Title: Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE

Introduction: Long-Term Evolution (LTE) technology utilizes broadcast signals to transmit essential information from a cellular network to user devices. The base station transmits information in synchronized time to the User Equipment. Despite its various practical applications, the broadcast signal is not security protected at all. In LTE, communication between a UE and network is secured only after successful authentication and security handshake procedures. Some studies have shown that employing a fake base station that attracts UEs to be connected to itself by transmitting a signal stronger than legitimate base station.

Overshadowing LTE Broadcast Message: Our Experiment setup assumes an active adversary with minimum privilege. The adversary does not know the LTE key of the victim UE. The adversary is able to eavesdrop on the downlink broadcast messages transmitted from the legitimate LTE cell to the victim UE. Under the above assumptions, we show that an active adversary can inject malicious messages into the victim UE(s) by overwriting the legitimate messages. This is achieved 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, wherein the stronger signal is decoded when multiple simultaneous wireless signals collide in the air. For an accurate overshadowing time and frequency should be synchronized.

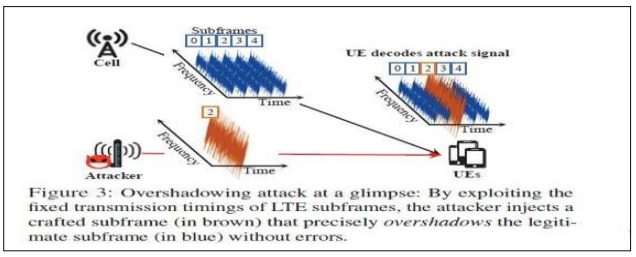

Figure 3: Overshadowing attack at a glimpse: By exploiting the fixed transmission timings of LTE subframes, the attacker injects a crafted subframe (in brown) that precisely *overshadows* the legitimate subframe (in blue) without errors.

Experimental Setup: We add a custom-built receive function for time synchronization with the legitimate cell. An USRP X310 equipped with a UBX daughter board and GPSDO was employed, which was connected to an Intel Core i5-3570 machine with an Ubuntu 14.04. To overshadow the signal from a legitimate eNB, the USRP was augmented with ZVE-2W-272 amplifier. UE's specification was LG G7 ThinQ smartphone with SnapDragon845, which is the latest Qualcomm LTE chipset. Two scenarios were considered such as LOS and NLOS.

Table 3: Success rate of `SigOver` attack in various conditions.

	LOS	NLOS
RRC Connected	97%	98%
RRC Idle	100%	98%

In the RRC Idle state, we inject a paging message at the exact paging occasion (e.g., Subframe 9) and pagingframe of the victim UE, this channel estimation is carried out solely on the injected signal. However, in the RRC Connected state, repeated injection is required to overcome the influence of the legitimate signals. To achieve this, we inject a paging message at the exact paging frame of the victim UE. As shown in Table,the SigOver attack maintained a success rate greater than 97% in different RRC states and the LOS and NLOS setups.

Defending Against SigOver Attack: As the SigOver attack exploits the lack of integrity protection in broadcast messages, one natural defense against SigOver attack is to employ integrity protection in the messages using a digital signature scheme. For this, each base station needs to have a certificate issued by its operator and a UE needs to be provisioned with a root certificate. Signing every single broadcast message may incur a substantial computational overhead at the base station, considering the low periodicity of essential broadcast messages such as MIB (40ms) and SIB1/2 (80ms). Furthermore, message size increases due to the signature and certificate broadcasting. ID based signature scheme has substantially low-key management overhead and eliminates the certificate broadcast and verification overhead.

Conclusion: we present the SigOver attack, which outlines the first realization of a signal overshadowing attack on the LTE network. We implement the SigOver attack using a low-cost SDR and open source LTE library, while resolving the challenges in satisfying the stringent transmission requirements and crafting a malicious frame. The key features of the SigOver attack are stealthiness, power efficiency and sustainability. The evaluation revealed that the SigOver attack achieves a 98% success rate with low power cost.

Name: Radhika Bailurkar, UID:
2019430003 Name: Sushama Garud,
UID:
2019430006

Title: Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE

Proceedings: 28th USENIX Security Symposium,August 14–16, 2019 • Santa Clara, CA, USA