# Exploiting Automation in LTE Mobile Networks

Altaf Shaik[*], Ravishankar Borgaonkar[§]

[*]Technische Universität Berlin and Kaitiaki Labs
Email: altaf329@sect.tu-berlin.de

[§]SINTEF Digital and Kaitiaki Labs
Email: rbbo@kth.se

## Abstract

The control and management of mobile networks is shifting from manual to automatic in order to boost performance and efficiency and reduce expenditures. Especially, base stations in today's 4G/LTE networks can automatically configure and operate themselves which is technically referred to as Self Organizing Networks (SON). Additionally, they can auto-tune themselves by learning from their surrounding base stations. This talk inspects the consequences of operating a rogue base station in an automated 4G/LTE network. We exploit the weaknesses we discovered in 4G/LTE mobile phones and SON protocols to inject malicious packets into the network. We demonstrate several attacks against the network and discuss mitigation from the mobile network operator's perspective.

## Introduction

Self-organizing networks (SON) were introduced in 4G/LTE networks to reduce the cost of network deployment and its maintenance. SON introduces automation into network management activities and reduce human intervention. Further this offers high quality of service and bandwidth to the users.

SON based networks mostly rely on the information gathered from mobile phones to perform self-configuration, self-optimization, and self-healing functions. However, we learnt in the past that mobile phones can be attacked over-the-air using rogue base stations. This white paper presents various DoS attacks that exploit the vulnerabilities identified in the LTE handover protocols and the SON architecture. The attacks can shut down network services for the certain period of time in a 2 $km^2$ area of a city. Furthermore, they can block network services to a selective set of UEs in a targeted area of 200 m to 2 km in radius and downgrade them to use less secure 2G and 3G network services.

Our key idea is to introduce a rogue base station that uses legitimate mobile devices as a covert channel to launch attacks against SON enabled LTE networks. To demonstrate the

impact of our attacks, we inject fake measurement reports and network configurations into the SON ecosystem. We have implemented our attacks and confirmed their effectiveness (following responsible disclosure policies) against commercial LTE network operators. The hardware required for our attacks is inexpensive and costs around 300 $. We reported our findings to the affected vendors, operators, and GSMA organization.

This paper is structured as follows: Chapter 1 describes the vulnerabilities identified in the SON system. Chapter 2 details about the attack setup and briefly explains the attacks on commercial networks and phones. Chapter 3 concludes this paper. This whitepaper assumes that the readers have sufficient knowledge about LTE and SON protocols. Detailed information about the attacks can be found in [1].

# 1. LTE and SON vulnerabilities

During our investigation we identified several vulnerabilities in the LTE handover and SON procedures and are as follows.

a. **Handover Vulnerability**. In a RRC connected state eNodeB receives measurement reports from the UE to track its mobility. Precisely, these reports contain network information that is used by the eNodeB to make handover decisions. Note that, measurement reports are received over an encrypted channel that is set up after a successful authentication procedure. However, this important network information is not verified by the network, in particular by the eNodeB, before making any handover decisions. This indicates that by operating a rogue eNodeB an adversary can exploit the handover procedure and inject false network information into the measurement reports.

b. **SON Design Weaknesses**. We discovered weaknesses in the SON design and decision making approach that cause DoS attacks against the serving network. In particular, we consider the following issues allow an adversary to create instabilities in the network operations when exploited with the aforementioned LTE protocol weakness.

   - The capability of an eNodeB to create neighbor relations through ANR process in an uncontrollable manner generates excess signaling load over the X2 interface. For example, a rogue eNodeB can induce unwanted signaling messages over the X2 interface and exhaust the related network resources.

   - When an eNodeB encounters a PCI collision, optimization process requires a restart of this eNodeB. Hence, the trigger for restart is merely controlled by a single parameter called PCI which is broadcasted in nature. Such a poor

decision making strategy of SON based on unreliable parameters, allows an adversary to control the operation of an eNodeB.

- Although measurement reports and RLF reports are securely transmitted to the eNodeB, the information contained in them is not verified by the network. Hence, a compromised UE can deliberately inject false information into these reports that is later used by the SON engine to perform optimizations which result in poor network performance.

In summary, it is evident from these weaknesses that SONs operate based on numerous parameters collected from LTE network operation such as measurement reports, RLF reports and PCI. These parameters are leveraged to perform network optimizations. Significantly, SON lacks a mechanism to verify the authenticity of these parameters and entirely trusts the LTE security mechanisms for the correctness of these parameters.

# 2. Experimental setup and attacks

We describe the attacks briefly followed by the experimental setup required to perform. It consists of several hardware and software components as shown in figure 1.

a. **Hardware**. Hardware testbed consists of a UDOO X86 embedded PC and a LimeSDR [2]. UDOO is based on Intel Atom processor and connected to LimeSDR via USB 3 port. The LimeSDR is a software-defined radio module costing 150 $ and is controlled by a PC-based software to transmit and receive signals over-the-air. The total cost of hardware used for our attacks is about 300 $. Additionally we used some of the latest LTE smartphones available in the market supporting for test purposes. We also used SON capable eNodeBs to test our attacks. For certain security reasons we do not specify the eNodeB's we tested.

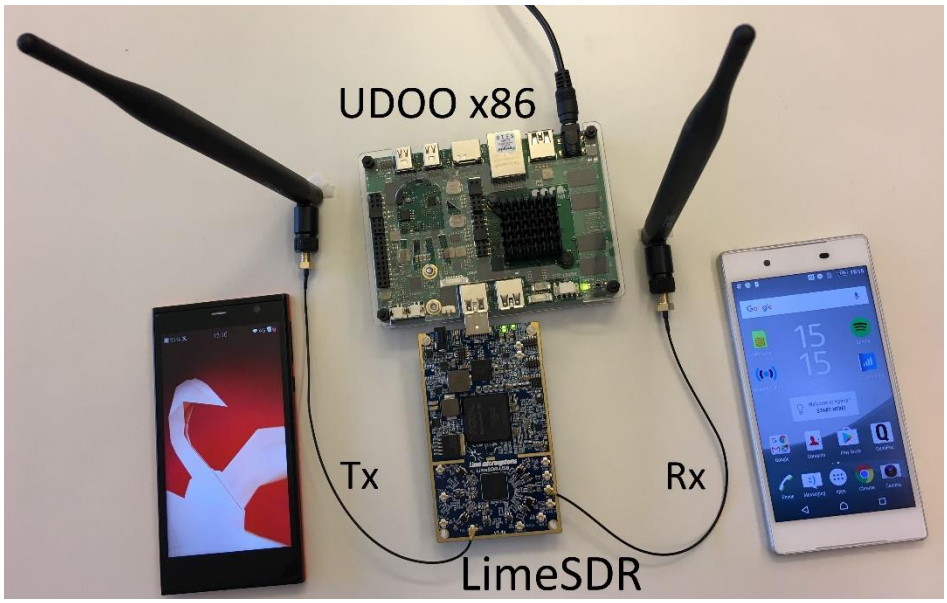

Figure 1: Experimental setup

b. **Software**. For passive mode, we use modified *cell_search* application from the open source project srsLTE [3]. It resides on the PC and controls the LimeSDR to passively sniff LTE broadcast information. By default, the application can only detect the PCI of the strongest cell on a given EARFCN. We have modified the application to detect the PCI from all available cells from all operators present in a certain area and further decode their respective SIB type 1 information.

   For active mode, we use *pdsch_enodeb* application from srsLTE which uses LimeSDR to operate a rogue eNodeB. The passively collected SIB information is used to configure the eNodeB and perform active attacks. To evaluate and verify our attacks, we also built a custom tool called *cell_logger* which runs on the host PC to acquire information directly from the UE's baseband processor and decode the RRC messages exchanged with eNodeB.

c. **Ethical Considerations**. Our research reveals vulnerabilities in the LTE and SON specifications which are already deployed into LTE phones and networks worldwide. Hence, by following responsible disclosure policies, we reported our findings to the GSMA body, two vendors and two leading network operators in Europe. The vulnerabilities are acknowledged by the involved parties. We performed our active attacks in a Faraday cage and against our test devices to avoid disturbance to other nearby UEs. For passive attacks in the real network, we took the permission from the operator and cared not to interrupt normal network services in the testing zone.

We perform three types of attacks to demonstrate the DoS attacks on the subscribers and the network.

a. **X2 signaling load** – Heavy load is generated on the X2 interface by operating a rogue eNodeB with several legitimate cell IDs. Legitimate eNodeBs make attempts to add the new eNodeBs into their network by sending messages over X2 interface.

b. **Cell outage** – By impersonating a PCI of a cell it is possible to restart a legitimate eNodeB. This restart can take up to 7-8 minutes depending on the configuration of the device. During this period there a cell outage is noticed by the UEs and they connect to other LTE eNodeBs or switch to 2G/3G networks.

c. **Handover Hijacking** – The LTE handover procedure is hijacked by impersonating a neighbor cell PCI. The handover procedure is failed since the rogue eNodeB does not possess the security keys required to handle an active call session. Meanwhile the UE creates a RLF report and forwards it to the real network indicating the handover failures. IN particular the report contain the PCI of the eNodeB that caused the RLF. In this case it is the PCI of the legitimate eNodeB since its being impersonated. When similar reports are accumulated in large numbers the SON considers the eNodeB as malfunctioned and initiates a repair and restore procedure. In certain cases, the eNodeB is disconnected from the live network.

All the attacks mentioned above are highly feasible and can be easily performed on LTE smartphones and networks since the vulnerabilities are majorly present in the LTE and SON specifications rather than their implementations. As a result, all the LTE phones conforming to the specifications are affected by our attacks. One can argue that it is easy to perform DoS attacks with a mobile network jammer. But unlike jamming, our DoS attacks are controlled and can be targeted to a particular operator(s) or subscriber(s). Moreover, jamming can only disrupt communications during their operation period but our attacks can slander legitimate eNodeBs within 2 minutes. Further, our attacks are persistent even after shutting down our rogue eNodeB because SON require periodical statistics to adjust network settings.

# 3. Conclusion

In this paper, we uncovered vulnerabilities in LTE handover protocols that can deny calls/data services to subscribers and demonstrated it with an off-the-shelf 300 $ rogue eNodeB. We clearly highlighted that SON operates based on the inputs from several vulnerable information sources standardized in LTE protocols. With the support of several SON manuals and expertise from network operators, we derive that operating a rogue eNodeB in a SON based LTE network can cause eNodeB malfunctions, service interruptions and instabilities in the network operation. This can adversely affect the revenue and the reputation of the operator. A detailed analysis of the attacks and mitigations and covered in [1].

# References

[1] https://dl.acm.org/citation.cfm?id=3212497

[2] Lime Microsystems. 2016. LimeSDR. https://www.crowdsupply.com/lime-micro/limesdr

[3] https://github.com/srsLTE/srsLTE