Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/070626

A Practical Attack on Mobile Data Network Using IP Spoofing

Dong W. Kang *, *Joo H. Oh, Chae T. Im, Wan S. Yi and Yoo J. Won*

Korea Internet & Security Agency, IT Venture Tower, Jungdaero 135, Songpa, Seoul, Korea

Received: 17 Mar. 2013, Revised: 18 Jul. 2013, Accepted: 21 Jul. 2013
Published online: 1 Nov. 2013

Abstract: As the mobile Internet has become widespread in recent years, communication based on mobile networks is increasing. As a result, security threats have been posed with regard to the abnormal traffic of mobile networks, but mobile security has been handled with focus on threats posed by mobile malicious codes, and researches on security threats to the mobile network itself have not attracted much attention. In this paper, we analyzes security threats that occurred to mobile networks recently, and checks the security threats likely to occur in actual commercial service networks and their results. We propose a countermeasure that can respond to such security threats, present results that can be applied to actual commercial networks, and thus make it possible to proactively respond to security threats described in this paper.

Keywords: Mobile Network Security, GTP, IP Spoofing, Overbilling

1 Introduction

Looking at the history of mobile communication, mobile communication started as voice service with focus on AMPS(Advanced Mobile Phone Service), the representative 1G (First Generation) mobile communication, in 1978, and voice and data service began to be provided at the same time with 2G represented by CDMA (Code Division Multiple Access). Afterwards, mobile communication is evolving beyond 3G WCDMA (Wideband Code Division Multiple Access) capable of providing faster data services, and LTE (Long Term Evolution) called 3.9G into 4G mobile communication. Early mobile communication service was developed for voice communication, but as the Internet in the wired environment advanced, demands for mobile service, which provides mobility based on mobile communication service, increased. Accordingly, data networks for providing data communication as well as voice service were added to mobile networks, and voice is processed as VoIP (Voice over Internet Protocol) in accordance with the All-IP communication paradigm. The importance of IP-based data networks is growing gradually.

The data service provided by early mobile networks started out as a type of mobile service provided by communication companies in a limited way, but the advances of the Internet and mobile operating system created a mobile ecosystem. At the same time, mobile networks are open to the Internet, and various services in the wired environment were offered in the mobile environment as well. As a result, the data communication volume of mobile networks increased explosively, and is expected to rise continuously in the future [1].

As the increased traffic includes not only the traffic for various mobile service, but also the traffic in the wired environment that could not be seen in existing mobile networks, unnecessary abnormal traffic also increased. In the conventional wired environment, the increased traffic did not mean much to the receiver unless there are large quantities of abnormal traffic like UDP (User Datagram Protocol) packets and TCP (Transmission Control Protocol) packets, which failed to connect. However, in mobile networks, due to the narrow bandwidth, complicated signaling for management of wireless resources, and operation of limited resources, traffic, which did not matter in the existing wired environment, can become a security threat in the mobile network. Also, aggressive security threats, likely to cause the failure of mobile networks, may cause not only data services, but also voice services to fail unless they are responded to in advance [2].

* Corresponding author e-mail: lupin428@kisa.or.kr

At present, as most security systems are optimized to IP-based wired networks, they processes mostly IP protocols, and identify send and receive objects based on IPs. However, mobile networks protocols specialized for mobile networks like GTP (General Packet Radio Service Tunneling Protocol) [3], and IP is not the unique value that can identify a user. Also, as abnormal traffic for mobile networks may look different than that for the wired environment, it is very difficult to bring the security systems for the wired environment inside the mobile network.

The mobile network is the backbone network of the country. If an important infrastructure fails, the repercussions are enormous. In this paper, we analyzes security threats likely to occur in mobile data networks, in particular, security threats using IP spoofing likely to affect the charging system and deteriorate service quality for users of mobile service, proves them in actual commercial service networks, and proposes a countermeasure. The proposed countermeasure is to analyze protocols specialized for mobile networks like GTP, detect and block abnormal traffic, and extract information like the phone number of the user that caused the abnormal traffic. Chapter 2 briefly describes the structure of the mobile network, and Chapter 3 discusses the security threats of mobile networks including IP Spoofing. Chapter 4 proves the security threats in actual commercial service networks, and Chapter 5 proposes countermeasures.

2 Mobile Network and Related Work

2.1 3G/LTE Network

The basic configuration includes the mobile terminal (aka UE: User Equipment), base stations, and the mobile network for control and communication. In general, from the terminal to the external Internet, the mobile network has the hierarchical tree structure. The closer it is to the outside, the more integrated the components are.

3G network[4] provides data service through UTRAN (Universal Mobile Telecommunication System Terrestrial Radio Access Network) and PN (Packet Network) as shown in Fig. 1. UTRAN consists of base stations that communicate with UEs and RNC(Radio Network Controller) that controls base stations. UTRAN communicates with PN, and PN is connected to the external network like the Internet. The protocols, used in the 3G mobile networks, are separately composed of the control protocol for controlling data communication and the data protocol for transmitting actual data. There are various protocols for communication between complicated mobile network components that perform different functions respectively, and particularly in the data network, GTP-C v1 is used as the core control protocol. In the data protocol, the IP packets sent from UEs are relayed to outside of PN. At this time, the core protocol used in PN is GTP-U. GTP-C v1 and GTP-U vary depending on the message type of GTP.

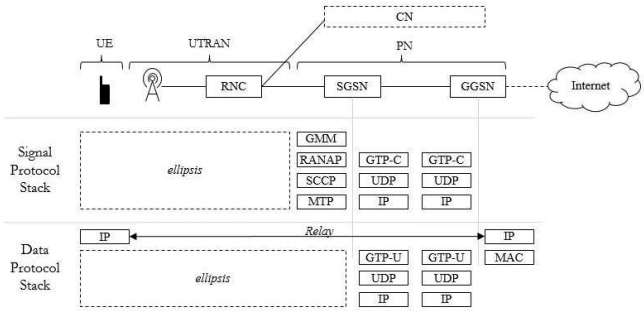

Fig. 1: 3G mobile network structure

In LTE network[5], UTRAN evolved to E-UTRAN (Evolved UTRAN), and PN also evolved to EPC (Evolved Packet Core). In LTE, the role of base stations includes some functions of 3G RNC, and most components consist of IP-based networks. Also, unlike 3G, the control protocol and the data protocol were partially changed, and particularly the control message and the data transmission message have different communication paths as shown in [Fig. 2]. The S-GW (Serving Gateway) and P-GW (PDN Gateway) of LTE can be mapped to the SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node) of 3G. One of the differences is that the control protocol uses GTP-C v2. In other words, the management function of the fundamental GTP tunnel of 3G is not very different from that of LTE. The only difference is the version of GTP-C. Accordingly, this paper describes the data network based on 3G.

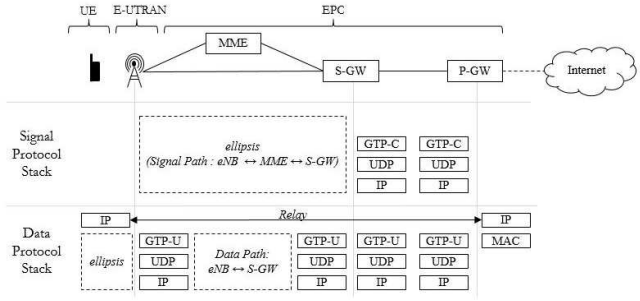

Fig. 2: LTE mobile network structure

2.2 GPRS Tunneling Protocol

In 3G and LTE networks, GTP[3] is used for data communication. As a tunneling protocol, GTP generates the logical tunnel identified by TEID (Tunnel Endpoint Identifier) for the traffic taking place at the UE (outbound and downlink) and the traffic sent from outside to the UE (inbound and downlink) before data communication. This GTP tunnel is generated and managed by GTP-C. Fig. 3 illustrates the generation and packet structure of the GTP tunnel. If the GTP tunnel is generated, the IP packet generated at the UE will be loaded on GTP-U and sent to GGSN. At this time, the outbound TEID allocated to the UE will be recorded in the GTP-U header before transmission. Likewise, the traffic received by the UE is transmitted by GTP-U. The inbound TEID assigned to the UE will be recorded in the GTP-U header before transmission. If data send and receive does not take place for a certain amount of time, GTP-C can be used to release the logical GTP tunnel.

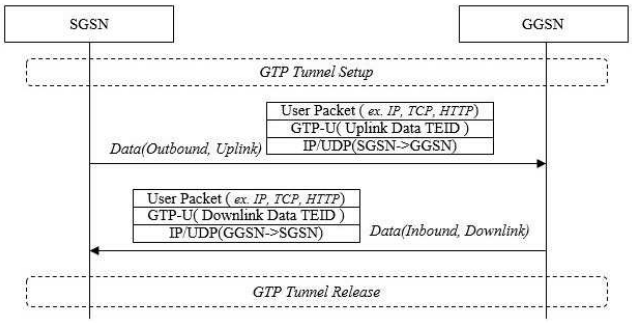

Fig. 3: GTP tunneling setup flow

2.3 Related works

The security threats of mobile networks have been partially studied. Ref. [6] defined the security threats that can occur in a structure where the 3G mobile network and the Internet are interworking, and [7] analyzed DoS (Denial of Service) attacks based on occupation of wireless resources by abusing the timing of wireless resource allocation and release on mobile networks. Also, [8] experimentally analyzed how much load the overload of the paging signal, which is one of the control messages occurring on mobile networks, can give to mobile networks, and [9] used the MMS transmission vulnerability abusing the paging channel to propose battery resources attacks of the UE. Ref. [10] analyzed attacks that can abuse SMS on the Internet to generate DoS on mobile networks.

Mobile networks like 3G and LTE have been monitored and security research projects are underway mostly in Europe, such as Germany and Austria. The DARWIN project[11] was led by Austria, defined unwanted traffic of 3G mobile networks, and conducted researches that can monitor and detect abnormal traffic likely to affect 3G mobile networks[12]. This study was conducted to monitor and analyze failures of mobile networks in various unexpected situations where mobile services are used. ASMONIA[13] was led by Germany which started in 2010. It monitors abnormal traffic of 4G mobile networks and conducts security researches. This study analyzed the security threats of each element of the 4G environment, that is, of each interface between the UE and mobile network components, and the possibility of attacks and repercussions.

3 Mobile Network Attacks Using IP Spoofing

IP Spoofing means that the sender alters an IP address other than assigned to the sender as the source IP. IP Spoofing makes it difficult to trace the IP of the attacker, and has been used by various attacking techniques like DoS attacks in the wired environment. But IP Spoofing can be filtered in a limited way by the Network Ingress Filtering of the switch or router in the wired environment.

As IP Spoofing is not taken seriously in the mobile environment, the resulting security threats were not taken into consideration in a big way, but IP Spoofing in the mobile environment can lead to overbilling and power consumption for certain UE, occupy the wireless resources of the mobile network, and induce abnormal traffic into components in the mobile network such as GGSN, P-GW.

Mobile networks may be configured differently depending on service providers, but mostly, as shown in Fig. 4 (a), they have NAT (Network address translation) which provides communication between UEs and external services. Unless the internal network requests communication, NAT cannot allow attempt to communicate with an object on the network from outside. This has something to do with the distinct characteristics of the mobile network. As the communication packet in the mobile network is to be billed, unnecessary traffic must be minimized, and only required communication for service must be available. And the mobile network must go through a complex signaling process to send data to the UE. In particular, as the wireless resources between the base stations and the UEs are limited for each base station, they are allocated to the UE only when necessary, and then released. Likewise, the UE with limited electric power is not active all the time. Instead, it is deactivated after a certain amount of time to reduce the power consumption of the UE, and wireless resources are released. If IP Spoofing is used, however, NAT will be incapacitated, and abnormal traffic may be brought to the

IP that did not attempt communication inside the mobile network, as shown in Fig. 4 (b).

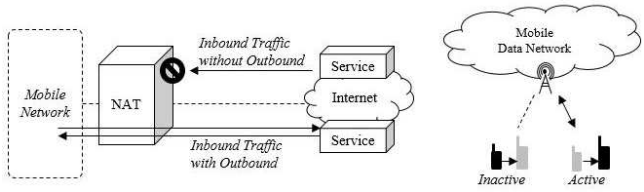

Fig. 4: (a) NAT structure, (b) status change of UE

3.1 IP spoofing in Mobile data network

In the mobile network, the IP packet generated at the UE is relayed to GGSN or P-GW. It means that the IP packet of the UE passes the packet data network unconditionally in any case, and through additional security devices like NAT. At this time, NAT maps the source IP/port of the outbound packet and the external destination IP/port, and enables communication with the IP of NAT by creating the NAT table.

Based on the above structure, the conceptual procedure of IP Spoofing in the mobile network is illustrated in Fig. 5. Before IP Spoofing is described, it will be assumed that there are UE A and B, and both UEs are capable of data communication. And 192.168.1.1 was assigned to UE A, and 192.168.2.2 was assigned to UE B. And it will be assumed that the external service server provides echo service at 9.9.9.9/456, as shown in Fig. 5.

Step 1. First of all, UE A alters the source IP to 192.168.2.2, not its own IP 192.168.1.1, and sends it to the external service server (9.9.9.9/456). The spoofed packets sent by UE A pass through a data network like CN and are transmitted to NAT.

Step 2. NAT maps the source IP of the IP packet 192.168.2.2 and the external IP 9.9.9.9 to create the NAT table, and modifies the source IP (port) with the IP of NAT, and transmits the packet to the external service server.

Step 3. The external service server sends response packets to the source IP of the received IP packet, and through NAT to CN. CN and EPC search for the UE corresponding to 192.168.2.2 which is the destination IP address, verify that it is UE B, establish the GTP tunnel of UE B, and send response packets.

Step 4. UE B receives unwanted response packets.

3.2 Attack using IP spoofing

The core of IP Spoofing is that unwanted abnormal traffic, not the requested communication traffic, can be brought to unspecified individuals in the mobile network. IP Spoofing can be used to send an unwanted bill to users with a certain IP, and sends abnormal signals in the mobile network concurrently to cause overload in the network or consume the resources of the UE and mobile network. Also, it may cause overload in important components in the mobile network.

Overbilling for users In general, charging for data usage in the mobile network is done on the basis of IP. For example, a component like GGSN which can handle user packets, outputs information on traffic use based on IP and the charging system gets such information together, and calculates data usage. Of course, some traffic caused by well-known worms and certain DNS service may be excluded from the billing according to the policy of the service provider. If the type of the traffic like the number of send & receive packets, can be viewed as normal communication, however, charging may be done for the IP.

As shown in Fig. 6, attackers will execute abnormal service in a certain external server. If packets are inputted, this service sends a large volume of traffic to the packet source. Attacker A sends the packets, spoofed to a certain IP (B‘s IP), to a pre-specified external server. The external server sends a large volume of traffic to the source IP (B‘s IP) of the received packets, and user B receives a large volume of unintended traffic. In this process, for example, attacker A sent less than 2bytes of packets for the attack command, but user B can receive a large volume of packets bigger than 1Kbyte as specified in the external server as long as MTU allows it. In this case, attacker A is billed for 2bytes on the surface, and user B is billed for the received packets. Billing details may vary depending on the billing policy of the mobile communication service provider, but what is important is that overbillings can be made due to IP Spoofing.

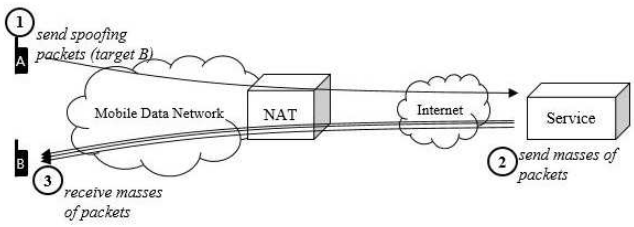

Fig. 6: Overbilling attack

Consumption of resources Wireless resources in the mobile network are limited resources, and the complicated control process is essential for establishing

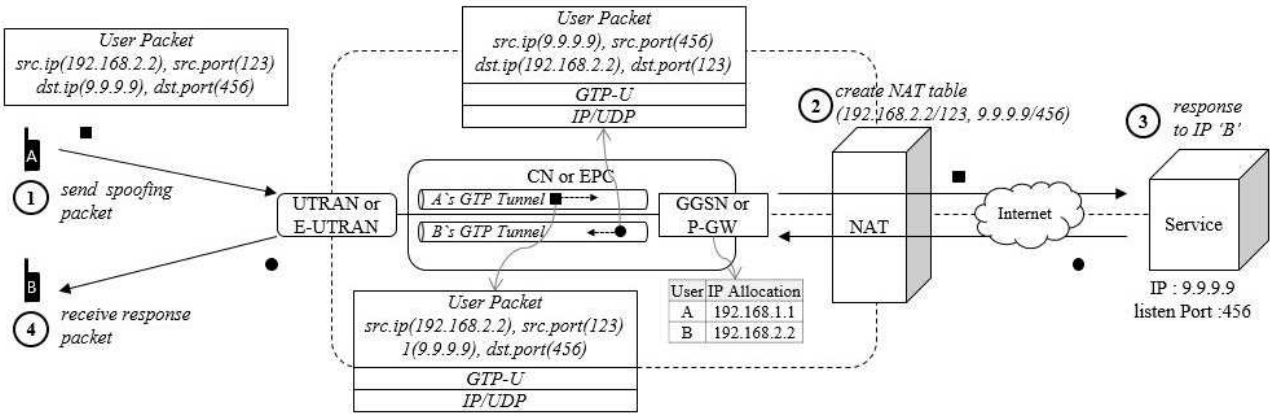

Fig. 5: IP spoofing in mobile data network

and managing such resources. For example, the UE has the Active mode and the Inactive mode. The UE requests and sets up wireless resources in the Active mode only when necessary, and then goes into the Inactive mode to save unnecessary resources, and hands over wireless resources so that other UEs can use them. Also, when the base station receives communication requests from outside, as the UE is already using wireless resources if it is in the Active mode, it will simply transmit data, but if the UE is in the Inactive mode, the paging signal for looking for a UE will be sent to the base station wirelessly, and the wireless resources for data communication with the responding UE will be set up. If the UE's Active/Inactive switching time is t, and communication traffic arrives every $t+\alpha$, the signal and wireless resource setup/release procedure for repeated wireless resources setup and the switching of the UE's Active/Inactive mode may be repeated. Or if communication traffic comes every $t-\alpha$, resources may be occupied continuously, and other UEs use of wireless resources may be hindered. If these attacks are not happening to one UE, but to UEs in a certain area, or on a large scale, it may be a great burden on the mobile network.

The attacker implements a simple echo service for periodically sending packets to an external server, and as illustrated in Fig. 7, spoofs packets to multiple IPs, creating traffic small in size, but aimed at multiple targets. Then, response packets for multiple IPs are generated externally, and sent to respective UEs. If the UE is Active, it will continue to occupy wireless resources, whereas if it is Inactive, it will switch to Active and masses of signals for setting up wireless will be generated concurrently, causing DoS attacks in the network.

Overload for mobile network These expensive components such as SGSN, GGSN, S-GW and P-GW, process the large volume of traffic in the mobile network. So Availability is important, but the mobile network has been regarded until now as a safe network regarding

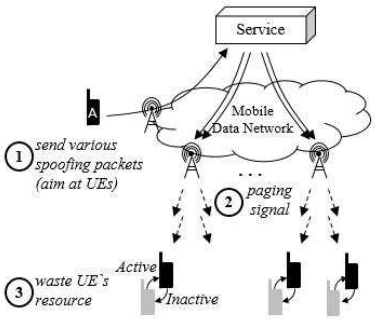

Fig. 7: Resource consumption attack

which there is no concern over abnormal traffic sent to the machines from outside or inside. The attacker implements an attack service that sends abnormal traffic to an external server, and as shown in Fig. 8, the UE sends the spoofed packets to the IP of the internal machine. The external attack server can send a large volume of attack traffic to the internal network machines, and the internal machines receiving the attack traffic may find it burdensome to process the traffic. For example, if the attacker acquires the IP of the internal GTP-related machine through GTP Scan, and the attack server abnormally alters the GTP protocol, an important processing protocol, and sends it as attack traffic, each key machine can receive DoS attacks due to unnecessary processes like exception handling of abnormal GTP packets and errors.

4 Attack in Real Field

To verify a security threat by IP spoofing in the commercial mobile network, we conducted the test with an Android-based smart phone that is relatively free to manage and control. For test, the attacker and the victim

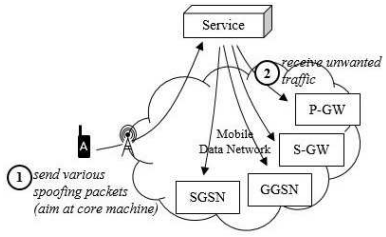

Fig. 8: Overload attack for mobile network

used the same UE, i.e. *Samsung Galaxy Nexus*, subscribing to a flat rate monthly pricing on a commercial 3G service network. The attacker‘s UE was rooted to transmit IP Spoofing packets, and the Linux shell was loaded so that the IP Spoofing program could work. Wi-fi was deactivated in each UE, and the UEs were connected to the 3G network. Apps like *Myip* were used to check the IP of the UE, and both the attacker and the victim used *tcpdump* to collect packets from inside the UE. The packets spoofed to the IP of the victim‘s UE from the attack UE were sent to the external echo server. We checked the network traffic collected from each UE, and found that, as shown in Fig. 9, the spoofed packets sent by the attacker were sent to the external server, and the packets sent by the external server were received by the victim‘s UE. The receiving UE generated ICMP for the received packets. (The IP of the UE is a public IP band on the surface, but it is used only inside the mobile network, and is changed through NAT for Internet communication)

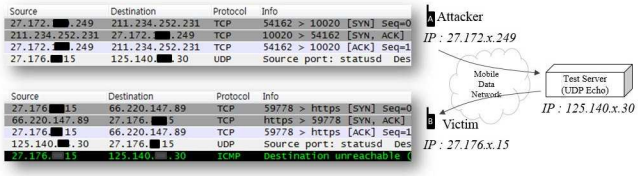

Fig. 9: IP spoofing result in real field

4.1 Overbilling attack

In the experiments for checking the occurrence of overbillings due to IP Spoofing, the active applications in the UE were suspended as much as possible in advance, and the current data usage was checked. Then, we used apps like *Myip* to check the IP of the victim‘s UE, and sent the UDP packets, spoofed from the attacker‘s UE to the IP of the victim‘s UE, to the external attack server. After the attack is completed, we checked the charging status of each UE, and obtained the results as shown in TABLE I. The results show that the attacker can cause overbillings to a user with a specific IP.

Table 1: Result of Overbilling Attack

Option	Scenario 1	Scenario 2
Size of attack packet	2byte	2byte
Number of attack packet	10,000	110,000
Traffic from Attacker	0.02MByte	0.2MByte
Traffic from Attack Server	9.9Mbyte	109.3Mbyte
Receive traffic at Victim	9.8MByte	106.7MByte
Receive traffic at Attacker	0byte	0byte
Billing for Victim (Data Usage)	9.8MByte	106.7MByte
Billing for Attacker (Data Usage)	0byte	0byte

4.2 Battery depletion attack

Regardless of whether there was any charge made to the UE, IP Spoofing can continuously deplete the battery of the UE. We created an environment similar to that causing overbilling. And the attacker sent the attack message when the battery of the victim‘s UE was fully charged, and we made sure that the external attack server sent an unlimited volume of traffic. As a result, as illustrated in [Figure 9], more than 80% of the battery was depleted in just 5 hours. The battery was discharged about 12 times faster than the normal discharging speed, as shown in Fig. 10. The victim‘s phone was Google‘s reference phone(*Galaxy Nexus*) manufactured by Samsung at the end of 2011. According to the official specs, the smart phone had 210 hours of waiting time, and 18 hours of continuous talking time.

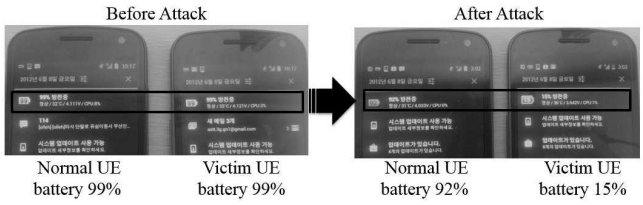

Fig. 10: Result of battery depletion attack

5 Approach for IP Spoofing Prevention in Mobile Network

In the mobile network, it is advantageous to detect user packets before getting out of the GTP tunnel in order to

detect IP Spoofing. IP Spoofing is hard to detect using method like Network Ingress Filtering because the more traffic goes outside the traffic is becoming increasingly intensive. And also the L2 layer carrying user IP packets are newly created in GGSN or P-GW. Accordingly, to detect IP Spoofing in the mobile network, we must check if the source IP of the user packets transmitted by the Outbound GTP-U packet in the GTP tunnel section is valid. The process of generating the GTP tunnel using GTP-C v1 as an example is roughly illustrated in Fig. 11.

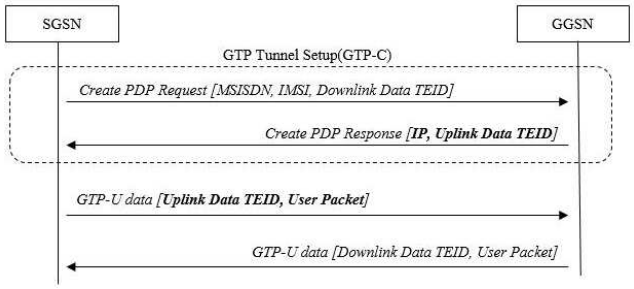

Fig. 11: Information exchange during GTP tunnel setup

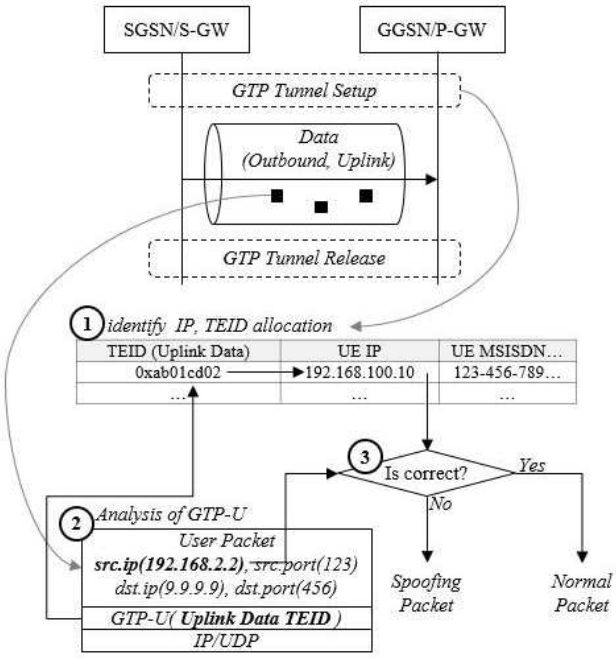

Fig. 12: Scheme for IP spoofing detection

To create the GTP tunnel, SGSN use the UE information (MSISDN, IMSI, etc.) regarding which UE the tunnel is for, and assign the IP the UE will use in response. TEID exists separately for each UE depending on directionality and packet type (GTP-C/GTP-U). When creation of a tunnel is requested, TEID (Downlink Data TEID) for sending data to the UE will be sent as well, and the response will include TEID (Uplink Data TEID) used for the data the UE sends outside. Accordingly, while the GTP tunnel is generated, depending on the direction in which the UE sends data, TEID to be used and the IP to be used by the UE will be determined. Accordingly, we can use the GTP tunnel information to detect IP Spoofing as shown in the Fig. 12. As the GTP tunnel information necessary for IP Spoofing is information that can be checked regardless of the GTP-C version, it can be applied not only to 3G, but also GTP-C v2 used in LTE.

6 Conclusion

As the mobile network is now open to the Internet, it is faced with various security threats that could not be expected previously. Also, the spread of high-performance smart phones are perfect tools for attackers. The Linux-based Android system can control the diverse functions of the smart phone through rooting, and this paper presented various security threats caused by IP Spoofing, and the results of actual tests.

In particular, as the threats of abnormal charging and UE battery depletion can bring monetary damages to users of commercial service networks and lower the usability of UEs, they may hinder the progress of the mobile Internet. This paper presented a method of utilizing the GTP tunnel information, used in the mobile network to detect IP spoofing. To this end, we can take advantages of existing GTP tunnel information, or collect/analyze GTP-C and apply it to security machines for detecting IP Spoofing. To detect and prevent IP Spoofing, we are planning to develop IPS in the GTP section capable of detecting and preventing IP spoofing, apply it to actual networks, and check its function and performance. The equipment we will develop can analyze GTP-C to extract GTP tunnel information, which will in turn be used for detecting and blocking IP Spoofing.

As the backbone network of the country, the mobile network is an important communication infrastructure. Accordingly, we must be able to detect security threats, which can be abused for cyber terrorism against the mobile network as early as possible, and continuously conduct researches for countermeasures.

Acknowledgement

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

References

[1] CISCO, Global Mobile Data Traffic Forecast 2011-2016, Cisco Visual Networking Index, (2012).

[2] F. Ricciato, P. Svoboda, E. Hasenleithner, W. Fleischer, On the impact of unwanted traffic onto a 3G network, Proceedings of the Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 49-56 (2006).

[3] 3GPP, GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 10), TS 29.060 V10.2.0, (2011).

[4] H. Holma, A. Toskala, WCDMA for UMTS - Radio Access for Third Generation Mobile Communications, Willey, (2004).

[5] 3GPP, General Packet Radio Service (GPRS); Service description; Stage 2, TS 23.060 V10.3.0, (2011).

[6] K. Kotapati, P. Liu, Y. Sun, T. F. LaPorta, A taxonomy of cyber attacks on 3G networks, Proceedings of the IEEE international conference on Intelligence and Security Informatics, 631-633 (2005).

[7] F. Reicciato, A.Coluccia, A. D'Alconzo, A review of DoS attack models for 3G cellular networks from a system-design perspective, Journal of Computer Communication, **33**, 551-558 (2010).

[8] J. Serror, H. Zang, J. C. Bolot, Impact of paging channel overloads or attacks on a cellular network, Proceedings of WiSe '06 Proceedings of the 5th ACM workshop on Wireless security, 75-84 (2006).

[9] R. Racic, D. Ma, H. Chen, Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery, Proceedings of the Securecomm and Workshops, 222-231 (2006).

[10] W. Enck, P. Traynor, P. McDaniel, T. La Porta, Exploiting open functionality in SMS-capable cellular networks, Proceedings of the 12th ACM conference on Computer and communications security, 393-404 (2005).

[11] DARWIN Project, http://www.ftw.at/ftw/research/projects/

[12] F. Ricciato, Traffic monitoring and analysis for the optimization of a 3G network, Journal of Wireless Communication, **13**, 42-49 (2006).

[13] ASMONIA Project, http://www.asmonia.de/

Dong W. Kang was born in August 1, 1982, Republic of Korea. In 2007, he has received bachelor's degree in computer engineering and finally, in 2009, he received master's degree in information security from Soonchunhyung University in Asan, Korea. He joined Korea Internet and Security Agency in January 2009, and researches about Botnet, 3G mobile security include GTP and SS7 on 3G Network. In 2011, he became Senior Research Associate and researches for 4G/LTE network security include EPC, Femtocell networks.

Joo H. Oh was born in 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 analysis, 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 T. Im was born in 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 in 2011. 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 research 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.

Wan S. Yi was born in December 10, 1967 at DaeGu, Republic of Korea. In 1991, he has received bachelors degree in computer science from Virginia Polytechnic Institute and State University, Blacksburg, Virginia, USA. In 2001, he received masters degree in information security from Dongguk University in Seoul, Korea. Finally, in 2011, he received Doctorate degree in Computer Engineering from SungKyunKwan University in Seoul, Korea. His main interest area is information security product evaluation against Common Criteria ISO 15408, Critical Information Infrastructure Protection and Internet Incident Response. Dr. Yi served in Korean Air Force as an Interpreter for Commander in Chief, ROK/US Combined Forces Command. He retired from service in 1994 as a first lieutenant. Then he worked for Hyundai Information Technology Corp from 1994 to 1996. And finally, he joined Korea Internet and Security Agency in August 1996. In 2012, he became Vice President and is responsible for Internet Incident Prevention division.

Yoo J. Won joined the Korea Internet&Security Agency (KISA) in September 2004 and has spent most of his time working for research of information security technology. Before Joining KISA, he was at AhnLab as a CTO from 2001 to 2004. From 1987 to 2001, he was a Director at the Electronics and Telecommunications Research Institute (ETRI). He received a Ph.D degree in computer science from Chungnam National University and B.S, M.S degree in Statistical Computing at the same University. Following his successful research of information security technology in 2007, Yoojae Won led the IT Infrastructure Protection Division and became resolved in various security issues such as VoIP, IT Business, U-IT Service. In 2011 he was assigned to Executive Vice President of Korea Internet Security Center.