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

Summary:

This paper presents a signal injection attack that exploits the major weakness of broadcast messages in LTE that lack integrity protection as these messages aren’t protected from being modified using any cryptographic primitives. The signal overshadowing attack SigOver performed, modifies the transmitted signal over the air. It results in a 98% success rate which is better than the 80% success rate observed in the fake base station attacks. It presents 5 new attack scenarios and implications. The paper also proposes two potential countermeasures to defending against the SigOver, which leveraged the digital signature and channel diversity.

Strengths:

1. Unlike the Fake base station attacks which are noticeable via high signal power and/or DoS, SigOver attack is stealthy and scalable as it leverages the fact that UE decodes only the stronger signal when receiving multiple signals. This happens such that the attack signal is only overshadowing targeted signal without interfering with other signal transmissions between the UE. The SigOver is also able to scale by simultaneously affecting multiple UEs nearby.
2. It is mentioned that the subframes are decoded independently which doesn’t affect legitimate frames but at the same time progresses the attack by making the UE display abnormal behavior frame by frame.
3. The new attack’s threat scope is validated by presenting 5 more scenarios I.e. signaling storm, DoS against UE’s, network downgrade and UE location tracking.

Weakness:

1. The new threat scope mentioned with given attacks was tested just in LOS conditions. This leaves the effectiveness of these attacks questionable in real world scenario where it might not always be possible for the attacker to be close to the UsE. What differences would NLOS entail isn’t discussed.
2. The DoS attack by overshadowing paging with IMSI has a weak point - it relies on the ambiguity of the 3GPP standards in defining the mechanism for handling paging in the RRC Connected state. This means that not all devices may respond to the attack in the same way, and some may not respond at all. Additionally, the attack can be sustained only by repeated injection of the paging message, which could potentially be detected and blocked by the network.
3. The network downgrade attack has a weak point as well - it only downgrades the victim UE to the 3G network, which is slower than the LTE network. However, it does not provide the attacker with any access to the victim's data or network traffic. It is also stated that the attack may not work on some smartphones that do not respond to the paging message in the RRC Connected state, making them immune to the attack.