Pay As You Want: Bypassing Charging System in Operational Cellular Networks

Hyunwook Hong(✉), Hongil Kim, Byeongdo Hong, Dongkwan Kim,
Hyunwoo Choi, Eunkyu Lee, and Yongdae Kim

Korea Advanced Institute of Science and Technology (KAIST)
291 Daehak-ro, Daejeon, Republic of Korea
{hyunwook.h, nagoyam159, byeongdo, dkay,
zemisolsol, ekleez, yongdaek}@kaist.ac.kr

Abstract. Accurate and fair data charging in cellular networks is an important issue because of its large impacts on profits of operators and bills for users. In this study, we analyze the data charging policies and mechanisms for protocols and applications. The analysis shows that all operators in South Korea did not charge the payload of Internet Control Message Protocol (ICMP) echo request/reply messages, as well as the payload attached to Transmission Control Protocol (TCP) SYN and TCP RST packets. In addition, the operators only utilize IP addresses to verify whether the traffic comes from the expected application. By misusing the findings with consideration of Network Address Translator (NAT) in IPv4 cellular networks, we validate with empirical experiments the feasibility of free-riding attack, which enables an adversary to use the cellular data service for free, and propose effective countermeasures.

Keywords: Cellular Networks, Mobile Data Services, Data Charging

1 Introduction

As 3G/LTE cellular networks are deployed, the popularity of mobile devices such as smartphones and tablets, increased, enabling a large number of users to enjoy cellular data services. According to a report [14], 64% of adults in the U.S. own a smartphone, and 19% of them rely on a smartphone to access the Internet. However, these cellular data services are not given to users for free. Most operators charge the cellular data based on data usage volume of the user with their policies. Considering the large impacts on profits of operators and bills for users, an accurate and fair data charging has become an important issue for both cellular operators and users. As discovered in previous works [8, 11], some operators did not charge the traffic for control purposes in operations of networked systems, such as the Domain Name System (DNS) [11] and Transmission Control Protocol (TCP) retransmission traffic [8]. Furthermore, operators also do not charge the data traffic from a designated mobile application, such as a customer service application. These charging policies open the feasibility of the free-riding attack, which enables an adversary to use the cellular data service for free. For this reason, we investigated the charging policies for protocols and applications that have not been examined previously.

First, we analyzed the charging policies for two different protocols, namely, Internet Control Message Protocol (ICMP) and Transmission Control Protocol (TCP) in six major operators, three of which are from the U.S. and the other three are from South Korea. We found that all operators in South Korea did not charge ICMP echo request/reply messages, as well as the payload attached to TCP-SYN and TCP- RST packets. On the other hand, only one operator in the U.S. did not charge the payload attached to those TCP packets.

Second, we focused on the charging policies for applications in three major operators of South Korea. The subscribers of optional services can enjoy music and video contents by using the provided mobile applications with additional data volumes. In addition, operators generally provide mobile applications for customer services to request an inquiry of subscriber information; and the data usage from these applications are not charged. To identify the vulnerability of these charging policies, we first analyzed the charging mechanisms for these applications, and found the way for misusing them. We disclosed that operators utilized only IP addresses to verify whether the traffic comes from the expected application. Moreover, we assume an adversary in IPv4 networks (for both the cellular network and the Internet); therefore, we considered Network Address Translator (NAT) in cellular networks. Since NAT drops incoming packets that do not exist on the recorded NAT mapping table, we not only developed two methods so that the downlink traffic can pass through NAT: creation of a real and a fake connection to make a 5-tuple entry on NAT mapping table, but also found the way for identifying the 5-tuple entry. Using these methods, we conducted empirical experiments and obtained result showing that the normally generated data traffic, which masquerades as the data traffic generated from the designated application, was not charged. This finding could validate the feasibility of the free-riding attack.

We propose countermeasures for the free-riding attack. Operators can limit the size of payload or the amount of traffic in the fixed time period for the ICMP traffic, and block uncommon traffic, such as TCP-SYN or TCP-RST packets containing the payload. The free-riding attack that misuses charging policies for the application requires more efforts than other attacks because it is difficult to differentiate between the normal traffic and the misused traffic. The attack can be mitigated by locating the application server inside cellular networks. Furthermore, operators can utilize the anomaly detection and prevention. However, operators should be reminded that the application of these countermeasures can cause unexpected problems such as false positives; therefore, sufficient consideration on their implications should be given.

We summarize our contributions as follows:

- We analyze the charging policies and mechanisms for two different protocols and five applications, and found that these charging policies and mechanisms can be misused.

- We develop and demonstrate free-riding attacks using the analyzed charging policies and mechanisms. In addition, we responsibly disclosed all these vulnerabilities to the operators.
- We propose effective countermeasures that can mitigate the attacks targeting charging policies and mechanisms for protocols and applications.

The rest of the paper is organized as follows. We provide related works in Section 2. In Section 3, we describe the architecture of cellular network with charging system and the methodology of our experiment. Then, we analyze the charging policies for two protocols in Section 4 and examine policies for applications in Section 5. Finally, we discuss and propose countermeasures in Section 6, and conclude our work in Section 7.

2 Related Works

Several studies reported that the data charging systems in cellular networks can suffer from two types of attack: over-billing and free riding attacks [8–12]. Peng *et al.* [11] demonstrated these two attacks in 3G cellular networks. They showed that an adversary could use free data by exploiting the loopholes where data communication using DNS port number is not charged. Furthermore, closing a connection based on the timeout could expose a client to an over-billing attack. Peng *et al.* [12] also reported vulnerabilities of the charging system. They showed that the source IP spoofed data are not charged and an adversary could impose overcharged bills to a victim. Moreover, the adversary can hide inflated data usage volume by adjusting the Time To Live (TTL) value in the IP header. Go *et al.* [8] misused the TCP retransmission for an attack vector. Since a charging system only inspects the IP layer in the middle of the network, it cannot identify the accurate state of TCP context; thus, it is difficult to identify whether the retransmission is malicious or not. Their analysis on the charging policy for TCP retransmission shows that some countries charged the retransmission data while others did not. By exploiting this policy, they showed that over-billing and free-riding attacks were feasible. On the other hand, several studies demonstrate the possibility of over-billing and free-riding attacks by exploiting a voice over LTE (VoLTE) interface newly adopted to LTE networks [9, 10]. Li *et al.* [10] disclosed that an adversary could send a large amount of packets from a VoLTE interface to a data interface of a victim. This attack misused the accounting policy that the VoLTE interface is free while the data interface is charged. Kim *et al.* [9] demonstrated that four free data channels were available: direct communication of phone-to-phone and phone-to-Internet and SIP/media tunneling. They also showed that an over-billing attack is possible by spoofing the phone number of the caller.

In this study, we examine the data charging policies for the ICMP and TCP traffic, which is used for control purposes in network operations, and analyze the charging policies and mechanisms for applications used by optional services and customer services. Furthermore, we demonstrate the free-riding attack by misusing the findings from the analysis.

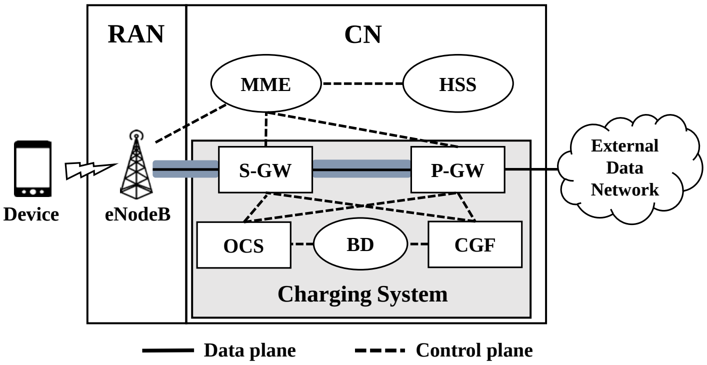


Fig. 1. Charging Architecture in LTE Network.

3 Background

3.1 Architecture of cellular charging system

Fig. 1 shows that the cellular network consists of the Radio Access Network (RAN) [1] and the Core Network (CN) [3]. RAN acts as an intermediary to provide connection between a cellular device and the CN. It transmits data between the cellular device and the CN, and controls information for radio resources. The CN is a major part of the cellular network that provides call control and charging among others. The Serving Gateway (S-GW) and the Packet data network Gateway (P-GW) are the key elements in the CN. The S-GW routes and forwards data packets from and to the base station and the P-GW. The P-GW supports connectivity between a cellular device and external data network, such as the Internet [5].

For the charging system, several components, such as the Billing Domain (BD), the Charging Gateway Function (CGF), and the Online Charging System (OCS), are used [2]. There are two charging modes: offline and online [4]. When a cellular device uses the data service, charging procedures are triggered. In offline charging mode, the S-GW/P-GW initially makes Charging Data Records (CDRs) and records data volume. Charging information comprises as follows: source/destination IP address and port number and protocol ID, such as TCP and UDP. The CGF validates CDRs, and filter the data according to the policy of the operator. Then, the CGF sends CDRs to the BD. The BD generates billing information from the charging ID in the CDRs at the end of the process. In online charging, a user has to pre-pay to acquire their credits for data service. The OCS checks whether a user has sufficient credits or not, and the S-GW/P-GW deducts credits based on his/her data usage. Data service is stopped when the user's credit is depleted.

3.2 Methodology

In this study, we examine the charging policies at each layer of the cellular network, such as network, transport, and application layer. For network and transport layers, we investigate the ICMP and TCP traffic in six major operators, where three are from the U.S. and the other three are from South Korea. We also analyze the charging policies for applications in three major operators of South Korea. For non-disclosure reason, we anonymized the name of operators by labeling them as US-I, US-II, and US-III for the U.S. and KR-I, KR-II, and KR-III for South Korea operators. Since all operators offer interfaces for the charged data usage, we can check the charged data usage by using web pages or mobile applications provided by the operators. However, because these interfaces do not reflect the data usage in real time, after the sufficient time has passed (at least 1 hour later), we check the last applied time for the charged data usage and verify it.

Moreover, all experiments are conducted on IPv4 cellular networks with devices connected to the LTE network. In IPv4 networks, NAT [15] is used to resolve the lack of public IPv4 address resources; thus, our experiments are carried out by considering NAT. Since NAT drops incoming packets that do not exist on the recorded NAT mapping table, we developed two methods for creating the mapping so that the traffic can pass through NAT. (see Section 5). On the other hand, in IPv6 networks, all proposed attacks could be launched more easily than in IPv4 networks because NAT is not used in IPv6 networks. Note that our experiments do not affect any other users in cellular networks, and we only conduct the experiments for research purposes and responsibly disclose our finding to operators.

In this study, we discover the methods to avoid the charging mechanisms; thereby, users can use the cellular data service for free. In addition, we develop free-riding attacks by misusing the analyzed charging policies and mechanisms. To implement the attack, we utilize similar methods used in previous work [8]. Fig. 2 depicts the process of the free-riding attack which requires a collaborating tunneling proxy to relay the tunneled packets and real traffic. Specifically, for uplink traffic (from cellular device to server), packets are tunneled to the proxy and de-tunneled by the proxy and relayed to the destination server. For downlink traffic (from the server to the cellular device), the packets are sent to the proxy which tunnels them to the cellular device, and the device de-tunnels and passes them to the application. In this scenario, the charging system in the cellular core network can only observe the traffic between the cellular device and the proxy, which will not be charged.

4 Charging Policies for Control Traffic of Protocols

In this section, we investigate the charging policies for two different control packets: (1) an ICMP packet, and (2) a TCP control packet for operators in the U.S. and South Korea. Then, we demonstrate the feasibility of the free-riding attack by misusing these charging policies.

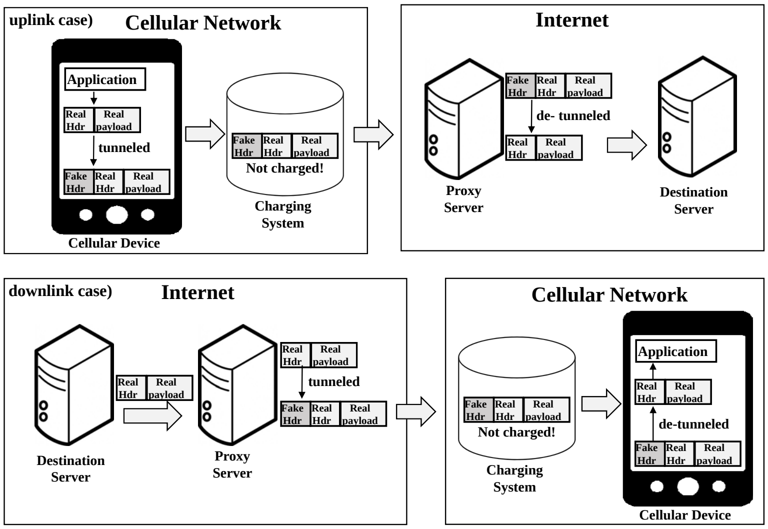
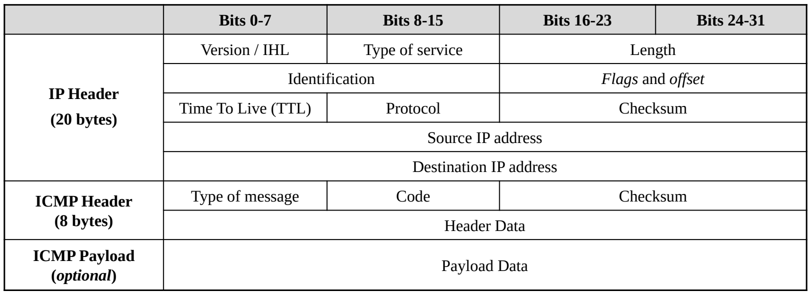


Fig. 2. Free-riding attack process.



	Bits 0-7	Bits 8-15	Bits 16-23	Bits 24-31
IP Header **(20 bytes)**	Version / IHL	Type of service	Length	
	Identification		*Flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Header **(8 bytes)**	Type of message	Code	Checksum	
	Header Data			
ICMP Payload **(*optional*)**	Payload Data			

Fig. 3. Composition of an ICMP packet.

4.1 Charging policies for ICMP traffic

ICMP messages are used for diagnostic or control purposes in response to errors in IP operations of networked systems [6, 13]. Operators usually have different charging policies for this traffic. Fig. 3 shows that an ICMP packet comprises an IP header, an ICMP header, and an ICMP payload. ICMP messages are classified by the Type and Code fields in the ICMP header. Among several types of ICMP messages, we focused on an ICMP echo request (Type=8, Code=0) message. The ICMP echo message is used for identifying reachability of target hosts by sending an echo request to the target hosts and receiving the response if they reply. In addition, this ICMP echo message could contain any payload that does not exceed maximum transmission unit (MTU) or risk being fragmented. Considering this in our experiment, we sent 30 × 1,024 IMCP echo request messages containing 1,024 bytes payload (30 MB traffic) from our mobile device to our server on the

Internet. Similarly, our server responded to these messages with ICMP echo reply messages containing 1,024 bytes payload. We repeated this experiment for each operator, and checked whether each operator charged for this traffic. According to the RFC standard [13], the payload in the ICMP echo reply should be the same as the payload in the IMCP echo request. However, in our experiment, we used different payload for each request and reply since our purpose is to check whether the ICMP echo request/reply could be utilized for the free data channel. The result of this experiment is presented in the Table 1.

Table 1. The amount of charged traffic of ICMP echo request and reply in Korea and the U.S. operators.

	KR-I	**KR-II**	**KR-III**	**US-I**	**US-II**	**US-III**
ICMP echo request	0 MB	0 MB	0 MB	30 MB	30 MB	30 MB
ICMP echo reply	0 MB	0 MB	0 MB	30 MB	30 MB	30 MB

Table 1 shows that all operators in South Korea did not charge the ICMP echo messages, whereas all U.S. operators charged these messages. Thus, for the operators in South Korea, an adversary could perform the free-riding attack by utilizing tunneling technique of the ICMP echo message traffic. Consequently, we conducted this attack, and verified that any data traffic through the ICMP tunnel was not charged. This finding validates the feasibility of the free-riding attack.

4.2 Charging policy for TCP control traffic

TCP utilizes various control packets to provide stateful connection by using flags, such as SYN for the synchronization of the sequence number, ACK for the reliability of the data transmission, and FIN and RST for the appropriate termination of the connection. These control packets could be generated by the network condition regardless of the intention of the user and it is unclear whether operators should charge for this traffic. For this reason, we examined the charging policy for TCP traffic for control purposes. We utilized SYN and RST packets for this experiment. As similar with the ICMP case, we sent 30 × 1,024 SYN packets containing 1,024 bytes payload (30 MB) from our cellular device to our server on the Internet. Likewise, on our server, we sent same amount of RST packets to our mobile device on receiving SYN packets. The result of this test is presented in the Table 2.

Table 2 shows that all operators in South Korea did not charge for both SYN and RST packets containing the payload, whereas two of the U.S. operators charged for those traffic. From this experiment, an adversary can also misuse the SYN and RST packets for free data channel. Consequently, we conducted the free-riding attack by utilizing the tunneling technique, and verified that any of the data traffic passed the TCP-SYN/RST tunnel was not charged. The

Table 2. The amount of charged traffic of TCP control packets in Korea and the U.S. operators.

	KR-I	**KR-II**	**KR-III**	**US-I**	**US-II**	**US-III**
SYN with payload	0 MB	0 MB	0 MB	30 MB	30 MB	0 MB
RST with payload	0 MB	0 MB	0 MB	30 MB	30 MB	0 MB

finding validates the feasibility of the free-riding attack. Note, IPv4-based cellular networks utilize NAT; therefore, all traffic should be initiated within the cellular network. The details of this issue are introduced in the following section.

5 Charging Policies for Applications

5.1 Mobile applications for optional services and customer services

Operators recently provide various optional services as well as charging plans to meet the diverse needs of their customers for data service. Some optional services offer a new type of charging plan for specific mobile applications that provide music and video streaming. Once mobile users subscribe these services, operators apply a different charging policy for these services regardless of the current data usage plan. For example, operators give sufficient (e.g. 2 GB for a day) or even unlimited data as long as the subscriber uses a designated application for content streaming. Another interesting fact is that operators in South Korea do not charge for the data used for inquiry of subscriber information. In other words, mobile users can check their current data usage, change, or join a new usage plan without being charged using a given mobile application for the customer service from their operators. In this context, from security perspective, one may concern whether an adversary could masquerade a normal data traffic as the traffic generated from given applications. To this end, we analyzed the charging mechanisms for these applications and demonstrated how an adversary deceives the charging policy.

5.2 Deceiving charging policy

As described in Section 3, S-GW/P-GW records the data volume with a CDR that comprises the information in the protocol header (source/destination IP addresses and port number, protocol). An adversary can easily obtain this information by inspecting the traffic generated from the application, thus the adversary is able to bypass data charging for her data usage with the modified header that masquerade as the traffic from the application. To this end, we first examined the traffic generated by the applications, identified the information for the CDR, and developed the method for the free-riding attack. We utilized the mobile applications for the customer service of three major operators in South Korea, and three optional services (two of which for video streaming, one for music streaming) of two operators in South Korea. Consequently, we obtained the

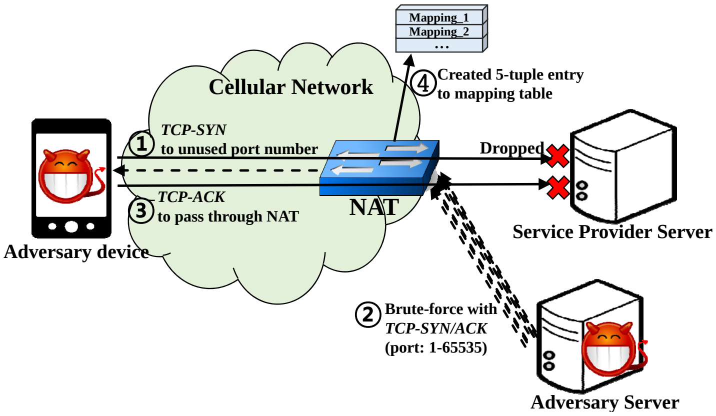

Mapping_1
Mapping_2
…
④ Created 5-tuple entry to mapping table
Cellular Network
① TCP-SYN to unused port number
Dropped
NAT
③ TCP-ACK to pass through NAT
Service Provider Server
Adversary device
② Brute-force with TCP-SYN/ACK (port: 1-65535)
Adversary Server

Fig. 4. Procedures of creating a fake connection.

server IP address and port number that the applications connect to, and found that all the applications utilized TCP connections for their communication. We describe the steps for deceiving the charging policy of the operators with several considerations.

Considerations. First, an adversary can launch the free-riding attack only for downlink traffic (from the server to the cellular device). In the case of the downlink, the server of the adversary on the Internet can send the data that masquerades as the data from the server that the applications connect to, and the adversary can receive this data at the cellular device of the adversary without being charged. On the other hand, in the case of the uplink (from the cellular device to the server), because the masqueraded data will not arrive at the server of the adversary, but arrived at the server of the service provider; thus, there is no way to receive the data departing from the cellular device of the adversary. For this reason, we focused on the downlink traffic and developed the free-riding attack for downlink. Next, since we assume that all the proposed attacks are launched in IPv4 networks (for both cellular network and the Internet), we considered NAT in cellular networks. When a device inside the cellular network initially connects to an external host, NAT translates the IP address and port number of the device to its own external values, and creates a 5-tuple[1] entry on its external mapping table. The traffic, which does not map on the table, will be blocked by NAT. Thus, to allow the downlink traffic to pass through NAT, we developed two methods for creating a 5-tuple entry on NAT.

Creating a 5-tuple entry on NAT. The first method is creating a real connection between the cellular device and the server, and using the 5-tuple for the connection. This method is quite simple because it requires only identifying the 5-tuple for the connection. However, the connection not used by a client after

[1] Protocol, server IP address and port number, External IP address, and port number of NAT.

the TCP three-way handshake can be closed by sending TCP-FIN or TCP-RST from the server of the service provider. In this context, a new connection has to be created whenever the server closes the connection, and this requires frequent identification of the 5-tuple. The other method is creating a fake connection between the cellular device and the server. This method is only valid when the server of the service provider does not respond to any packets from the device. Otherwise, every connection is reset by the server. Thus, creating a fake connection for the running services (port number) is impossible. For this method, the device first sends a TCP-SYN packet to the server of the service provider, and an adversary on the Internet respond to the packet with a TCP-SYN/ACK packet that masquerade as the response of the server. After receiving the TCP-SYN/ACK packet at the device, the device completes TCP three-way handshake by responding to the TCP-SYN/ACK packet with a TCP-ACK packet. The procedures of creating a fake connection are presented in Fig. 4. The 5-tuple entry created by the TCP-SYN packet is removed in a short time (according to the test, it took 10 seconds); therefore, an adversary also needs to identify the created 5-tuple entry within a short time. However, in this case, the adversary does not need to consider the case that the connection is closed by the server of the service provider.

Identifying the connection information. These two methods for creating the 5-tuple entry require identification of the 5-tuple to pass through NAT. Among these five tuples, we could identify the protocol, server IP address, and server port number by inspecting the traffic generated from the target application, but the external IP address and port number of NAT require other techniques. To this end, we analyzed the mapping pattern of NAT by repeatedly re-establishing connections and observing the variation of the external IP address and port number. As a result, we found that the external IPv4 address of NAT is not changed frequently when a new TCP connection is established from the same device (regardless of the server IP address and port number). Therefore, if an adversary creates a TCP connection between her device and the server, and observes the external IP address of NAT at the server, she can predict the external IP address of NAT for the next connection from the same device. On the other hand, the external port of NAT varied randomly whenever a new connection is established. However, because the port number is allocated within the range 1-65,535 (2 bytes), the adversary can brute-force the port number. In other words, she can send packets to all port numbers from 1 to 65,535. The size of a packet is 44 bytes; therefore, it would take around 0.2 seconds to send to all the ports with a 100 Mbps network (44 bytes × 8 bits/byte(s) × 65,535 / 100 Mbps = 0.22 seconds). While sending the packets, the payload containing the current port number is attached to each packet; thus, when the packet passed through NAT and arrived at the cellular device, it can offer the external port number of NAT in the payload.

Attack validation. With these methods, we conducted experiments to verify the feasibility of the free-riding attack. The experiments were performed similar to Section 4. While carrying out the experiments, we could utilize two methods:

creating a real or a fake connection for all the tested applications. As a result, we found that the downlink traffic using these connections was not charged. The traffic using the fake connection, which utilizes an actual unused port number at the server, was not charged. This implies that the operators only use the server IP address when they verify whether the traffic is generated from target applications or not. This finding validates the feasibility of the free-riding attack.

6 Countermeasures and Discussion

The suggested free-riding attacks misuse charging policies of operators; therefore, operators can easily block the attacks by modifying their charging policies. However, these policies are closely related with the needs of customers, profits of an operator, and recommendations from the government. Thus, operators cannot change their policies without sufficient consideration. For this reason, we can consider mitigation in the technical aspects rather than policy aspects.

For the ICMP traffic, operators can limit the size of the payload or the amount of the traffic in the fixed time period. Furthermore, for TCP control packets, the problem can be alleviated by blocking uncommon traffic, such as a TCP-SYN packet containing the payload. Although a TCP-SYN or a TCP-SYN/ACK packet can include payload [7], these packets are rarely used in networks. Thus, we can expect that blocking these packets does not have significant impact on the operators. On the other hand, the attacks, masqueraded as the traffic from an application, are more difficult to prevent because there is no certain way to differentiate between the normal traffic and the masqueraded traffic. As a countermeasure, the attacks can be mitigated by locating the content server inside cellular networks. However, this is not easy to adopt since the service is usually operated by a third party. Another method is for operators to utilize the anomaly detection and prevention. For example, when the amount of the downlink traffic is significantly more than the acknowledgment traffic of the uplink, or the large amount of traffic using unused port number in the real system is observed at the server of the service provider, it is likely to be an attack. However, this method can cause false positives; thus, it should be given more considerations prior to application.

7 Conclusion

In this study, we analyzed the charging policies for two different protocols, namely, ICMP and TCP, in six major operators of the U.S., and South Korea. We found that all operators in South Korea did not charge ICMP echo request/reply messages, and TCP-SYN and TCP-RST packets. In addition, we also investigated the charging policies and mechanisms for applications used for optional services and customer services, and discovered that operators utilized only the IP addresses to verify whether the traffic comes from the expected application. By misusing the findings with consideration of NAT in IPv4 cellular networks, we validated the feasibility of the free-riding attack.

Our study provides some insights. Operators should be reminded that unthoughtful charging policies can lead to the free-riding attack. Furthermore, the charging system limitation that lies in the middle of communication allowed the viewing of the information in the protocol header only, making it difficult to handle the charging problems occurring at the end points. Therefore, we recommend that operators adopt additional methods to monitor their core networks and end points.

Acknowledgement. This research was supported by (1) Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning), and (2) the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2016-R0992-16-1006) supervised by the IITP.

References

1. 3GPP: Access Network (E-UTRAN); Architecture description. TS 36.401, 3GPP (2010)
2. 3GPP: Telecommunication management; Charging management; Charging architecture and principles. TS 32.240, 3GPP (2010)
3. 3GPP: LTE; Network architecture. TS 23.002, 3GPP (2011)
4. 3GPP: Telecommunication management; Charging management; Online Charging System (OCS): Applications and interfaces. TS 32.296, 3GPP (2011)
5. 3GPP: LTE; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN). TS 29.061, 3GPP (2015)
6. Braden, R.: Requirements for Internet Hosts - Communication Layers. RFC 1122 (INTERNET STANDARD) (Oct 1989), http://www.ietf.org/rfc/rfc1122.txt, updated by RFCs 1349, 4379, 5884, 6093, 6298, 6633, 6864
7. Cheng, Y., Chu, J., Radhakrishnan, S., Jain, A.: TCP Fast Open. RFC 7413 (Experimental) (Dec 2014), http://www.ietf.org/rfc/rfc7413.txt
8. Go, Y., Won, J., Kune, D.F., Jeong, E., Kim, Y., Park, K.: Gaining Control of Cellular Traffic Accounting by Spurious TCP Retransmission. In: Network and Distributed System Security Symposium (NDSS) (2014)
9. Kim, H., Kim, D., Kwon, M., Han, H., Jang, Y., Han, D., Kim, T., Kim, Y.: Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations. In: ACM Conference on Computer and Communications Security (2015)
10. Li, C.Y., Tu, G.H., Peng, C., Yuan, Z., Li, Y., Lu, S., Wang, X.: Insecurity of Voice Solution VoLTE in LTE Mobile Networks. In: ACM Conference on Computer and Communications Security (2015)
11. Peng, C., Li, C.y., Tu, G.H., Lu, S., Zhang, L.: Mobile data charging: new attacks and countermeasures. In: Proceedings of the 19th ACM SIGSAC Conference on Computer and Communications Security (2012)
12. Peng, C., Li, C.Y., Wang, H., Tu, G.H., Lu, S.: Real Threats to Your Data Bills: Security Loopholes and Defenses in Mobile Data Charging. In: ACM Conference on Computer and Communications Security (2014)

13. Postel, J.: Internet Control Message Protocol. RFC 792 (INTERNET STANDARD) (Sep 1981), `http://www.ietf.org/rfc/rfc792.txt`, updated by RFCs 950, 4884, 6633, 6918
14. Smith, A.: US Smartphone Use in 2015. Pew Research Center (2015)
15. Srisuresh, P., Holdrege, M.: IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663 (Informational) (Aug 1999), `http://www.ietf.org/rfc/rfc2663.txt`