Sesia, S., Toufik, I., Baker, M.: LTE-The UMTS Long Term Evolution from Theory to Practice. The People's Posts and Telecommunications Press (Posts & Telecom Press), Beijing (2009)
12. Jermyn, J., Sallesloustau, G., Zonouz, S.: An analysis of DoS attack strategies against the LTE RAN. J. Cyber Secur. **3**(2), 159–180 (2014)
13. Henrydoss, J., Boult, T.: Critical security review and study of DDoS attacks on LTE mobile network. In: 2014 IEEE Asia Pacific Conference on Wireless and Mobile, pp. 194–200. IEEE (2014)
14. Ambrosin, M., Cecconello, S., Conti, M., Lain, D.: A roaming-based denial of service attack on LTE networks: poster. In: ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 283–284. ACM (2017)
15. Ayyaz, S., Khan, M.A., Ahmad, J., et al.: A novel security system for preventing DoS attacks on 4G LTE networks. In: International Conference on Wireless Networks, ICWN (2016)
16. Chiba, T., Katoh, T., Bista, B.B., et al.: DoS packet filter using DNS information. In: 20th International Conference on Advanced Information Networking and Applications, pp. 1–6. IEEE (2006)
17. Wang, H., Zhang, D., Shin, K.G.: Change-point monitoring for detection of DoS attacks. IEEE Trans. Dependable Secure Comput. **1**(4), 193–208 (2004)
18. Lee, P.P.C., Bu, T., Woo, T.: On the detection of signaling DoS attacks on 3G wireless networks. In: IEEE International Conference on Computer Communications, INFOCOM 2007, pp. 1289–1297. IEEE (2007)
19. Ballani, H., Francis, P.: A simple approach to DNS DoS mitigation. ACM Sigcomm Hotnets **12**(34), 5536–5539 (2016)
20. Pappas, V., Zhang, B., Osterweil, E., Massey, D., Zhang, L.: Improving DNS Service Availability by Using Long TTLs. draft-pappas-dnsop-long-ttl-02. June 2006