Demystifying the Presence of Cellular Network Attacks and Misbehaviors

Mitziu Echeverria [1] Omar Chowdhury [2]

[1]*The University of Iowa* [2]Stony Brook University

Abstract

Cellular networks nowadays are not only responsible for powering up worldwide communication systems, but also enable highly sensitive applications, such as the earthquake and tsunami warning system (ETWS), telemedicine, and autonomous vehicle communication. Due to its importance, one would expect this technology to be highly robust, secure, and reliable. However, even in the newest generations (i.e., 5G), this is not the case. Due to either implementation slipups, errors in the standard, or misconfigurations. These errors enable numerous destructive attacks, enabling malicious parties to track a victim's location, disrupt cellular services, and eavesdrop on calls, among other implications. To make matters worse, developing defenses against these types of attacks is a non-trivial task as it requires network operator cooperation. Most importantly it requires a significant amount of resources to be allocated by network operators and device manufacturers. To justify allocating resources to fix these issues, network operators need to quantify the misbehaviors and attacks being carried out in the wild. Unfortunately, there is no mechanism in place to perform this type of measurement.

Furthermore, there is no empirical evidence of cellular network attacks occurring in the wild, which digresses the community from focusing on developing defenses. Instead, the defense community has to rely vastly on anecdotal evidence to motivate their work, such as the presence of rogue base stations near government facilities. To provide the required empirical evidence and quantify the misbehaviors and attacks, we present HoneyLTE. HoneyLTE is the first tool that efficiently measures cellular network attacks and misbehaviors in the wild.

Background

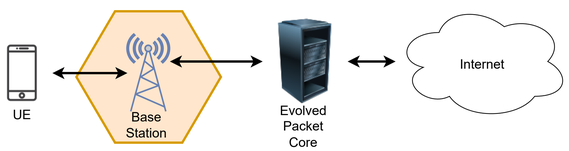

Figure 1. LTE Architecture

Architecture - The LTE network (Figure 1) consists of the following three components:

- **UE -** The User Equipment is a device that connects to the network, and contains credentials to perform mutual authentication between itself and the network.
- **eNodeB -** The base stations (eNodeBs) provide cellular connectivity, and serve as an intermediary between the UE and the network operator.
- **EPC -** The Evolved Packet Core provides a series of services for the UE and can generate challenges to aid in the mutual authentication process.

Layers

The LTE protocol stack consists of multiple protocols, the most important for our work are the following:

- **NAS** The Non-Access Stratum (NAS) protocol is the logical channel between the UE and the EPC. This protocol allows the UE and EPC to mutually authenticate each other.
- **RRC** The Radio-Resource Control (RRC) layer is the backbone to the NAS and other protocols. It is the main comunication between the UE and the servicing eNodeB.

Previous Attempts by the Community

Previous work has attempted to provide a similar system [1, 2, 4, 8]. Unfortunately, these previous attempts have various of the following limitations which severely impact their feasibility and widespread adoption:

- Requires dedicated and expensive equipment.
- Fail to detect benign misbehaviors.
- Fails to store and analyze previously seen sessions.

Requirements

Based on the limitations present in previous attempts, such system should have the following requirements:

- The system must be relatively cheap and not require special hardware
- The system needs to identify misbehaviors, and attacks, by both rogue and legitimate base stations or network operators.
- The system should be capable of identifying various types of attacks and misbehaviors.
- The systems to analyze the messages at runtime, and store for future analysis.

HoneyLTE

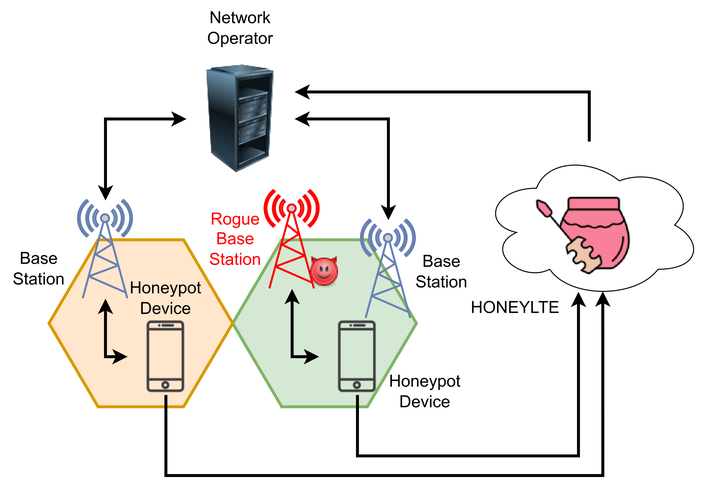

Figure 2. HoneyLTE Architecture

HoneyLTE (Figure 2 can be seen as a system of honeypot devices mimicking the behavior of legitimate cellular devices to collect, and measure cellular network attacks and misbehaviors. Each honeypot device can be either a COTS Android device or a hardware setup relying on Universal Software-defined Radio Peripheral devices (i.e., USRP boards). Each honeypot device runs a similar monitoring system to the one defined in, which is highly efficient and effective at detecting misbehaviors and network attacks. In addition, each honeypot device periodically uploads an efficient representation of its collected message traces to a central server through a Wi-Fi connection. HoneyLTE then uses the generated warnings, and the gathered data to alert the network operator of any issues encountered and provide relevant suggestions. For instance, if a honeypot device detects a cellular network attack, HoneyLTE will alert the network operator of the presence of the rogue base station. Similarly, if benign misbehavior is detected, the network operator is alerted, and HoneyLTE provides suggestions for correcting this error or misconfiguration. If a new attack or misbehavior is discovered, the honeypot devices can be updated over the air to detect it. Additionally, HoneyLTE can examine previous message traces to detect the presence of this attack in the past.

Deployment

HoneyLTE will be a global measurement platform, enabling volunteers to set up a honeypot device to communicate with a central HoneyLTE server. The data collected by this system will be publicly available. This will allow users to potentially identify new vulnerabilities and/or perform other types of measurements.

HoneyLTE Challenges

The design choice bring the following challenges:

- **Capturing Sensitive Information -** Unfortunately due to the nature of cellular network protocols, sensitive information for other users (non-volunteers) within the vicinity would be captured. For instance, the publicly available 'paging' messages potentially can contain permanent identifiers.
  Additionally, collecting cellular network information about a volunteer can reveal sensitive information such as their itinerary.
- **Anonymity for Volunteers -** Providing anonymity to the volunteers is of utmost importance to avoid personal risks. For instance,

HoneyLTE Solutions

To overcome the challenges we propose the following solutions:

- **Concealing Sensitive Information -** In order to conceal sensitive information such as the volunteers' itinerary or private sensitive identifiers, we propose to use differential privacy.
- **Providing Anonymity to the Volunteers -** In order to increase the anonymity we can provide to our volunteers, we propose to use VPN-based vantage points to connect to the central HoneyLTE server which is a well known solution in the censorship community [5].

Feasibility Study

To understand the feasibility of HoneyLTE, we deployed a small-scale version of it across multiple geographical regions within a 70-mile range using 4G LTE enabled COTS Android devices. We powered on the honeypot devices for approximately 24 hours. We repeated this experiment using different SIM cards for the four major US cellular network providers. No attacks were discovered, however, we quickly identified a highly destructive network operator misbehavior in three of the operators. The operators were sending the 'EMM Information' message in plaintext, even after setting up the security context, which is a known vulnerability by the community [6]. This enables an adversarial controlled eNodeB to modify the EMM payload, including the time, which modifies the UE's device. This is detrimental to time sensitive applications, such as certificate validity checks.

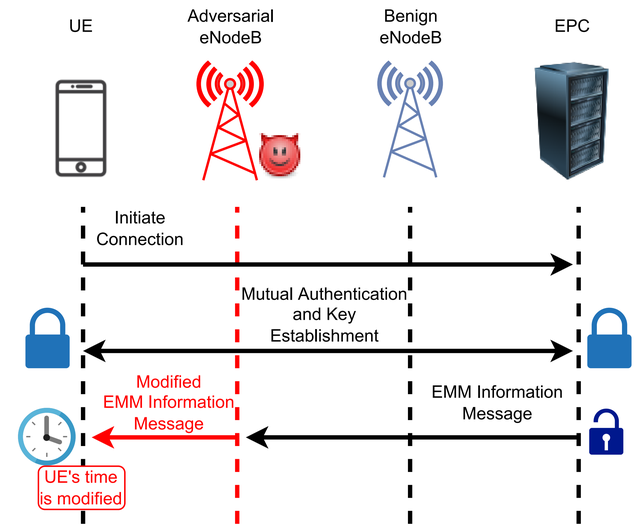

Figure 3. EMM Information Attack discovered [6], which three major U.S. network operators were susceptible to and were identified with HoneyLTE.

How Efficient is the Monitor?

The monitor used in HoneyLTE is borrowed from our previous work [2] which has the following efficiency measurements:

Parsing Speed - This monitor is highly efficient as it can parse $6.6 * 10^2$ packets per second, per layer. To put that in context, we observed a maximum of 2.76 messages per second in real world traces.

Power Consumption - To measure the power consumption, we used a monsoon meter. Our monitor showed to be highly efficient by only adding a $\sim$4mW overhead which is negligible.

Memory Overhead - We implemented our monitor on top of srsLTE [3], an open source software defined radio protocol stack to measure this. We used the **time** Linux command to obtain the maximum resident set size. The monitor added an overhead 159.25KB which is a 0.04% overhead.

References

[1] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. Imsi-catch me if you can: Imsi-catcher-catchers. In *Proceedings of the 30th annual computer security applications Conference*, pages 246–255, 2014.

[2] Mitziu Echeverria, Zeeshan Ahmed, Bincheng Wang, M Fareed Arif, Syed Rafiul Hussain, and Omar Chowdhury. Phoenix: Device-centric cellular network protocol monitoring using runtime verification. *arXiv preprint arXiv:2101.00328*, 2021.

[3] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D Sutton, Pablo Serrano, Cristina Cano, and Doug J Leith. srslte: An open-source platform for lte evolution and experimentation. In *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization*, pages 25–32, 2016.

[4] Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu. Fbs-radar: Uncovering fake base stations at scale in the wild. In *NDSS*, 2017.

[5] Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill. Iclab: A global, longitudinal internet censorship measurement platform. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 135–151. IEEE, 2020.

[6] Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, and Jean-Pierre Seifert. White rabbit in mobile: Effect of unsecured clock source in smartphones. In *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 13–21, 2016.

[7] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3):379–423, 1948.

[8] Zhou Zhuang, Xiaoyu Ji, Taimin Zhang, Juchuan Zhang, Wenyuan Xu, Zhenhua Li, and Yunhao Liu. Fbsleuth: Fake base station forensics via radio frequency fingerprinting. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 261–272, 2018.

mitziu-echeverria@uiowa.edu