CS 6480: Paper reading summary
HA 21.a

Jose Monterroso

School of Computing, University of Utah

November 17, 2020

1 Hiding in plain signal: physical signal overshadowing attack on LTE

Paper discussed in this summary is "Hiding in plain signal: physical signal overshadowing attack on LTE' [4].

1.1 First pass information

1. *Category:* This paper is an analysis of an existing system as well as a description of a research prototype. The existing system that is being analyzed is 4G LTE security, while the research prototype being described is the signal overshadowing attack.

2. *Context:* The technical area of this paper relates to 4G LTE mobile networking security. Our paper on 5G [1] is the closes we have gotten to a paper discussing the 4G LTE network design. We have also seen papers in the past that discuss a different attack vector on 4G LTE named aLTEr [2].

3. *Assumptions:* The authors assume that their paper is the first to present a signal injection attack. I believe this is accurate as they should have done research to verify no others have published such works, furthermore, I haven't heard or seen a paper that does such an attack.

4. *Contributions:* The papers main contributions are as followed. First, they produce the first signal overshadowing attack on LTE. Secondly, they demonstrate the practicality and stealthiness of the SigOver attack via a real world experiment. Thirdly, they present novel attack scenarios and analyze their implications in experiments. Lastly, they investigate prevention and detection strategies against the SigOver attack.

5. *Clarity:* Although this paper's length is longer than usually it does appear to be well written.

1.2 Second pass information

- *Summary:* The authors of this paper present the world's first signal injection attack that exploits the fundamental weaknesses of broadcast message in LTE and modifies a transmitted signal over the air. The first section after the introduction provides us with the needed background information of the LTE network architecture and the essential procedures of radio connection establishment, mobility management, and security setup between a device and an LTE network. The next section describes the attack model, the description of the SigOver attack and a comparison with with a fake base station. The authors mention that an adversary can inject malicious messages into the victim UE(s) by overwriting the legitimate messages. This can be done by

carefully crafting a message that overlaps a legitimate message with respect to time and frequency. In principle the SigOver attack leverages the capture effect, where the stronger signal is decoded when multiple simultaneous wireless signals collide in the air. Next, the Authors perform a SigOver attack in the wild and analyze the reliability of the attack. Their setting is within a university basement and office. They used an LG G7 ThinQ smartphone with SnapDragon845 which was the latest Qualcomm LTE chipset at the time of this paper's release. We find that the SigOver attack demonstrated a 98 percent success rate when compared with the 80 percent success rate of the attack achieved by the fake base station. Next, the authors present various attack scenarios and implications for each. Such attacks exploit paging and SIB. In section 6 the authors discuss two possible defense strategies against the SigOver attack. Such solutions revolve around digitally signing all broadcast signals by using the public key infrastructure. Furthermore, you can detect the SigOver attack because it leverages the changing nature of the physical signal during the processing of the overshadowing signal. Lastly, the authors discuss related works before arriving to a conclusion.

1.3 Third pass information

- *Strengths:* I really enjoyed the introduction because it presented me with all the high level overview information that you would need from the paper. I also thought the background section gave a good overview of how LTE manages the UEs, eNBs, and EPCs of the networks. I like how they had potential competitions and explained why the SigOver attack is better, it really brings up the attacks value. I really liked the use cases section which they called the attack scenarios and implications section because it brought up the valid idea that their attack method is valid and can be used differently. I though that that way they described the potential solution while also included the deployment and technical challenges made it seem like these guys really though everything out pretty well.

- *Weaknesses:* Some of the little sub-sections within the background sections were a bit confusing and I wish they would have been more specific. They mention they implement their attack based on the pdsch enodeb and add a custom-built received function for time synchronization I wonder if this can be generalized to other eNbs but they don't mention any others. All in all, I thought that this was a good paper that didn't have many weaknesses.

- *Questions:* I'm still a bit confused about the frequency synchronization aspect especially when they mention the oscillator and how they compensate for it.

- *Interesting citations:* I always seem to find security papers really interesting as the majority of the things that people write about are loopholes or small very detailed points of access. I like reading about the creativity and ingenuity people have to go through to find these security flaws. I find that this paper was full of security references, however the spoofing attack [3] caught my interest as they appear to investigate the requirements for a perfect spoofing attack.

- *Possible improvements:* This paper was a bit long for my taste but I realize that the length was generated due to the background and the specific and detailed nature of the author's writing.

- *Future work:* The authors mention checking if SigOver is possible for 5G. I would also be curious if this method can apply to all base stations in the real world. I'd be interested in seeing if overshadowing a signal can be applied to any other forms of communication theory.

References

[1] GROUP COMPANIES, N. Making 5g a reality. *NEC White Paper* (Feb. 2018).

[2] Rupperecht, D., Kohls, K., Holz, T., and Popper, C. Breaking lte on layer two. *2019 IEEE Symposium on Security and Privacy (SP)* (May 2019).

[3] Tippenhaur, N., Popper, C., Rasmussen, K., and Capkun, S. On the requirments for successful gps spoofing attacks. *CCS '11: Proceedings of the 18th ACM conference on Computer and communications security* (Oct. 2011).

[4] Yang, H., Sangwook, B., Son, M., Kim, H., Kim, S., and Kim, Y. Hiding in plain signal: Physical signal overshadowing attack on lte. *SEC '19: Proceedings of the 28th USENIX Conference on Security Symposium* (Aug. 2019).