How Voice Service Threatens Cellular-Connected IoT Devices in the Operational 4G LTE Networks

Tian Xie
Computer Science and Engineering
Michigan State University
East Lansing, USA
xietian1@msu.edu

Chi-Yu Li
Department of Computer Science
National Chiao Tung University
Hsinchu, Taiwan (R.O.C)
chiyuli@cs.nctu.edu.tw

Jiliang Tang, Guan-Hua Tu
Computer Science and Engineering
Michigan State University
East Lansing, USA
{tangjili,ghtu}@msu.edu

***Abstract*—LTE networks are rolling out cellular Internet-of-Things (IoT) services. Cellular-connected IoT devices are becoming increasingly popular and the number is forecasted to grow almost fourfold from 2015 to 2021. Since they share the same infrastructure with non-IoT devices such as smartphones, we may expect no big differences between them in terms of voice/data service accounting/charging (e.g., paying for what you get) and security risks. However, our study shows that cellular IoT users may pay more than what they get, as well as are vulnerable to voice signaling spams and thus suffer from an overcharging attack which leads to financial loss or denial of service. We validate our proof-of-concept attack in a major U.S. cellular network operator which takes higher than 35% market share. We finally propose a solution to address the identified security vulnerabilities.**

I. Introduction

The cellular network is the only wireless infrastructure that offers ubiquitous data and voice services. On top of the existing network infrastructure, it introduces cellular Internet-of-Things (IoT) to interconnect "Things". Owing to its ubiquitous coverage, cellular-connected IoT devices proliferate. The number is forecasted to grow almost fourfold from 2015 to 2021 and reaches 1.5 billion with a compound annual growth rate of 24.6% [9]. Several cellular IoT technologies (e.g., Rel-8/Cat.4, Rel-8/Cat.1 [17]) have been proposed in 4G LTE networks to support a variety of IoT service demands from critical IoT applications (e.g., safety control) to massive ones (e.g., smart metering). They can support a wide range of data rates from 0.2 Mbps to 150 Mbps [25] and achieve low-power consumption (e.g., sustaining a ten-year battery life [20]). In contrast, other non-cellular IoT technologies (e.g., LoRA [6] and SigFox [23]) mainly target low-speed (e.g., less than 50 Kbps) and low-power IoT services.

Three major U.S. cellular network operators including Verizon, AT&T, and T-Mobile have launched cellular IoT services based on the Rel-8/Cat.4 IoT technology, one of the most popular ones for wearable devices, car-connected hotspots, and critical IoT devices. The operators charge an IoT device for both of a service consumption fee and a device access fee. The service consumption can be counted together with an existing service plan of conventional devices (e.g., smartphones). That is, the owner can choose to add the IoT device to his/her existing mobile service plan, which was mainly used for his/her smartphone(s). The device access fees of current IoT devices are usually cheaper than those of conventional smartphones (e.g., they are $5 and $20 for smartwatches and smartphones, respectively, when they are added to a non-unlimited data plan in Verizon), possibly due to their hardware limitations (e.g., small screens or low-speed 4G modems).

At the first glance, the existing network infrastructure serving conventional non-IoT devices should be able to well support those low-profile IoT devices. However, our study on the cellular Rel-8/Cat.4 IoT service charging yields a counter-intuitive finding.

Our results show that IoT users may pay more than non-IoT users for the same voice/text services and suffer from a new IoT overcharging attack, where adversaries can remotely increase data usage on the victims' IoT devices and thus cause them to be overcharged. In addition to the financial loss, it can be exploited to launch a denial-of-service attack against IoT users. More threateningly, the malware is not required to being installed on victims' devices and the victims are unaware of the attacks. The fundamental root cause is that cellular charging functions are not customized for IoT services according to their operations, which are different from non-IoT ones. Specifically, conventional charging functions operating on a per-bearer (i.e., IP connectivity) basis for smartphones may not be applied to all of IoT devices due to their hardware limitations. We validate the attack, IoT overcharging, in a major U.S. cellular network operator, which takes higher than 35% market share, and then propose a recommended solution, flow-based charging.

The rest of this paper is structured as follows. Section II presents related work. Section III introduces the background of cellular IoT support and potential security, as well as our threat model and methodology. In Section IV, we present how improper IoT service charging functions cause a new security vulnerability, sketch a proof-of-concept attack and discuss some remaining issues. Our proposed solution is described in Section V. Section VI concludes the paper.

II. Related Work

Current studies about IoT security can be mainly categorized into three dimensions: (1) device software/hardware, (2) network protocols, and (3) security architecture. In the first

Technologies	Rel-8/Cat.4	Rel-8/Cat.1	Rel-12/Cat.0	Rel-13/Cat.M1	Rel-13/NB-IoT
IoT types	Critical	Critical/Massive	Massive	Massive	Massive
Downlink peak rate	150 Mbps	10 Mbps	1 Mbps	1 Mbps	0.2 Mbps
Uplink peak rate	50 Mbps	5 Mbps	1 Mbps	1 Mbps	0.2 Mbps
Duplex mode	Full	Full	Half/Full	Half/Full	Half
UE bandwidth	20 Mhz	20 Mhz	20 Mhz	1.4 MHz	180 KHz
UE max transmission power	23dBm	23dBm	23dBm	20 or 23dBm	23dBm
Complexity vs. Cat.1	125%	100%	50%	20-25%	10%
Voice over LTE	Yes	Yes	Yes	Yes	NA
Battery life	day(s)	year(s) [7]	>10 years [20]	>10 years [20]	>10 years [20]

TABLE I
SUMMARY OF CELLULAR IOT TECHNOLOGIES IN 4G LTE [7], [12], [13], [17], [20], [25].

dimension, a study [8] shows that an IoT botnet built from the Mirai malware [1] is able to launch a 600 Gbps traffic attack. Another work [16] presents a threat that adversaries can compromise smart meters to reduce their utility bills. In the second dimension, Sastry *et al.* [22] discover several security vulnerabilities and pitfalls (e.g., using the same keys in multiple ACL entries) in IEEE 802.15.4 (LR-WPANs, Low-Rate Wireless Personal Area Networks), which is designed for wireless communication between low-power IoT devices. Last, some novel security architectures have been proposed, e.g., data-origin authentication, integrity verification, privacy preserving, and identity-based encryption. Jia *et al.* [15] propose `ContexIoT`, a context-based permission system for IoT platforms. It provides contextual integrity (privacy as contextual integrity [19]) and prototypes it on the Samsung SmartThings platform. Different from them, we here focus on the security of cellular IoT charging in 4G LTE networks.

III. New Security Issues Caused by Cellular IoT Support

In this section, we review the IoT support in cellular networks and identify its potential vulnerabilities, as well as describe our threat model and assessment methodology. In this work, we consider two top-tier U.S. operators, which are denoted as OP-I and OP-II for privacy concerns.

A. Cellular IoT Primer

Cellular IoT is a newly emerging IoT solution supported by cellular networks. It leverages the existing 4G LTE network architecture to support a variety of IoT devices based on various network specifications. We next introduce the network architecture and various IoT specifications.

1) Network Architecture: Figure 1 illustrates a simplified 4G LTE network architecture for the cellular IoT support. It consists of two major components: Radio Access Network (RAN) and Core Network (CN). The RAN offers various radio access specifications to the diversified IoT devices (*e.g.*, car connected devices, smart meters, wearable devices, etc.). The CN consists of three planes: management, control, and data planes. The traffic of both the management and control planes is forwarded through the signaling path, whereas data-plane traffic is delivered along the data path. In the management

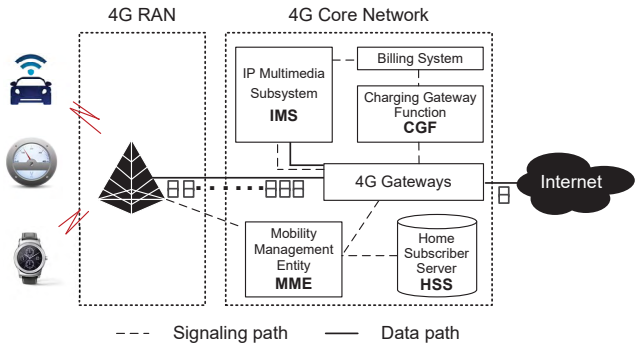

Fig. 1. 4G LTE network architecture for cellular IoT support.

plane, the Charging Gateway Function (CGF) and the billing system are used to account for the service amounts consumed by mobile devices and generate their bills, respectively. The traffic statistics used for the charging are collected by the 4G gateways and then reported to the CGF. In the control plane, the CN includes two main entities: Home Subscriber Server (HSS) and Mobility Management Entity (MME). The HSS records the IoT devices' service subscription, whereas the MME administrates mobility, authentication, and resource reservation (e.g., data bearer establishment). In the data plane, the CN connects the RAN, the IP Multimedia Subsystem (IMS), and the Internet. It relies on the 4G gateways to forward data-plane packets between the RAN and the IMS, as well as those between the RAN and the Internet. These two forwarding paths serve IMS services and the Internet access, respectively. The IMS provides IoT devices with IP-based services, e.g., VoLTE (Voice over LTE) [1] allows users to dial calls from their wearable devices.

2) IoT Specifications: Various network specifications in the 4G LTE network have been proposed to meet diverse demands from IoT devices. They cover both critical applications (e.g., traffic/safety control) and massive ones (e.g., smart agriculture). The former requires ultra reliability, low latency, and high availability, whereas the latter focuses on low cost, low energy, and small data volumes. Totally, five specifications, which require different hardware capabilities, are introduced: Release-8/Category-4 (Rel-8/Cat.4), Rel-8/Cat.1,

[1] VoLTE is the designated voice solution to the LTE mobile network.

Rel-12/Cat.0, Rel-13/Cat.M1, and Rel-13/NB-IoT [7], [12], [13], [17], [20], [25]. The first one is designed for the critical applications, the second is for both critical and massive applications, and the last three are for the massive ones. The details are summarized in Table I. Nowadays, the Rel-8/Cat.4 cellular IoT technology has been widely used, whereas the Rel-8/Cat-1 and Rel-13/Cat.M1 ones were newly launched by major U.S. operators (e.g., T-Mobile, AT&T) in 2017. The remaining Rel-13/NB-IoT is projected to be launched in the following years.

B. Potential Vulnerabilities

The cellular network seeks to offer network services to various IoT devices. The service charging function, which records the amounts of voice/data services consumed by each device, should be customized for the IoT devices, since that of conventional non-IoT devices (e.g., smartphones) may not be applied to them. The conventional charging function operates on a per-bearer (i.e., IP connectivity) basis. For example, a VoLTE-enabled smartphone creates different bearers for the VoLTE voice and mobile data services. The bearers are assigned different charging mechanisms: time-based and volume-based charging, respectively. However, the per-bearer charging method may not work for the IoT devices with hardware limitations (e.g., only supporting a single bearer or unable to always keep multiple bearers). Without carefully examining the charging-related or charging functions for the IoT devices, enabling cellular IoT support may result in monetary loss for IoT users.

C. Threat Model and Methodology

In this work, victims are IoT users. The adversary requires only commodity smartphones with their root privileges. In all cases, the adversary has no control of the network infrastructure or victims' devices.

We validate our proposed vulnerabilities and attacks in two top-tier U.S. carriers, OP-I and OP-II. They together take more than 65% of market share [24] in the U.S. We conduct experiments by using two popular Rel-8/Cat.4 cellular-connected smartwatch models and three smartphone models. Those two smartwatch models include LG Watch Urbane 2nd edition with Android 6.1.1 and Samsung Gear S3 frontier with Tizen OS 2.3.2. Those three phone models are Samsung Galaxy S5, LG G3, and Samsung Galaxy S6. We understand that some feasibility tests and attack evaluations might be harmful to mobile users or carriers, so we proceed with this study in a responsible manner. All the victims are the authors of this paper. We purchase sufficient text/voice/data volumes for all of our experiments, so the carriers do not get hurt.

IV. Improper IoT Service Charging Function

The existing service charging function may be improper for the IoT devices, since they may operate differently from the conventional devices. When it is applied to the IoT services without any changes, vulnerabilities may arise. We next present its vulnerability and exploit it to devise an overcharging attack, which causes users to be overcharged.

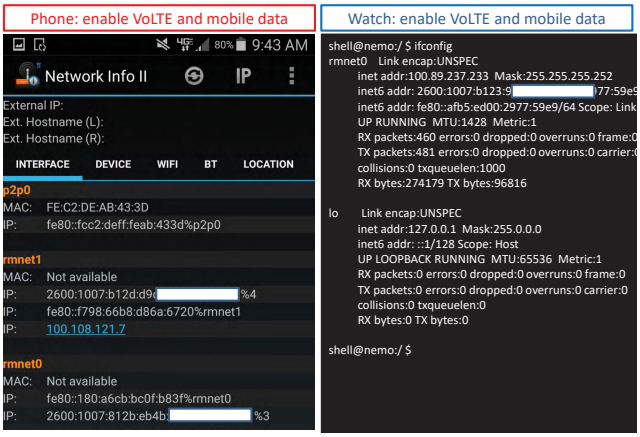

Fig. 2. The network interface information for a smartphone (left) and a smartwatch (right), which support both mobile data and VoLTE services.

A. Vulnerability: IoT Service Mismatched Charging

The conventional devices differentiate services by bearers (i.e., IP connectivity), and then different charging methods are applied based on a per-bearer charging function. This charging function may not work for the IoT devices, which may have only one bearer for their multiple services. When a single bearer needs to carry multiple services, either a new charging function is required, or the IoT services are charged in a different way from the conventional ones.

We discover a vulnerability that the charging method of the VoLTE service for IoT devices (i.e., smartwatches) is different from that for smartphones. This mismatch of service charging methods may be abused in the OP-I network. Note that the VoLTE service is supported by four major cellular IoT technologies including Rel-8/Cat.4, Rel-8/Cat.1, Rel-12/Cat.0 and Rel-13/Cat.M1 ([12], [13]). Operators can determine if the VoLTE service is enabled for cellular IoT devices or not. For example, in the OP-I network, VoLTE service is enabled on the smartwatches, whereas the OP-II still uses the Circuit-switched Fallback (CSFB) [3] voice service[2] for its wearable devices.

A VoLTE-enabled smartphone usually maintains two bearers: one is used for mobile data service, whereas the other is for the VoLTE signaling messages (e.g., call setup signaling). Whenever a VoLTE call is established, another bearer is created for the delivery of voice packets. Different charging methods are applied to the data and VoLTE services based on their three different bearers [5], [18]. Specifically, the bearers of the data service and the VoLTE signaling are assigned volume-based and time-based charging schemes, respectively. The bearer of the VoLTE voice is not associated with any charging scheme since the VoLTE service charging relies on its signaling only.

We discover that in our test smartphones, two network interfaces, `rmnet0` and `rmnet1`, are created for the data and VoLTE bearers, respectively. However, we find that the

[2]A 4G LTE device will be switched to 3G system while it tries to access the voice service.

test smartwatches are unable to always keep multiple network interfaces on. In some locations (e.g., in weak signal areas), only one interface, `rmnet0`, is observed, on the smartwatches which support both data and VoLTE services, whereas the smartphones can keep both of `rmnet0` and `rmnet1` on in the same locations. It may be caused by the hardware restrictions of smartwatches (e.g., smaller antenna) since it is not rare to be observed in practice. Figure 2 shows the network interface information of the smartphone and the smartwatch. Note that by observing the VoLTE signaling messages [18], we identify that the smartwatch has the VoLTE service only in the OP-I network but not in the OP-II network.

When the smartwatch relies on a single bearer to serve both the data and VoLTE services, the services may be assigned the same charging method. It is either the volume-based or the time-based charging scheme. Since the smartwatch is still associated with a volume-based charging record from the carrier (i.e., it consumes data volume of its service plan), the bearer's charging method should be volume-based. The VoLTE service may thus be charged based on its data volume, and there is a mismatch between the VoLTE service charging schemes for the smartphone (i.e., time-based) and the smartwatch (i.e., volume-based). Moreover, once the VoLTE signaling is not free in terms of traffic volume, signaling spams may cause mobile users to be overcharged.

a) Validation: To validate whether the VoLTE service charging is volume-based for the smartwatch, we make tens of VoLTE calls to it and then check its data usage volume. We then develop two Android applications: one is to collect data usage volume on the smartwatch using the Android class `TrafficStats`, and the other is to automatically make VoLTE calls from an Android smartphone. In our experiments, we make 50 VoLTE calls to the OP-I's smartwatch. We observe that average data volumes of the VoLTE signaling and VoLTE voice traffic are around 13 KB per call and 5.4 KB per second, respectively. By checking the smartwatch's data usage and call duration from the OP-I's website, we validate that those 50 calls are charged based on both their aggregate volume and their total call duration.

b) Root Causes: Carriers do not revisit the per-bearer charging function for the IoT devices, but the design of the IoT's bearer usage should be different from the existing one due to their limited hardware capability or/and power-saving requirement. The per-bearer charging, which associates each bearer with only one charging scheme, is not applied to multiple services with different charging methods over a single bearer. As a result, when two functions (i.e., the bearer usage and the charging function) affect each other and one of them needs to be changed, it is necessary to reexamine them together with the changes.

B. Proof-of-concept Attack: IoT Overcharging

We exploit the aforementioned vulnerability to devise an IoT overcharging attack which empowers adversary to remotely cause a mobile victim to be overcharged by sending a large number of VoLTE call signaling spams to the victim's smartwatch. To launch this attack, the adversary needs to know the phone number associated with the victim's device. Note that the victim is unaware of the attack since the adversary never causes the victim's smartwatch to ring. Even if the devices associated with the attacked phone numbers are not smartwatches in the OP-I network, they do not ring either. Thus, this attack can be launched on a large scale by targeting all the phone numbers belonging to the OP-I.

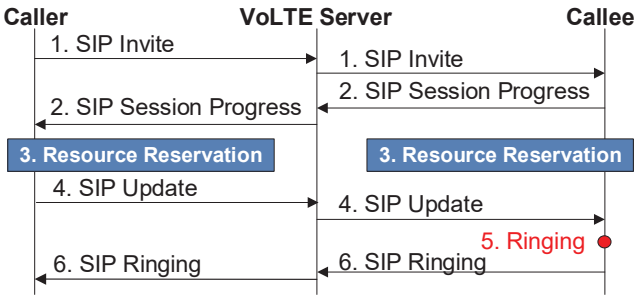

Fig. 3. A simplified VoLTE call flow [10].

In order to prevent the victim's smartwatch from ringing during the attack, the attack calls need to be carefully manipulated to terminate right before the event that triggers the play of victim's ringtone. Figure 3 illustrates a simplified VoLTE call flow. At the beginning of the VoLTE call setup, the caller sends a `SIP INVITE` message to the callee via the VoLTE server, and then receives a `SIP SESSION PROGRESS` message from the callee. Right after sending and receiving the message, the callee and the caller respectively make their resource reservation. After completing the reservation of resources, the caller will send a `SIP UPDATE` message to the callee. Without receiving this message, the callee does not ring. An adversary can thus suppress the callee's ringtone for each attempt call by interrupting the call right after the `SIP SESSION PROGRESS` message is observed on the caller. We then develop an Android application, *VoLTECaller*, on top of the tool which we previously developed to silently drain the smartphone batteries of victims and suffocate their data services [26]. It makes a VoLTE call towards the victim and then interrupts the dialing right after observing the `SIP SESSION PROGRESS`.

We want to note one thing. Even if the callee (the victim) uses the traditional circuit-switched (CS) voice solution instead of VoLTE, this approach still works. The CS callee does not ring until the VoLTE caller completes his/her resource reservation. Specifically, after the VoLTE-CS gateway[3] receives the caller's `SIP UPDATE` message, it will send a CS signaling message, `ISUP CON` [11], to the CS callee and the callee starts to ring. The callee does not ring without receiving the `ISUP CON` message. Moreover, the time that is required to trigger the CS-based callee's ringtone, is much longer than that for the VoLTE callee [14]. As a result, the VoLTE call made by the *VoLTECaller* does not cause the callee to ring,

[3]It is called Media Gateway Control Function (MGCF) in mobile network standards [2].

no matter which voice solution (VoLTE or CS-based) is used by the callee.

We use the *VoLTECaller* application to validate the feasibility of the IoT overcharging attack and evaluate its damage impacts. It places 100 VoLTE calls from our VoLTE-enabled smartphone to our test smartwatch and records the data usage of the smartwatch. The attack lasts for around five and half minutes. Figure 4 plots the data usage per second (Top) and accumulated usage (Bottom) on the victim's watch. We have three observations. First, the victim's watch does not ring during the attack. Second, the attack causes the recorded data volume to increase by 681 KB. We also verify that the volume is similar to the amount charged by the OP-I. Third, only 3.24 seconds are averagely required by each VoLTE call attempt.

Besides, we find that not all the calls successfully increase the data volume received by the callee from our collected trace. With a further analysis, we infer that during the initial period of a VoLTE call setup (i.e., the delivery of the `SIP INVITE` and `SIP SESSION PROGRESS` messages), the OP-I's VoLTE server may communicate with the caller on behalf of the callee.

This design not only spares the cellular network a period of time to find the callee and makes it prepared for the VoLTE signaling exchange but also prevents some 4G LTE callers supporting both of VoLTE and CS-based voice solutions from introducing extra call signalings[4]. Therefore, if the caller cancels the VoLTE call before the callee is ready for the VoLTE signaling exchange, the callee will not receive any signaling messages from that call attempt. Due to various time durations required by the callee's preparation for different call attempts, not all of the attack calls are successful (i.e., causing the callee to receive signaling spams). In our experiments, the success rate is about 52%, but the victim's smartwatch does not ring for all the cases. If the attack lasts for a day, adversaries are projected to cause the victim to be overcharged around 177 MB.

C. Discussion

We next discuss two remaining issues of this VoLTE signaling spam overcharging attack.

Small damages? People may argue that the 177 MB overcharging volume per day is not considered as a serious attack. Li and et al. [18] have showcased how to launch an overcharging attack against a smartphone user without limits in 2015. However, the vulnerability discovered in this work can have much bigger negative impacts than that in [18]. First, that study's overcharging attack requires the IP address of the victim's device before the attack is launched. In practice, the device's IP address assigned by the carrier is not fixed and difficult to be exposed. Adversaries may need to deploy the malware to get it. Different from this attack, our overcharging attack requires only the victim's phone number instead of IP address. Hence, it is easy to launch attacks in practice.

[4]For some VoLTE/CS-based-Voice 4G LTE devices, they will use VoLTE service as primary voice service, but switch to 3G system to access CS-based voice service if they do not receive any response from VoLTE servers for a period of time (e.g., it is 5 seconds on T-Mobile Samsung S5).

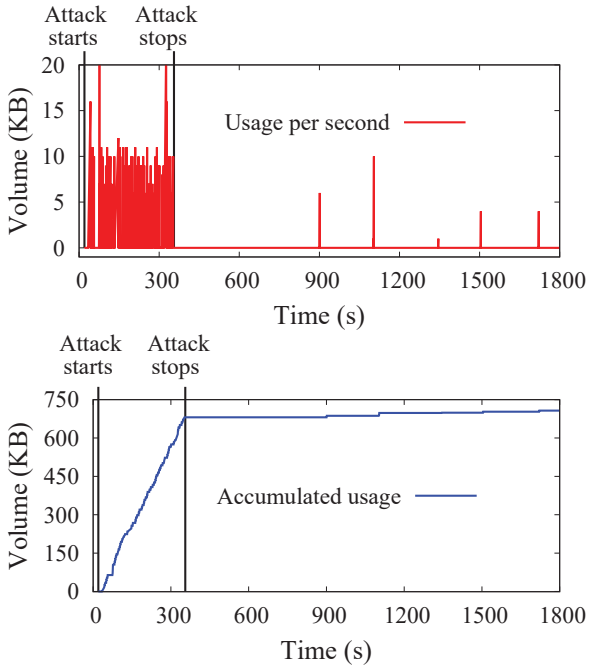

Fig. 4. Data usage volume of a test smartwatch under the IoT overcharging attack. There are 100 attack calls performed within first 324 seconds. Upper: usage volume per second. Bottom: accumulated usage volume per second.

Second, the victims of this VoLTE-based overcharging attack are IoT users instead of smartphone users. Unlike smartphone users, the IoT users may subscribe for only a small amount of mobile data service. For example, Verizon provides a cellular IoT charging plan for IoT users with lightweight usage, $2 for the monthly usage of 200 KB. By this attack, an adversary is capable of consuming 200 KB within 100 seconds. It can lead to two possible negative consequences: (1) denial of service, the victim cannot send and receive any data packets from IoT devices under the attack if s(he) does not automatically refill their IoT service plan after the purchased data quota has been reached. (2) non-negligible financial loss, the victim has to pay $2 for another 200 KB if s(he) automatically refills the IoT service plan. It means that the victim's bill will be increased by $2 every 100 seconds. Note that our proof-of-concept attack does not intend to cause significant damage in practice, but shows how the vulnerability can be exploited to launch a non-negligible attack. Therefore, we do not conduct a large-scale spamming attack, which should be feasible, in operational networks.

Limited to Rel-8/Cat.4 IoT devices supporting VoLTE? Some people may think that the identified security threat only hurts the Rel-8/Cat.4 IoT devices supporting VoLTE services. However, it may not be the case. First, all cellular IoT technologies (see Table I) are designed to support VoLTE services except for NB-IoT. Second, the problem is not rooted in the VoLTE service. The fundamental issue is that carriers do not distinguish both of IMS (IP Multimedia Subsystem)

signaling messages and IMS service data traffic from normal mobile data traffic (e.g., accessing the Internet). Thus, the IoT users have to pay both of service usage (e.g., $0.1 for a 1-min voice call) and data usage (e.g., 0.78MB for a 1-min voice call). Note that VoLTE is merely one of various IMS-based services (e.g., IMS-based text service, rich communication services, etc).

V. Solution: Flow-based Charging

In practice, operators charge a VoLTE call for its call duration instead of the data volume of the VoLTE signaling messages and voice packets. In the OP-I, this charging policy is enforced by a per-bearer charging function. The conventional devices differentiate services by bearers (i.e., IP connectivity), and then different charging policies (e.g., charging users for their data usage or service duration) are applied by operators to different bearers. However, this charging function may not work for the IoT devices, which may have only one bearer for all services.

To address this issue, we propose that operators should apply a more fine-grained charging method, the flow-based service charging, for IoT devices. The charging is based on each service data flow. It can thus support the IoT devices' charging requirements, which apply different charging policies to multiple traffic types (e.g., normal data service, IMS services, etc.) over a single bearer. The flow-based service charging is one of charging mechanisms stipulated by cellular network standards [4] and works as follows. One service data flow is typically identified by the five-tuple information: (1) source IP address or mask, (2) source port number, (3) destination IP address or mask, (4) destination port number, and (5) protocol ID (e.g., TCP or UDP). For example, a VoLTE signaling data flow in OP-I can be represented by the five-tuple: (*, *, VoLTE_Server_IP, 5060, TCP). Carriers can define a set of flow rules for each service and then apply a charging policy to the set. The identified security vulnerability can thus be eliminated. We believe that the proposed flow-based service charging is practical and will not introduce too much deployment effort to carriers since several U.S. ones such as T-Mobile and Verizon applied this mechanism to providing users with free DNS services (i.e., packets over TCP/UDP destination port 53 are free of charge) in their cellular networks [21].

VI. Conclusion

In this work, we study the security implication of such IoT charging that relies on the legacy features and the carriers' freedoms. Our study yields two insights. First, with improper charging functions in the current operational networks, the IoT users may be charged in the ways which they do not anticipate. For a voice call, they pay for not only service usage (e.g., $0.1 per minute) but also data usage (e.g., 0.78MB per minute). They are more vulnerable to signaling spamming attacks than non-IoT users. Second, to fairly and accurately charge IoT users, carriers have to identify each flow of data transmitted to/from the IoT devices and thus require more resources on the IoT devices than non-IoT ones. Without careful resources planning and well-designed IoT charging mechanisms/plans, carriers may not gain from the support of these cellular IoT devices. We hope our pioneering study will stimulate further research on cellular IoT security from both academia and industry.

References

[1] "Mirai Malware for Botnet," 2017, https://en.wikipedia.org/wiki/Mirai_(malware).

[2] 3GPP, "TS23.228: IP Multimedia Subsystem (IMS);Stage 2," http://www.3gpp.org/ftp/Specs/html-info/23228.htm.

[3] ——, "TS23.272: CSFB in EPS," 2012. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/23272.htm

[4] ——, "TS 23.203:Policy and charging control architecture," Dec. 2016.

[5] ——, "TS32.240:Telecommunication management; Charging management; Charging architecture and principles," 2016.

[6] L. Alliance, "Lora Alliance Technology," 2017, https://www.lora-alliance.org/technology.

[7] AT&T, "Low cost LTE modules for the Internet of Things," 2016, https://www.business.att.com/enterprise/Service/internet-of-things/networks/wnc-modules/.

[8] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb 2017.

[9] Ericsson, "Cellular networks for massive IoT," Jan. 2016, https://www.ericsson.com/res/docs/whitepapers/wp_iot.pdf.

[10] EventHelix, "IMS to IMS Call Flow," 2015, http://www.eventhelix.com/ims/ims_to_ims_call/ims_to_ims_call.pdf.

[11] ——, "IMS to PSTN(CS) Call Flow," 2015, http://eventhelix.com/ims/ims-to-pstn-call/ims-to-pstn-callflow.pdf.

[12] Gemalto, "VoLTE for LTE Cat. 1," http://www.gemalto.com/m2m/development/innovation-technology/volte-lte-cat1.

[13] D. Goovaerts, "Verizon Claims First Successful VoLTE Call on LTE Cat-M1 Network," Jun. 2017, https://www.wirelessweek.com/news/2017/06/verizon-claims-first-successful-volte-call-lte-cat-m1-network.

[14] K. Hill, "VoLTE gets high marks in initial benchmarking," https://www.rcrwireless.com/20150617/test-and-measurement/volte-gets-high-marks-in-initial-benchmarking-tag6.

[15] Y. J. Jia, Q. A. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. M. Mao, and A. Prakash, "ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms," in *IEEE NDSS'17*.

[16] B. Krebs, "FBI: Smart Meter Hacks Likely to Spread," 2012, https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/.

[17] A. Leckie, "LTE Category-0 & LTE-M low power M2M device roadmaps," May 2015, http://iotdevzone.com/blog/2015/05/18/lte-category-0-lte-m-low-power-m2m-device-roadmaps/.

[18] C.-Y. Li, G.-H. Tu, C. Peng, Z. Yuan, Y. Li, S. Lu, and X. Wang, "Insecurity of voice solution volte in lte mobile networks," in *ACM CCS'15*.

[19] H. Nissenbaum, "PRIVACY AS CONTEXTUAL INTEGRITY," 2004, https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf.

[20] Nokia, "LTE evolution for IoT connectivity," 2017, http://resources.alcatel-lucent.com/asset/200178.

[21] C. Peng, G. Tu, C. Li, and S. Lu, "Can we pay for what we get in 3g data access?" in *ACM Mobicom'12, Istanbul, Turkey, August 22-26, 2012*, 2012.

[22] N. Sastry and D. Wagner, "Security considerations for ieee 802.15.4 networks," in *ACM WiSe'04*.

[23] SigFox, "SigFox IoT Technology," 2017, https://www.sigfox.com.

[24] Statista, "Market share of mobile network carriers in the U.S," 2017, http://www.statista.com/statistics/199359/market-share-of-wireless-carriers-in-the-us-by-subscriptions/.

[25] T. Tirronen, "Cellular IoT Alphabet Soup," Feb. 2016, https://www.ericsson.com/research-blog/internet-of-things/cellular-iot-alphabet-soup.

[26] G. H. Tu, C. Y. Li, C. Peng, and S. Lu, "How voice call technology poses security threats in 4g lte networks," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sept 2015, pp. 442–450.