World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:6, No:9, 2012

3G WCDMA Mobile Network DoS Attack and Detection Technology

JooHyung Oh, Dongwan Kang, Sekwon Kim, ChaeTae Im

***Abstract*—**Currently, there has been a 3G mobile networks data traffic explosion due to the large increase in the number of smartphone users. Unlike a traditional wired infrastructure, 3G mobile networks have limited wireless resources and signaling procedures for complex wireless resource management. And mobile network security for various abnormal and malicious traffic technologies was not ready. So Malicious or potentially malicious traffic originating from mobile malware infected smart devices can cause serious problems to the 3G mobile networks, such as DoS and scanning attack in wired networks. This paper describes the DoS security threat in the 3G mobile network and proposes a detection technology.

***Keywords*—**3G, WCDMA, DoS, Security Threat

I. Introduction

CURRENTLY 3G mobile networks such as WCDMA and CDMA 2000 have been built. As of December 2005, there were over 300 million CDMA subscribers worldwide. Emerging 3G mobile network standards such as EV-DO and HSDPA promise to deliver broadband mobile internet services with peak rates of 2.4 Mbps and 14.4 Mbps, and HSPA+ will allow uplink speeds of 11Mbps and downlink speeds of 42Mbps, respectively. Also 3G mobile networks with a higher mobility than a Wi-Fi environment was provided.

However, there has been a 3G mobile network data traffic explosion due to the large increase in the number of smartphone users. Also, new mobile services to satisfy the various needs of smartphone users are being developed day by day. In other words, this means an increase in data traffic over the mobile networks. [1][2].

Furthermore, with the growing popularity of the tethering service, which enables the use of a mobile communication terminal as an Internet modem, malicious traffic from the wired environment (e.g., PCs) is moving into the mobile communication network.

However, no security technology has yet been applied to the equipment that constitutes the mobile communication network, as the domestic communication network has a closed service provision structure that allows strict traffic control by the service provider. Therefore, it is difficult to deal with a smartphone infected by malicious mobile codes and malicious traffic flowing from the wired environment. In addition, existing network security equipment detects and responds to harmful traffic based on the IP.

However, it is impossible to apply violation prevention technology in the existing Internet network, because the mobile communication network allocates the IP address dynamically each time a terminal accesses the network, and most organizations use the NAT-based private IP address.

Many study projects aimed at developing security technology exclusively for the mobile communication environment are mainly conducted by universities and research institutes. The METAWIN and DARWIN projects implemented in Europe between 2004 and 2009 analyzed data traffic on the 3G mobile network in order to develop a technology capable of detecting and coping with abnormal traffic, which can cause network errors. A study on a technology for removing security threats, which can occur while migrating to the 4G LTE network, has been conducted under the ASMONIA project in Germany since 2010 [4][5]. In addition, ERNW, a security consulting service firm based in Germany, released an attack tool that can obtain the IP address of the network component needed for a DoS attack on the 3G mobile network, and also released a DoS attack on the 3G mobile network, using the GTP Echo scan message [9][10].

As described above, studies on attacks/security attacks that are peculiar to the mobile network and countermeasure technologies are continuously being carried out in foreign countries. However, researches and investments in the development of violation prevention technologies, which are specialized in the mobile communication network, are lacking in Korea, and even security threats released abroad have not been properly identified. Accordingly, this paper explains the DoS security threat caused by major resource exhaustion and equipment overload on the commercial 3G mobile network, and proposes a countermeasure technology.

This paper is composed as follows: Chapter 2 describes the vulnerabilities of the commercial 3G mobile network in Korea, and the DoS attack on the 3G mobile network that exploits these vulnerabilities; Chapter 3 explains the technology designed to respond to the DoS attack; and Chapter 4 presents the conclusion and proposals for future studies.

II. DoS Attack on the 3G WCDMA mobile network

The 3G mobile network uses the GTP protocol for network control and data transfer inside the network [7][8]. If a normal user attempts to access the Internet using the 3G data service, the GTP-C message is used to allocate the IP address to the user inside the network, and the user data is sent to the Internet network using the GTP-U message.

As shown in Fig. 1, the IP address and tunnel ID possessed by the GGSN(Gateway GPRS Support Node) are allocated, using the GTP-C message transmitted between the SGSN(Serving GPRS Support Node) and the GGSN; the IP address and tunnel ID are sent to the user terminal; and user traffic is sent via the GTP-U tunnel that is created later on.

JooHyung Oh is with the Korea Internet & Security Agency, Seoul, Korea (phone: 82-2-405-5282; fax: 82-2-405-5129; e-mail: jhoh@ kisa.or.kr).

Dongwan Kang is with the Korea Internet & Security Agency, Seoul, Korea (phone: 82-2-405-5257; fax: 82-2-405-5129; e-mail: lupin@ kisa.or.kr).

Sekwon Kim is with the Korea Internet & Security Agency, Seoul, Korea (phone: 82-2-405-5422; fax: 82-2-405-5129; e-mail: heath82@ kisa.or.kr).

ChaeTae Im is with the Korea Internet & Security Agency, Seoul, Korea (phone: 82-2-405-5540; fax: 82-2-405-5129; e-mail: chtim@ kisa.or.kr).

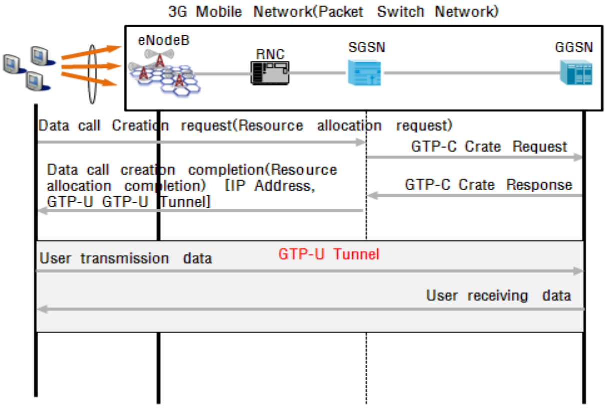

3G Mobile Network(Packet Switch Network)
eNodeB
RNC
SGSN
GGSN
Data call Creation request(Resource allocation request)
GTP-C Crate Request
Data call creation completion(Resource allocation completion) [IP Address, GTP-U GTP-U Tunnel]
GTP-C Crate Response
User transmission data
GTP-U Tunnel
User receiving data

Fig. 1 Usage flow of the 3G mobile Internet service

A. GTP-in-GTP based DoS Attack

GGSN installed at 3G WCDMA mobile network has GTP-in-GTP vulnerability. If the user terminal sends a malicious GTP-C message, a GTP-in-GTP type packet can be sent to the inside of the 3G mobile network via the GGSN.

The GGSN in the 3G network sends the user data received from the SGSN to the Internet network, based on the destination IP address. If the user sets the GTP-C message as the GGSN's IP address, it will be sent to the GGSN, as shown in Fig. 1

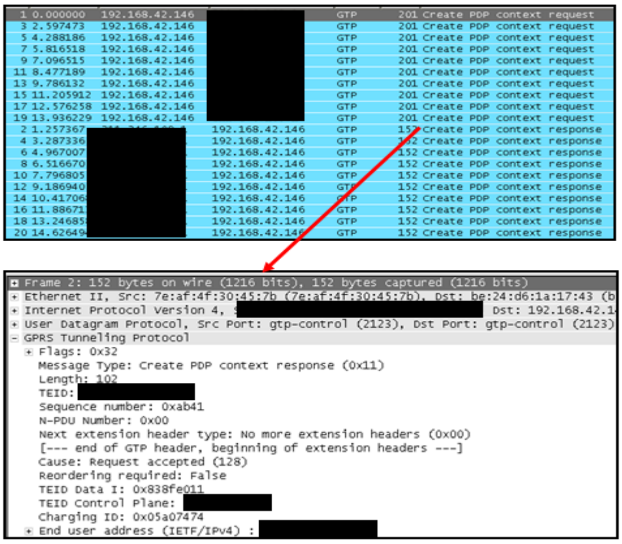
If the GTP-C message for 3G WCDMA mobile network control, such as IP address allocation for the 3G mobile network, sends the GGSN's IP address to the destination via the terminal, the IP address resource can be allocated abnormally. This type of GTP-in-GTP packet processing vulnerability can be exploited in most GGSNs installed in the domestic commercial service environment, and the P-GATEWAT equipment in the 4G LTE network that performs a similar function to the 3G network's GGSN as well.

If the terminal creates many "GTP-C Create PDP Context" messages and sends them to the GGSN's IP address, the TEID and IP address of the GGSN are allocated abnormally. Likewise, a DoS attack can be launched against normal users that use the 3G mobile Internet service, if the TEID and IP address of the GGSN are exhausted by exploiting the GGSN's GTP-in-GTP packet processing vulnerability.

B. Signaling DoS Attack

The 3G mobile network releases the allocated wireless resource, if the mobile terminal doesn't transmit the data for a certain period of time, in order to use the limited wireless resource efficiently. By taking advantage of this architecture, a DoS attack that causes RNC and SGSN overload using multiple signaling messages can be launched.

The signal message can be created by maliciously and abnormally repeating wireless resource re-allocation right after resource release [5].


```
  1 0.000000   192.168.42.146  [redacted]         GTP   201 Create PDP context request
  3 2.597473   192.168.42.146                     GTP   201 Create PDP context request
  5 4.288186   192.168.42.146                     GTP   201 Create PDP context request
  7 5.816518   192.168.42.146                     GTP   201 Create PDP context request
  9 7.096515   192.168.42.146                     GTP   201 Create PDP context request
 11 8.477189   192.168.42.146                     GTP   201 Create PDP context request
 13 9.786132   192.168.42.146                     GTP   201 Create PDP context request
 15 11.205912  192.168.42.146                     GTP   201 Create PDP context request
 17 12.576258  192.168.42.146                     GTP   201 Create PDP context request
 19 13.936229  192.168.42.146                     GTP   201 Create PDP context request
  2 1.257367   [redacted]      192.168.42.146     GTP   152 Create PDP context response
  4 3.287336                   192.168.42.146     GTP   152 Create PDP context response
  6 4.967007                   192.168.42.146     GTP   152 Create PDP context response
  8 6.516670                   192.168.42.146     GTP   152 Create PDP context response
 10 7.796805                   192.168.42.146     GTP   152 Create PDP context response
 12 9.186940                   192.168.42.146     GTP   152 Create PDP context response
 14 10.41706                   192.168.42.146     GTP   152 Create PDP context response
 16 11.88671                   192.168.42.146     GTP   152 Create PDP context response
 18 13.24685                   192.168.42.146     GTP   152 Create PDP context response
 20 14.62649                   192.168.42.146     GTP   152 Create PDP context response
```

```
⊞ Frame 2: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits)
+ Ethernet II, Src: 7e:af:4f:30:45:7b (7e:af:4f:30:45:7b), Dst: be:24:d6:1a:17:43 (b
+ Internet Protocol Version 4, [redacted] Dst: 192.168.42.1
+ User Datagram Protocol, Src Port: gtp-control (2123), Dst Port: gtp-control (2123)
- GPRS Tunneling Protocol
  + Flags: 0x32
    Message Type: Create PDP context response (0x11)
    Length: 102
    TEID: [redacted]
    Sequence number: 0xab41
    N-PDU Number: 0x00
    Next extension header type: No more extension headers (0x00)
    [--- end of GTP header, beginning of extension headers ---]
    Cause: Request accepted (128)
    Reordering required: False
    TEID Data I: 0x838fe011
    TEID Control Plane: [redacted]
    Charging ID: 0x05a07474
  + End user address (IETF/IPv4) : [redacted]
```

Fig. 2 GTP message sample that allocates resources to the 3G mobile network abnormally

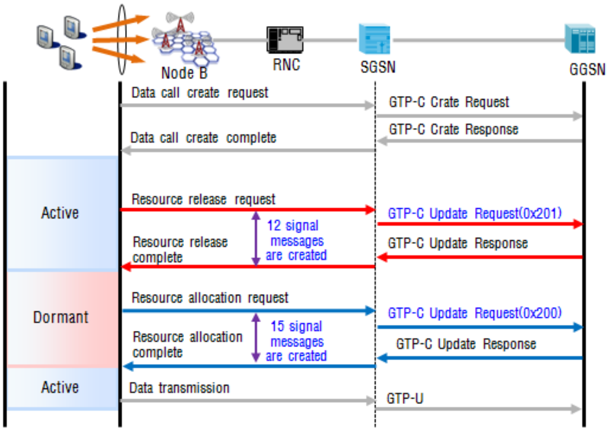

Node B
RNC
SGSN
GGSN
Data call create request
GTP-C Crate Request
GTP-C Crate Response
Data call create complete
Active
Resource release request
GTP-C Update Request(0x201)
12 signal messages are created
Resource release complete
GTP-C Update Response
Dormant
Resource allocation request
GTP-C Update Request(0x200)
15 signal messages are created
Resource allocation complete
GTP-C Update Response
Active
Data transmission
GTP-U

Fig. 3 Wireless resource allocation/release flow diagram of the 3G mobile network

As shown in Fig.3, if the active terminal doesn't establish the data communication for a certain period of time, a wireless resource release request message will be sent to the SGSN to switch to the dormant mode. In addition, if the terminal in a dormant mode transmits the data, the terminal can be switched to an active mode again by sending a wireless resource allocation message to the SGSN. Using this mode switching method, the 3G mobile network manages the limited wireless resource efficiently. When the wireless resource is maliciously and abnormally allocated/released, small traffic is sent at a particular interval to switch the dormant mode of the terminal to the active mode, and many signaling messages are created, which results in a DoS attack by causing overload on the RNC and SGSN.

III. Detection Method of 3G Mobile Network DoS Attack

In this section, detection methods of 3G mobile network DoS attack will be described in detail.

A. GTP-in-GTP based DoS Attack Detection

GTP-in-GTP based DoS attack can be detected and blocked by analyzing the packet port number on the GGSN that decapsulates the GTP packet for the first time. GTP-in-GTP packets are decapsulated first on the GGSN. At this time, the pre-defined GTP-C packet can be blocked, based on the transmitting UDP port number. As shown in Fig. 4, packets can be blocked if the packet port number is 2123, which is used by the GTP-C message, after decapsulation of the GTP-U message on the GGN.

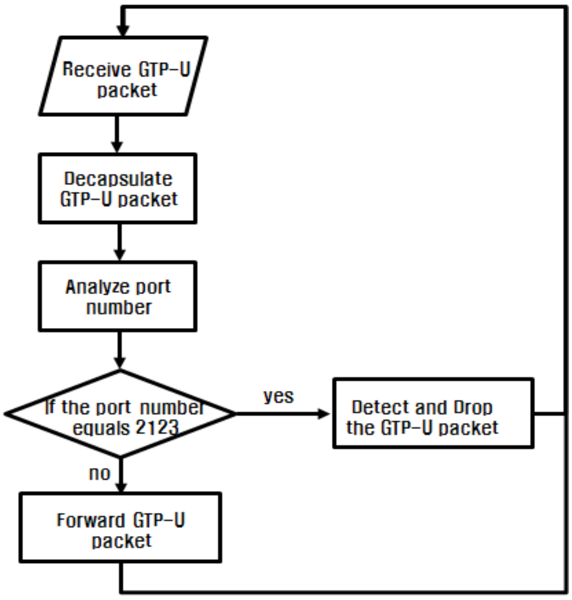


Fig. 4 Flowchart of GTP-in-GTP packet blocking technology for the 3G mobile network

However, this type of countermeasure is designed to collectively block user traffic that uses similar traffic (that is, GTP-C port numbers), rather than blocking the GTP-in-GTP message. According to the results of a commercial 3G mobile network traffic analysis, much UDP traffic uses the GGSN port. For more accurate GTP-in-GTP packet detection and blocking, the GTP-U message should be collected in real time in the Gn section that transmits the GTP message, and the GTP-C message inside the GTP-U should be detected by analyzing the GTP-U message. As the normal mobile terminal cannot send a GTP-C message that is used inside the mobile network, only GTP-in-GTP packets can be selected, by detecting the GTP-C message inside the GTP-U message. The suspected GTP-C packet can be selected first by analyzing the GTP-U payload received from the user, and the GTP-C message inside the GTP-U message can be accurately detected and blocked, by measuring length according to the type of GTP-C message.

B. Signaling DoS Detection

The signaling DoS attack can be detected by analyzing the GTP-C/U collected from the Gn sector. For malicious/abnormal wireless resource allocation, either no transmission traffic at all or only small-volume traffic is generated during the active to dormant switching period. Also, the time difference between wireless resource allocation/release and allocation/release is small to generate a large amount of signal messages in a short period of time.

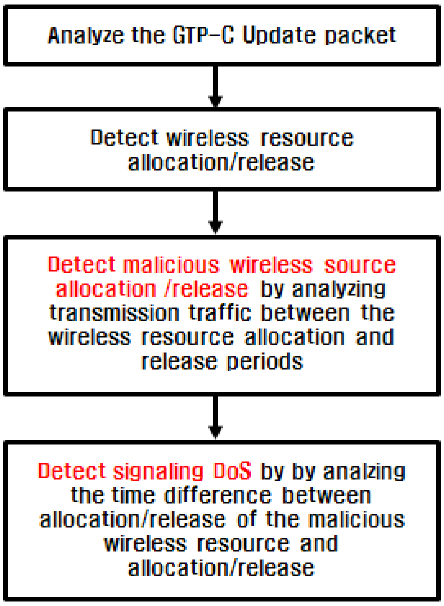

Analyze the GTP-C Update packet
Detect wireless resource allocation/release
Detect malicious wireless source allocation /release by analyzing transmission traffic between the wireless resource allocation and release periods
Detect signaling DoS by by analzing the time difference between allocation/release of the malicious wireless resource and allocation/release

Fig. 5 Flow chart of signaling DoS detection technology of the 3G mobile network

Therefore, as shown in Fig. 5, wireless resource allocation/release can be detected by analyzing the GTP-C Update Request message that is created while the terminal is switching from the active mode to the dormant mode, and back to the active mode. Also, malicious/abnormal wireless resource allocation can be detected by analyzing transmission traffic during the wireless resource allocation – release period. By analyzing the time difference between malicious/abnormal wireless resource allocation/release detected in this way and allocation/release, the signaling DoS caused by malicious/abnormal wireless resource allocation can be detected. The mobile terminal that causes the signaling DoS maliciously and abnormally can be handled by deleting the pre-determined data call. Unlike GTP-in-GTP, the signaling DoS can be created abnormally by firmware during the terminal manufacturing process. Therefore, even when the signaling DoS have been detected, it cannot be blocked on the 3G mobile network. Therefore, the signaling DoS can be prevented by deleting the terminal data call, if the "GTP-C Delete PDP Context" message is created and sent to the GGSN, using the tunnel ID information of the terminal that detects the signaling DoS attack.

IV. Conclusion

Due to the open nature of the mobile network and the increasing popularity of high-performance smartphones, diverse abnormal traffic is flowing into the network, leading to 3G mobile network DoS attack. As the 3G mobile network uses a protocol specialized in the G3 environment like GTP, and uses the private IP address based on the NAT network, it is impossible to apply security technology based on the IP protocol of the wired environment. This paper explains the 3G mobile network resource exhaustion type of DoS attack and the signaling DoS attack, which exploits the GTP-in-GTP packet processing vulnerability in the domestic 3G mobile network, and proposes a countermeasure technology specialized in the 3G mobile network.

Security product vendors in Korea cannot invest in technology development, because awareness of the importance of 3G-mobile network security is low, and the market for 3G mobile network security products has not yet formed. Therefore, as a further study, the proposed technology will actually be implemented as a system to distribute the related technologies

ACKNOWLEDGMENT

This research was supported by the KCC(Korea Communications Commission), Korea, under the R&D program supervised by the KCA(Korea Communications Agency)"(KCA-2012-11912-06001)

REFERENCES

[1] Mobile Traffic Data(2011~2016), CISCO VNI Mobile, 2012.
[2] Global Mobile Data Traffic. By Type, Morgan Stanley, 2010.
[3] Kang, D., Oh, J., and Im, C., Security Threats and Countermeasures on the 3G Network, Proceedings of ICCCIT 2011, October 2011.
[4] DARWIN, http:// http://userver.ftw.at/~ricciato/darwin/
[5] ASMONIA, http:// www.asmonia.de
[6] ERNW, http:// ernw.de/content/e6/e180/index_ger.html
[7] H. Holma, A. Toskala, WCDMA for UMTS – Radio Access for third Generation Mobile Communications 3rd, Willey, 2004.
[8] 3GPP, GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 10), TS 29.060 V10.2.0, 2011.
[9] Lee, P., Bu, T., and Woo, T., On the Detection of Signaling DoS Attacks on 3G Wireless Networks, Proceedings of InfoCom 2007, May 2007.
[10] V. Falletta, F Ricciato, P. Romirer-Maierthofer “Traffic Analysis at Short Time-Scales: An Empirical Case Study from a 3G Cellular Network,” IEEE Transactions on Networks and Service Management, Vol.5, No.1, pp.11-21, March, 2009.