Unveiling the Hidden Dangers of Public IP Addresses in 4G/LTE Cellular Data Networks

Wai Kay Leong, Aditya Kulkarni, Yin Xu and Ben Leong
School of Computing, National University of Singapore

ABSTRACT

While it is often convenient for mobile cellular devices to have a public IP address, we show that such devices are vulnerable to stealthy malicious attacks. In particular, we show with experiments on three 4G/LTE cellular data networks in Singapore that it is easy for an attacker to initiate three different types of attacks on such mobile devices: (i) data quota drain, (ii) DoS flooding, and (iii) battery drain. Our experiments show that a potential attacker can completely exhaust the monthly data quota within a few minutes, completely choke the data connection of a mobile subscriber with a data stream of just 3 Mb/s, and increase the battery drain rate by up to 24 times. Finally, we argue that a simple proxy-based firewall with a secret IP address would be an effective and feasible defense against such potential attacks.

1. INTRODUCTION

Cellular data ISPs typically use network address translation to share a limited number of public IP addresses among a large number of subscribers. This means that most cellular devices are provided with private IP addresses and thus unable to receive direct incoming connections from the Internet, which consequently provides some form of security against IP-based network attacks. While it is not yet common practice, a small number of users do request, and often pay additional fees for public IP addresses for their cellular data connections from their ISPs [2, 10]. If IPv6 were to eventually find widespread adoption, then all mobile devices are likely to have their own public IP addresses.

While a public IP address might be desirable, we have found that it can cause a cellular device to be vulnerable to some potential malicious IP-based attacks. In recent years, significant amount of research efforts have been focused to demonstrate such attacks which particularly include over-billing attacks [5], battery depletion attacks [15, 16], Denial of Service (DoS) attacks [8, 17, 19], IP spoofing and masquerading attacks [12].

Though traditional servers and desktop computers are equally susceptible to such attacks, their impact is more severe for cellular subscribers because i) cellular data charges are often expensive and monthly data quota is typically limited, and ii) battery power is a limited resource. In addition to the typical IP-based denial-of-service (DoS) flooding and IP spoofing attacks, cellular devices are vulnerable to additional forms of attack that drain their data quota or battery. Thus, we investigate three forms of potential attacks: i) data quota drain, ii) DoS flooding, and iii) battery drain.

All three local mobile ISPs in Singapore provide a public IP address to their 4G/LTE subscribers at no additional charge. As such, we were able to investigate the effect of these attacks on our own mobile devices on these networks. Surprisingly, we found that an attacker requires only a small amount of resources to conduct these attacks. In particular, a low-rate data stream of less than 3 Mb/s was sufficient to launch a DoS flooding attack that reduces the victim's throughput to almost zero. Also, because 4G/LTE speeds are very high, it only takes an attacker about 10 minutes to completely exhaust the monthly 2 GB data quota of a mobile subscriber using a data stream of 30 Mb/s. Finally, by simply sending a stream of 0-byte payload UDP packets every 15 s, an attacker can drastically increase the battery drain rate by up to 24 times, by preventing a mobile phone from going to sleep mode.

These attacks cannot be prevented by installing a firewall on a mobile device, as harm would already have been done once the data packets reach the device. While it might be possible for an ISP to install a firewall to protect its mobile subscribers, the stealthy nature of these attacks (because of their low data rate) makes them hard to detect, and it would also be difficult for an ISP to differentiate malicious packets from legitimate incoming packets. An attacker might also decide to spoof the IP address of legitimate sources. We argue that a simple proxy-based firewall would be an effective and feasible defence against such potential attacks. This firewall would be implemented with proxy servers with two IP addresses, one public and one secret. Incoming connections would be received on the public IP and legitimate data is then forwarded to the mobile subscriber via the secret IP.

2. RELATED WORK

The availability of a public IP address in LTE networks is known to make cellular devices inherently susceptible to the common IP-based security attacks [12]. Early forms of DoS attacks on cellular phones target the intense signalling demands of the SMS protocol to overwhelm the network [19]. In modern 3G/4G networks, DoS attacks such as paging and signaling attacks can be done at the link layer by targeting the protocol state machine to cause unnecessary state changes, to overwhelm the network. Many of these attacks have been studied recently [4, 17, 8]. Bassil et al. simulated DoS-based signaling attacks over LTE, where the signaling overhead is exploited to prevent legitimate users from accessing the network [3]. Pelechrinis et al. showed that DoS-based jamming attacks are possible at the MAC and PHY layers [13]. Such attacks however require specialized hardware that is not easily available. Our work instead investigates attacks that can effectively be carried out at the network or transport layers using a single desktop computer.

Racic et al. described a stealthy battery depletion attack which drains the battery of a mobile device by exploiting the MMS and the GSM protocol in 3G networks and sending a 1,500-byte UDP packet every 3 to 5 s [16]. Puustinen et al. showed that unwanted background Internet traffic can drain the battery of a cellular device with a public IP address by keeping its cellular radio active to receive packets [15]. They showed in a simulation that a well chosen time-out value can mitigate the effects of background traffic.

Go et al. highlighted that flawed accounting policies in the cellular ISP's in USA and South Korea can result in subscribers be-

ACM HotMobile'14, February 26-27, 2014, Santa Barbara, CA, USA.
Copyright 2014 ACM 978-1-4503-2742-8 ...$15.00.

ing wrongly charged for retransmitted TCP packets [5], and this vulnerability in the ISP's accounting mechanism can be exploited by adversaries to inflate the subscriber's bill by sending unnecessary retransmissions. Similarly, Kang et al. discussed how an attacker with a cellular device can spoof the IP address of another subscriber in the same local network and send request packets to Internet servers [9]. These servers will then send their responses to the unsuspecting victim, thereby causing additional data charges as well as draining the battery.

Our work builds on these earlier works and quantifies these forms of attack and shows how using a very small UDP packet sent at longer intervals of 15 s can be effective in draining the battery. With the availability of a public IP, the attacker does not even need to reside in the same cellular data network as the victim to carry out such attacks.

3. POTENTIAL IP-BASED ATTACKS

To perform measurements on real commercial cellular data networks, we obtained the latest post-paid 4G/LTE plans from the three local ISPs in Singapore, which we anonymize as A, B and C. We ran our experiments using the cellular data plans with a 4G/LTE USB dongle and two smartphones, namely a Samsung Galaxy S3 LTE and a Samsung Galaxy S4. A server in our lab on campus was used to probe and initiate the attacks. `tcpdump` was used to capture and examine the packets on both the devices and the server, and `Iperf` was used to create UDP and TCP data streams and to measure the resulting throughput of the link. To measure instantaneous battery current consumption, we used a Monsoon Power Monitor [11].

3.1 Preliminaries

For the attacks to work, the mobile device must be assigned a public IP address. Among the three telcos, ISP A assigns a public IP address by default on the USB dongle and on the Samsung Galaxy S3 LTE phone. We were, however, not able to obtain a public IP with the Samsung Galaxy S4 for the ISP A network in spite of trying different known Access Point Names (APNs) and installing custom ROMs and kernels. The reason for this is still unknown. For ISP B and ISP C, we found that they assigned a private IP address by default. However, by simply changing the APN, we were able to obtain a public IP address. Note that we did not pay for nor request for a public IP address from any of the ISPs.

After obtaining a public IP address, we first tested reachability by pinging the device from our server using ICMP ping and were able to obtain a response for all three ISPs. Next, we restarted the cellular network interface to get a new IP address and attempted to send UDP packets from our server to random ports on the device. We found that while ISP A and ISP B allow all the UDP packets to reach the device, ISP C appears to block UDP packets. Only by first sending a UDP packet from the device to our server, does ISP C forward UDP packets originating from our server to any port on the device. This suggests that a simple firewall rule was implemented in the ISP C network which blocks unsolicited incoming connections. While this firewall rule might be useful, it will also block legitimate incoming UDP connections to the device. We subsequently found an alternate APN for ISP C that also assigned a public IP but did not have a firewall that blocks unsolicited incoming UDP packets. We proceeded to use this APN for ISP C in our experiments.

We also found that all incoming TCP SYN packets are forwarded by all ISPs, even for the APN with a firewall. While this allows a connected mobile device to host a TCP server, it also renders the device vulnerable to DoS attacks. The characteristics of the LTE networks of the ISPs are summarized in Table 1.

Table 1: Summary of LTE network characteristics

Property	ISP A	ISP B	ISP C
Public IP	By default*	Set APN	Set APN
ICMP Ping	Yes	Yes	Yes
Unsolicited UDP	Yes	Yes	Depends†
TCP SYN	Yes	Yes	Yes
Downlink Buffer‡	2000 pkts	600 pkts	800 ms‡
Throughput (Mb/s)			
- Maximum	34.1	50.4	35.8
- Average	24.7	30.6	26.8

*Except for Samsung Galaxy S4

†Some APNs block unsolicited incoming UDP packets

‡ The downlink buffers for ISP A and ISP B are sized in packets, while ISP C implements some form of AQM that drop packets which remain in the buffer for more than 800 ms [20].

3.2 Quota Drain

Most cellular data plans do not have unlimited quota. Depending on the ISP data plan, subscribers typically either pay for the data consumed, or are given a monthly quota. In the latter, they will be charged for exceeding the allocated quota. In both cases, subscribers would want to minimize redundant data usage and cost.

Peng et al. analyzed the data charging and accounting process of mobile ISPs and showed that data is considered consumed once it passes through the gateway of the 3G/4G network [14]. Thus, it is possible for subscribers to be charged for packets that are never delivered to the device, but are instead dropped at the base station. In such cases, it does not matter if the packets from a DoS attack eventually reach the device or not. They will be counted towards the subscriber's data quota. Go et al. briefly mentioned the possibility of such an attack when they examined how subscribers can be overcharged by TCP retransmissions [5]. Because of the billing structure of mobile ISPs, an attacker can simply flood the victim with random packets at a very high rate, and the victim will have to pay for all the packets, even if they do not eventually reach the victim's device. As wired broadband Internet is very cheap these days, an attacker on a wired host can easily flood such a victim at a negligible cost.

In our subsequent discussions, we assume that the mobile ISPs can address this billing issue and accurately charge the subscribers for the actual data delivered to the device. Under this assumption, the amount of data that an attacker can use to flood a victim will depend completely on the throughput of the cellular link. We performed a throughput measurement of our three cellular data plans by recording the time taken to download 3 MB of data. To obtain spatial and temporal diversity, we carried the phone as we went about with our daily routines and measured the time taken for these data downloads in the background periodically, throughout the day. We plot the cumulative distribution of the throughput in Figure 1 and summarize the average throughput in Table 1.

From our results, we can see that the LTE networks can achieve very high download throughput. This means that it is easy for an attacker to send large amounts of data to exhaust the victim's data quota. We plot in Figure 2 the amount of time needed to transfer between 1 GB to 4 GB of data as the network throughput increases. Given that local 4G/LTE data plans in Singapore are typically allocated a data allowance of 2 GB per month, an attacker can potentially completely exhaust our data quota with a throughput of 30 Mb/s in less than 10 minutes.

While a sustained flood of random UDP packets could be easily flagged by the ISP's firewall as a potential attack and the attacker be blocked or restricted, a potential attacker can circumvent this by

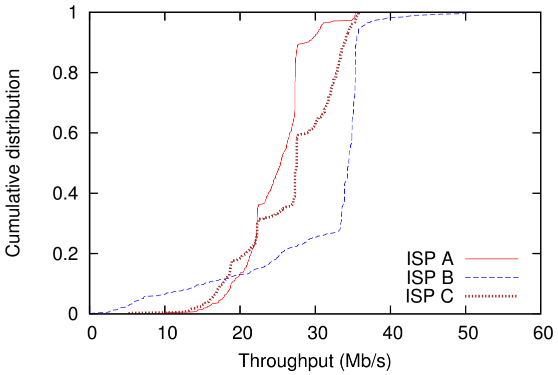


Figure 1: Cumulative distribution of measured throughput for LTE networks of local ISPs.

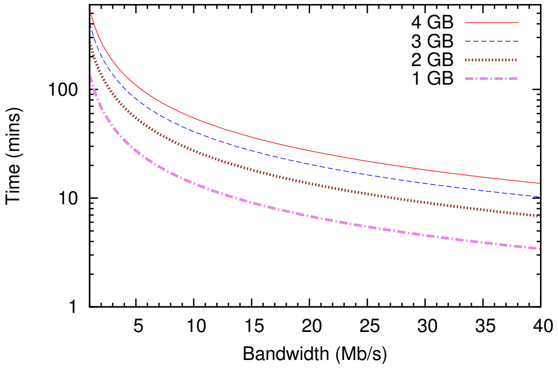


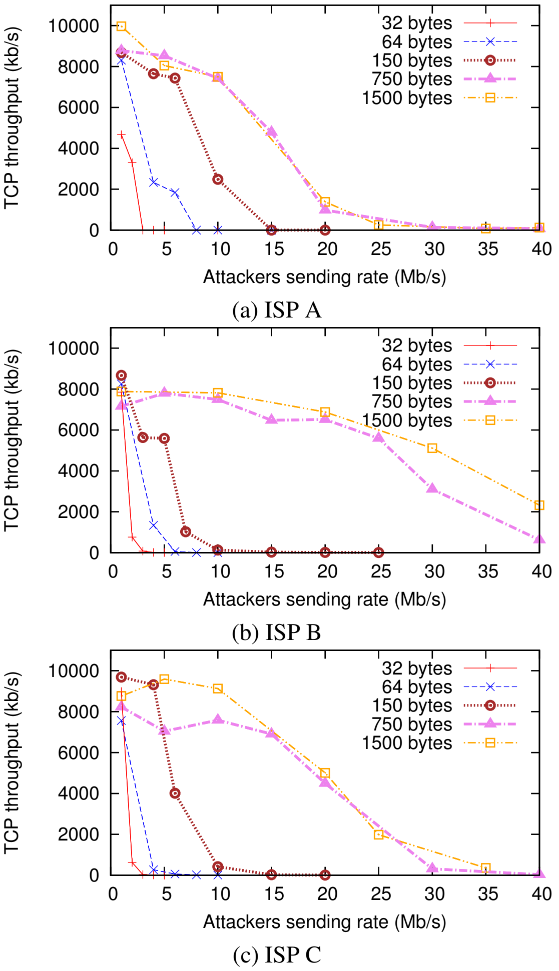
Figure 2: Amount of time needed to exhaust different sized quotas for different network throughputs.

scheduling the attack and spreading it out in small bursts over the entire billing month. While a regular stream of one packet every second would be easy to detect, sending 1 MB of data every 15 min would seem more legitimate, and result in 2.8 GB of accumulated data in a month. Since it takes less than half a second to transfer 1 MB of data at 30 Mb/s, this data transfer would be completed even before the victim has time to react. In today's context, 1 MB is not a particularly large or suspicious amount of data, and it would be hard to distinguish the attack flow from legitimate connections, especially if the attacker can spoof the source address of the packets.

3.3 DoS Flooding

We next investigate a naive denial-of-service attack where the victim is simply flooded with random traffic to congest the network link. We had earlier measured the size of the downlink buffers for the local ISPs, and found that the base stations implement separate buffers for each mobile device and schedule the transmissions with a fair queuing scheme [20]. The buffer sizes measured for the local LTE networks are given in Table 1.

Because 4G/LTE networks have such high speeds, ISPs typically provision a large buffer at the base stations of about 3 MB in size. This means that a naive DoS flooding attack will in principle have to send at least 3 MB of data at a high rate in order to saturate the buffer. However, we found that the downlink buffers of two of the three ISPs are sized in packets rather than in bytes. This means that a 1-byte packet will occupy the same buffer space as a 1,500-byte packet. Because of this property, an attacker is able to effectively saturate a subscriber's buffer using a stream of small packets. In addition, even if a sufficiently large buffer is provisioned, a high volume of small packets would increase the processing time in the receiver's network stack. This could potentially overwhelm mobile devices, since processors of mobile devices are slower than that for desktops systems and servers.



(a) ISP A

(b) ISP B

(c) ISP C

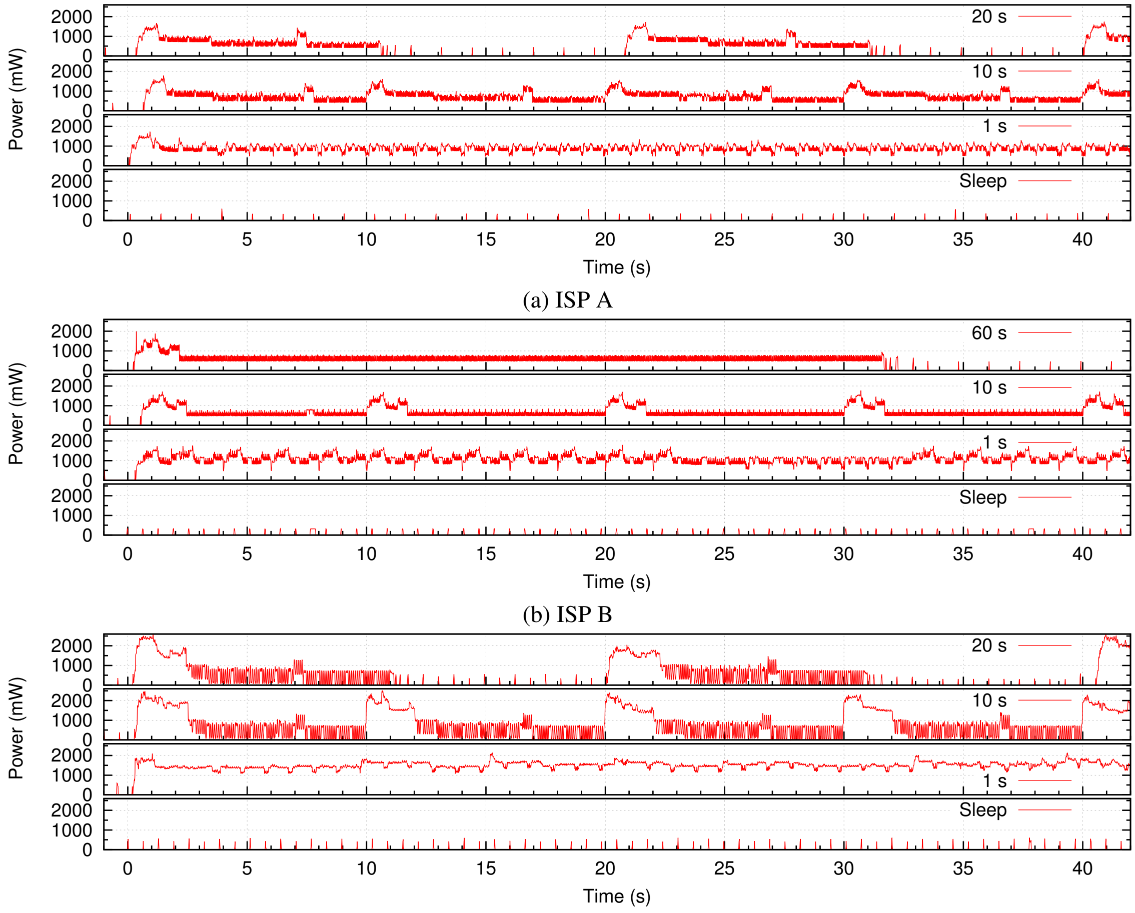
Figure 3: Plot of TCP goodput for UDP flooding at different rates for different packet sizes.

To investigate the effectiveness of a "small packet" DoS attack, we first sent a stream of UDP packets at a fixed rate to saturate the victim's buffer. After 1 s, we initiated a TCP connection from the server to the device in the presence of this background UDP stream. To avoid using an excessive amount of data, we stopped the UDP stream after 3 s and computed the TCP goodput achieved within this 2-second period. We varied the sending rate as well as the size of the UDP packets and plot the results in Fig. 3.

We can see from our results that by using small packet sizes, an attacker can effectively reduce the TCP throughput of a subscriber to almost zero, and he can achieve this at a very low data rate of less than 3 Mb/s. We also see that ISP C is also affected even though its buffer is not sized in packets. When examining the packet traces, we found that while no packets were lost, the time taken by the phone to process the UDP packets caused a delay in replying to the TCP SYN, thus affecting the TCP preformance. This shows that such "small packet" DoS attacks can still be effective against mobile devices with low processing resources independent of the ISP's buffering scheme. In our experiments for DoS flooding, we used a minimum packet size of 32 bytes because `Iperf` did not support smaller packet sizes. With a specially-written tool, it is possible to send UDP streams with no data payload.

3.4 Battery Drain

To conserve battery, a mobile device would typically put its radio to a low power `RRC_IDLE` state when there is no network communication. However, whenever a packet is received, the radio is



(a) ISP A

(b) ISP B

(c) ISP C

Figure 4: Trace of power consumption for 32-byte UDP packets with different inter-packet intervals.

promoted to a high powered RRC_CONNECTED state [1]. If there is no further communication after some timeout period, the radio state will be demoted back to the RRC_IDLE state. When a mobile device has a public IP address, it is possible for a malicious attacker to periodically send unwarranted packets to a mobile device and keep the device in the high powered RRC_CONNECTED state. This will cause significant and unnecessary battery consumption, since the radio is prevented from going to the RRC_IDLE state.

To investigate the impact of such an attack on battery consumption, we measured the current consumption of two mobile phones, a Samsung Galaxy S3 LTE and a Galaxy S4. We hooked up the two phones to a Monsoon Power Monitor [11] and measured the instantaneous current at 200-μs intervals. With this setup, we were able to observe minute changes in the current consumption as the phone sleeps and wakes.

We first began by turning off all sensors, background applications as well as the display to take a baseline reading. Thereafter, we sent a steady stream of 32-byte UDP packets from our server to the phone's IP address at a fixed interval, and recorded the current consumption. In Figure 4, we plot the traces of the power consumption for the Samsung Galaxy S3 LTE phone for different inter-packet intervals for each of the ISPs. We observed similar patterns with the Samsung Galaxy S4 phone.

Interestingly, we found that different ISPs use different sleep/wake schemes even for the same device. This coroborates previous work by Huang et al. where they investigated power consumption in 4G/LTE networks [6]. When idle, devices on the ISP B and ISP C networks periodically wake up every 0.5 s to listen for any incoming data, while those on the ISP A network wake up every 1 s. After receiving some data, a device will typically remain awake for a short duration to wait for potential new data before going back to sleep.

We can see in our traces that the different ISPs have different schemes for resuming sleep too. ISP A and ISP C both go back to sleep about 11 s after being woken up, while ISP B takes about 32 s to go back to sleep. This means that if an attacker is aware of the sleeping schedule for an ISP, he only needs to send a packet just when the phone is about to resume sleeping to prevent the phone from going back to sleep. In particular, this would be every 10 s for ISP A and ISP C, and every 30 s for ISP B. Huang et al. also reported observing go-to-sleep intervals of around 10 s [7]. This rather long time intervals between the attack packets would make such an attack rather stealthy and hard to detect.

We plot in Figure 5 the expected battery lifetime T_{alive} of the Samsung Galaxy S3 LTE on the stock battery of 2100 mAh against the inter-packet intervals for a 32-byte UDP packet stream. We measured the instantaneous current consumed by a mobile device using the Monsoon Power Monitor and estimated T_{alive} using following equation:

$$T_{alive}\ (h) = \frac{Battery\ Capacity\ (mAh)}{Average\ Current\ (mA)}$$

Because the average current consumption is approximately the same for all three ISPs when the inter-packet interval is 15 s, we use this value as the baseline to investigate the effect of a battery drain attack. In Table 2, we compare the estimated battery lifetime (T_{alive}), when the device is in idle mode with an active 4G data connection, to that when it is attacked with a stream of zero payload UDP pack-

Table 2: Estimated battery lifetime of Galaxy S3 LTE

	ISP A	ISP B	ISP C
T_{alive}(h)[*]	338.7	355.9	286.5
T_{alive}(h)[†]	13.8	12.2	12.0

[*] T_{alive} when phone has active 4G connection in idle mode

[†] T_{alive} when phone is under battery drain attack

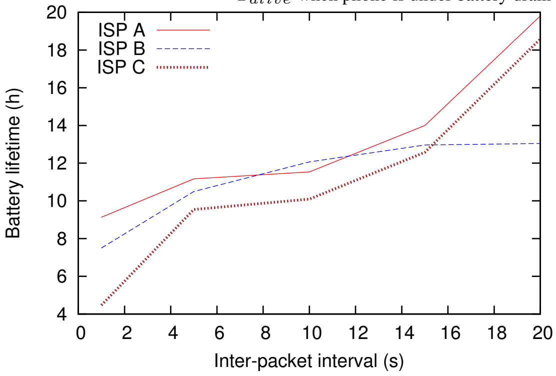


Figure 5: Effect of inter-packet intervals on expected battery lifetime for battery drain attack.

ets at 15 s intervals. For the duration of the experiment, all sensors, background applications and the display of the device were turned off.

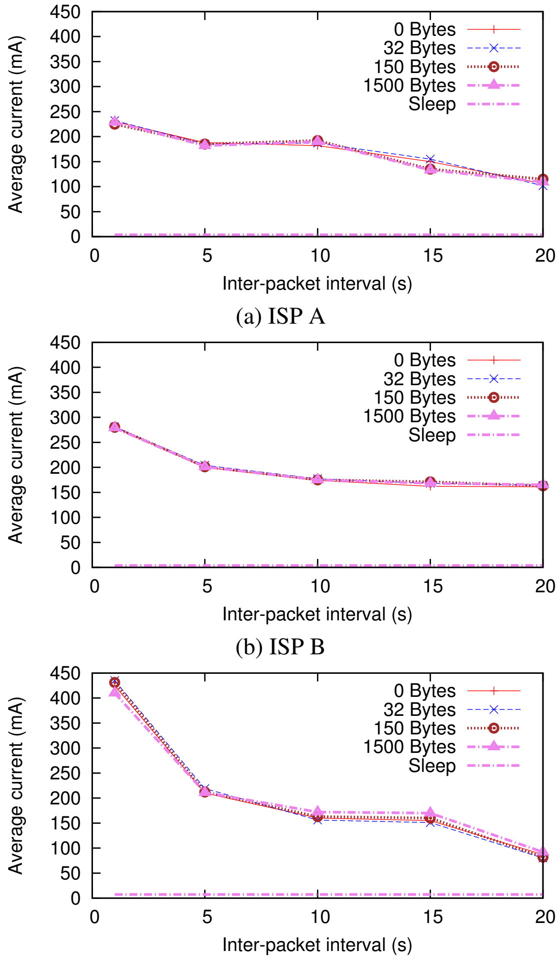
We see from our results that a malicious attacker can drain the battery of a phone by up to 24 times faster using a very low data rate UDP stream. Also, the battery usage display of the Android settings page will reflect that the OS is the main consumer of the power, which will potentially mislead the victim into thinking that the power drain was caused by the operating system, and makes this attack extremely hard to detect.

Finally, we investigated whether packet size has an impact on the sleep time and current consumption of the phones. We repeated the experiment using packet payloads of 32 bytes, 150 bytes and 1,500 bytes, and even with packets with no payload, and measured the average current consumption within a 1-min period and plot the results in Figure 6. While we cannot directly compare between the different ISPs, we can see that within the same ISP, packet size did not seem to have a significant impact. Thus, it is plausible for an attacker to launch an effective attack with UDP packets with no payload!

4. DEFENSE AGAINST ATTACKS

These attacks will not be possible if a mobile device uses a private IP address and Network Address Translation (NAT) to connect to the internet, as malicious packets from random sources will not be routed to the device. However, there are subscribers who want a public IP address, presumably to allow incoming connections to their devices and are willing to pay for such service being offered by the ISPs [2]. While an alternative is to use NAT traversal techniques to establish direct connections to the device, current NAT traversal techniques can be slow and are not 100% successful. Furthermore, NAT traversal requires the mobile device to rendezvous with a NAT traversal server. An attacker can therefore masquerade as the server and send packets to attack the mobile device.

The classic solution to such attacks is to employ a firewall to block malicious packets. However, implementing such a firewall on a mobile device will not help because by the time malicious traffic reaches the mobile device, harm would already have been done. The next natural solution would be to deploy the firewall within the ISP to filter malicious traffic before they can reach the mobile device. However, our results suggest that it would be difficult for an ISP to differentiate malicious data from legitimate traffic, and while we can try to whitelist legitimate traffic using some custom firewall rules, it might not be feasible for an ISP to provide such a level of service to all their subscribers. We believe that a more practical approach for an ISP would be to implement a simple IP-triggered firewall rule, where all incoming traffic from a host is blocked, unless the mobile device had previously sent a packet to the host. In fact, we observed such a firewall rule implemented in practice on one APN for ISP C.



(a) ISP A

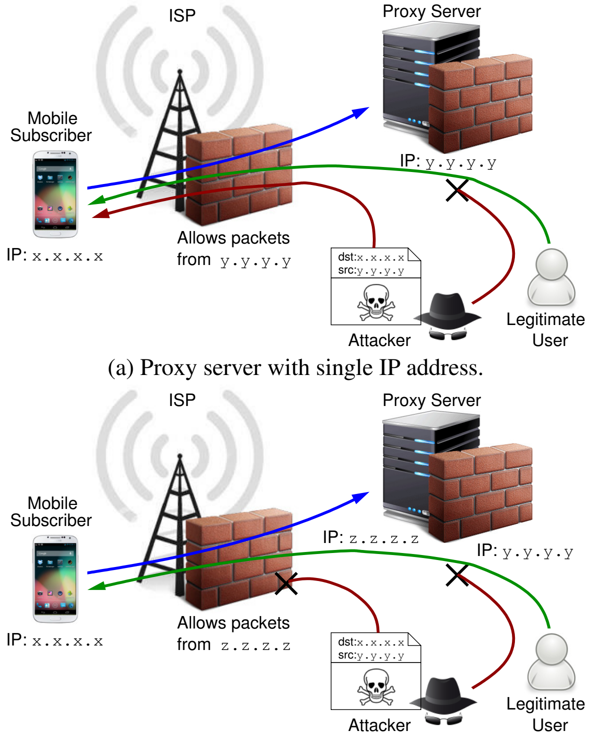
(b) ISP B

(c) ISP C

Figure 6: Effect of packet size and inter-packet interval on expected battery lifetime of a Galaxy S3 LTE.

The drawback of such a rule is that it would also prevent legitimate hosts from initiating connections to the mobile device, thereby undermining the provision of a public IP address in the first place. To address this issue, we can deploy a proxy server that redirects packets to the mobile device as illustrated in Figure 7. Once online, the mobile device will send a packet to the proxy server `y.y.y.y`, thereby creating a firewall rule to allow incoming packets from IP `y.y.y.y`. Legitimate users can send packets to the mobile device by forwarding packets via the proxy `y.y.y.y`, and a sophisticated firewall with custom rules can be implemented at this proxy to whitelist legitimate traffic. Alternatively, a legitimate sender can also request a "callback" from the mobile device (through the proxy), requesting the device to send a packet to the sender, thereby creating a rule in the ISP firewall that will allow direct incoming connections from the sender.

Unfortunately, like a NAT server, we will still have to explicitly



(a) Proxy server with single IP address.

(b) Proxy server with secret client-facing IP address.

Figure 7: Illustration of using a proxy with hidden access IP address to thwart mentioned attacks.

advertise the IP address of the proxy `y.y.y.y`. If an attacker is able to discover the IP address of the mobile device, he can masquerade as the proxy server, and send malicious packets through the firewall, as illustrated in Figure 7a. To address this potential vulnerability, we provide the proxy with a second IP address that is known only to the cellular device. This is illustrated in Figure 7b. Suppose the proxy uses a second IP `z.z.z.z` to connect to the mobile device, an attacker, who knows only of the advertised proxy address `y.y.y.y`, would not be able to masquerade as the proxy even if it knows the IP of the mobile device. To guard against spoofing attacks directed at the proxy, the proxy's firewall can perform deep packet inspection or authenticate the payload to verify it comes from legitimate hosts. Such multi-IP proxy servers can be implemented in a cloud service [18] and made available as a general service to cellular subscribers for an ISP.

5. CONCLUSION

While the availability of a public IP address in a cellular data network will allow new services to be deployed on mobile devices, it also introduces security vulnerabilities. We investigated three forms of IP-based attacks: (i) data quota drain, (ii) DoS flooding, and (iii) battery drain. While typical DoS flooding attacks can be easily detected, these attacks require such low data rates that they are difficult to differentiate from legitimate traffic without some form of deep packet inspection. As it is not feasible to expect ISPs to offer such inspection services to all subscribers, we propose that a simple proxy-based firewall with a secret IP address be used to thwart these attacks.

ACKNOWLEDGEMENT

This research was carried out at the SeSaMe Centre. It is supported by the Singapore NRF under its IRC@SG Funding Initiative and administered by the IDMPO.

6. REFERENCES

[1] 3GPP TS 36.331: Radio Resource Control (RRC) Protocol specification. `http://www.3gpp.org/lte`.

[2] Static IP addresses now available on 4G LTE, Sept. 2013. `http://wholesale.sprint.com/resources/global-wholesale-newsletter-stories/2013/09/03/static-ip-addresses-now-available-on-4g-lte`.

[3] R. Bassil, A. Chehab, I. Elhajj, and A. Kayssi. Signaling oriented denial of service on LTE networks. In *Proceedings of MobiWac '12*, 2012.

[4] M. Chandra, N. Kumar, R. Gupta, S. Kumar, V. Chaurasia, and V. Srivastav. Protection from paging and signaling attack in 3G CDMA networks. In *Proceedings of ETNCC '11*, 2011.

[5] Y. Go, D. F. Kune, S. Woo, K. Park, and Y. Kim. Towards accurate accounting of cellular data for TCP retransmission. In *Proceedings of HotMobile '13*, 2013.

[6] J. Huang, F. Qian, A. Gerber, Z. M. Mao, S. Sen, and O. Spatscheck. A close examination of performance and power characteristics of 4G LTE networks. In *Proceedings of MobiSys '12*, 2012.

[7] J. Huang, F. Qian, Y. Guo, Y. Zhou, Q. Xu, Z. M. Mao, S. Sen, and O. Spatscheck. An in-depth study of LTE: effect of network protocol and application behavior on performance. In *Proceedings of the ACM SIGCOMM '13*, 2013.

[8] R. P. Jover. Security attacks against the availability of LTE mobility networks: Overview and research directions. In *Proceedings of GWS - WPMC '13*, 2013.

[9] D. W. Kang, J. H. Oh, C. T. Im, W. S. Yi, and Y. J. Won. A practical attack on mobile data network using IP spoofing. *Appl. Math*, 2013.

[10] D. Mcqueen. The momentum behind LTE adoption [sGPP LTE]. *Communications Magazine, IEEE*, 2009.

[11] Monsoon Solution. Monsoon power monitor. `http://www.msoon.com/LabEquipment/PowerMonitor/`.

[12] Y. Park and T. Park. A survey of security threats on 4G networks. In *Globecom Workshops, 2007 IEEE*, 2007.

[13] K. Pelechrinis, M. Iliofotou, and S. Krishnamurthy. Denial of service attacks in wireless networks: The case of jammers. *Communications Surveys Tutorials, IEEE*, 2011.

[14] C. Peng, G.-h. Tu, C.-y. Li, and S. Lu. Can we pay for what we get in 3G data access? In *Proceedings of MobiCom '12*, 2012.

[15] I. Puustinen and J. Nurminen. The effect of unwanted internet traffic on cellular phone energy consumption. In *Proceedings of NTMS '11*, 2011.

[16] R. Racic, D. Ma, and H. Chen. Exploiting MMS vulnerabilities to stealthily exhaust mobile phone's battery. In *Proceedings of Securecomm and Workshops*, 2006.

[17] F. Ricciato, A. Coluccia, and A. Dalconzo. A review of DoS attack models for 3G cellular networks from a system-design perspective. *Computer Communications*, 2010.

[18] J. Sherry, S. Hasan, C. Scott, A. Krishnamurthy, S. Ratnasamy, and V. Sekar. Making middleboxes someone else's problem: network processing as a cloud service. In *Proceedings of the SIGCOMM '12*, 2012.

[19] P. Traynor, W. Enck, P. McDaniel, and T. La Porta. Mitigating attacks on open functionality in SMS-capable cellular networks. In *Proceedings of MobiCom '06*, 2006.

[20] Y. Xu, Z. Wang, W. K. Leong, and B. Leong. An end-to-end measurement study of modern cellular data networks. In *Proceedings of PAM '14*, 2014.