Paper: LTRACK: Stealthy Tracking of Mobile Phones in LTE

Summary:

The paper introduces a new tracking attack called LTRACK that extracts a user's device location and permanent identifier (IMSI) in an LTE network through a passive localization technique. LTRACK uses a new uplink/downlink sniffer that records the arrival time of LTE messages and calculates locations based on Timing Advance Commands. The technique is the first to implement passive localization in LTE through software-defined radio. LTRACK overcomes the challenge of linking location traces to a device's pseudonymous temporary identifier by introducing a new type of IMSI Catcher called IMSI Extractor that extracts a device's IMSI and binds it to its current TMSI. The IMSI Extractor is the stealthiest IMSI Catcher to date, relying on surgical message overshadowing instead of fake base stations and uplink/downlink sniffing to bind the collected traces to an IMSI, making it hard to detect. The paper also presents LTEprobe, the first white-box uplink, and downlink LTE sniffer, which records both protocol-level information and physical layer timings of messages. LTRACK is evaluated through experiments and successfully tested against a set of modern smartphones connected to an LTE testbed.

Strengths:

1. The IMSI extractor introduced achieve message injection by using overshadowing and uplink/downlink sniffing and hence makes it way harder for the existing IMSI catcher detection techniques to detect. This method is not just suggested but also tested on actual smartphones and industry grade eNodeB which makes the contribution promising.
2. The LTEprobe proposed, is also implemented in the attack which has two components, a first actual uplink sniffer and a downlink sniffer. The sniffing for both is made possible by leveraging unencrypted DCI messages. This highlights the feasibility of localization attacks.
3. The proposed attack works in case of misalignment as well. The errors caused can be corrected using time correction and uplink messages are decoded correctly.

Weaknesses:

1. The complexity revolving around calculating the 2 ellipses for determining the location of UE involves multiple probes haven’t been discussed. The time taken by the LTEprobe to make this calculation isn’t mentioned. This means that the cost of the attack might increase in the real world. The relation between the attack complexity and cost hasn’t been evaluated to determine how feasible it is to carry out.
2. It is mentioned that a database is maintained with various phones and their corresponding hardware errors as well as TMSI-IMSI pair. It hasn’t been explained what sort of database is being used, how long the processing for frequent hits on the database takes and what are its implications on the Ltrack attack. The paper considers 17 models which wouldn’t make a huge difference in the time complexity of this choice but when considering active usage in a congested city with more than 17 types of UE, this detail could affect the performance of the attack drastically.
3. The LTRACK attack is only applicable to LTE networks, and the paper does not discuss the vulnerabilities or countermeasures for other mobile network technologies widely used today.
4. The experiment is conducted in a controlled indoor environment with only one eNodeB and LTEPROBE, which may not accurately represent real-world scenarios with multiple base stations and potential interference.