Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE

Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim, *KAIST*

https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon

This paper is included in the Proceedings of the 28th USENIX Security Symposium.

August 14–16, 2019 • Santa Clara, CA, USA

978-1-939133-06-9

Open access to the Proceedings of the 28th USENIX Security Symposium is sponsored by USENIX.

Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE

Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim
Korea Advanced Institute of Science and Technology (KAIST)
{omnibusor, hoops, mcson, hongilk, songmin, yongdaek}@kaist.ac.kr

Abstract

Long-Term Evolution (LTE) communication is based on an open medium; thus, a legitimate signal can potentially be counterfeited by a malicious signal. Although most LTE signaling messages are protected from modification using cryptographic primitives, broadcast messages in LTE have never been integrity protected. In this paper, for the first time, we present a signal injection attack that exploits the fundamental weaknesses of broadcast messages in LTE and modifies a transmitted signal over the air. This attack, which is referred to as signal overshadowing (named `SigOver`) has several advantages and differences when compared with existing attacks using a fake base station. For example, with a 3 dB power difference from a legitimate signal, the `SigOver` attack demonstrated a 98% success rate when compared with the 80% success rate of attacks achieved using a fake base station, even with a 35 dB power difference. Given that the `SigOver` attack is a novel primitive attack, it yields five new attack scenarios and implications. Finally, a discussion on two potential countermeasures leaves practical and robust defense mechanism as a future work.

1 Introduction

Long-Term Evolution (LTE) technology utilizes broadcast signals to transmit essential information from a cellular network to user devices. At minimum, the information broadcasted by an LTE base station, which is referred to as an evolved NodeB (eNB), includes the synchronization information and radio resource configurations required for a User Equipment (UE) to access the cellular network. Based on the received broadcast signals, a UE registers with the network by performing an Authentication and Key Agreement (AKA) procedure. After registration, the UE monitors the broadcast signals for various objectives. For example, when the UE does not have a connection with an eNB due to its inactivity, it needs to listen to paging messages regularly to check the messages transmitted to it.Even when the UE has an active connection with an eNB, the UE keeps listening broadcast signals to determine potential changes in system-wide radio configurations which are required to be updated, and to identify the arrival of messages intended to multiple UEs.

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, namely Non-Access Stratum (NAS) and Access Stratum (AS) security mode procedures for the protection of *unicast* messages. Unprotected broadcast signals may be unavoidable to a certain extent in wireless communication; however, they subject the system and UEs to various vulnerabilities that can be exploited.

Previous studies [21, 26, 36, 39, 40] reported on several attacks that exploit *unprotected* broadcast signals. In general, such attacks employ a fake base station (FBS) that attracts UEs to be connected to itself by transmitting a signal stronger than those of the legitimate base stations. The attacks mainly exploit the paging messages, resulting in undesirable effects on the UE, e.g., out-of-service and battery drains. Notably, such FBS-based attacks entail noticeable characteristics (e.g., high signal power) and/or outcomes (e.g., service denial) that enable the victim UEs to identify the presence of the FBS (see Section 3.5 for details).

In this paper, we propose a new approach referred to as the `SigOver` attack, which injects a manipulated broadcast signal into UEs without employing an FBS. The `SigOver` attack overwrites a portion of the legitimate signal using the manipulated attack signal. The `SigOver` attack is based on the fact that the UE decodes a stronger signal when it concurrently receives multiple overlapping signals, which is referred to as the *capture effect* [51]. The main technical component of the attack is to synchronize the timing of the attack signal with that of the targeted legitimate signal so that the UE only decodes the attack signal (see Section 3). This attack is both stealthy and far-reaching. It is stealthy because the attack signal, which is transmitted at a significantly low power level, only overshadows the targeted signal; whereas the other signals/messages between the victim UEs and network remain intact. It is far-

reaching because the attack signal can simultaneously affect a large number of nearby UEs with low signaling and a low computational cost. Note that the SigOver attack does not require any active communication with the UEs, and it does not relay messages between UEs and an eNB.

The *SigOver attack* is the first practical realization of *the signal overshadowing attack on the LTE broadcast signals* using a low-cost Software Defined Radio (SDR) platform and open source LTE library [43]. The SigOver attack was made practical by addressing the following challenge: *time and frequency synchronization*. To overshadow the legitimate signal using the malicious signal, the SigOver attack needs to be tightly time-synchronized with the eNB's downlink physical channel to which the victim UE is listening. To achieve time synchronization, we leverage the synchronization signals of the eNB that are transmitted periodically with a fixed time gap. For accurate frequency synchronization, we employ a Global Positioning System (GPS) disciplined oscillator.

The feasibility of the SigOver attack was verified by testing it against 10 smartphones (listed in Section 5) connected to an operational network[1]. For the experiments, we introduced five new attack scenarios, which included the signaling storm, denial of service (DoS) against UEs, network downgrade, and UE location tracking (Section 5). The experimental results reveal that the SigOver attack overshadows the target signal and causes the victim device to decode it with a 98% success rate and a power difference of only 3 dB from a legitimate signal. On the other hand, attacks utilizing an FBS have only 80% success rate even with a 35 dB power difference. This implies that the SigOver attack is significantly more efficient than the attacks using the FBS.

Finally, two potential countermeasures against the SigOver attack are discussed in Section 6: (1) digital signature based solution and (2) channel estimation based detection. Moreover, a practical and robust solution to the SigOver attack is left as a future work.

Our contribution are summarized as follows:

- **First signal overshadowing attack on LTE:** To the best of our knowledge, the SigOver attack is the first realization of a signal overshadowing attack on LTE broadcast signals.
- **Implementation and evaluation:** We demonstrate the practicality and stealthiness of the SigOver attack via extensive real world experiments with high attack success rate.
- **Novel attack scenarios and implications:** We present novel attack scenarios and analyze their implications in detail based on the experiments.
- **Countermeasures:** We investigate prevention and detection strategies against the SigOver attack, e.g., the digitally signing on broadcast signals for prevention, and leveraging the changing nature of the physical signal for detection.

[1] All the experiments were conducted based on the permission of the operators.

2 Background

In this section, we present a brief description 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. (See the table in Appendix B for the acronyms used in this paper.)

2.1 LTE Network Architecture

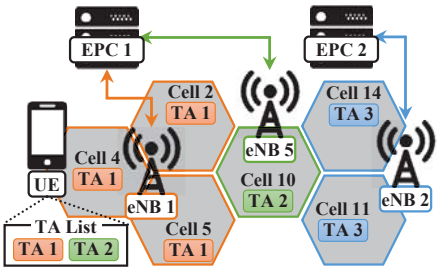


Figure 1: LTE network architecture

An LTE network consists of a UE, eNB, and Evolved Packet Core (EPC) components as illustrated in Figure 1.

A **UE** is an end device that provides various LTE services (i.e., voice and data services) to a subscribed user. It includes a smart card referred to as the Universal Subscriber Identity Module (USIM), which stores a permanent identity (International Mobile Subscriber Identity, IMSI) or a temporary identity (Globally Unique Temporary Identity, GUTI) for user identification, and a cryptographic key for encryption and integrity protection.

An **eNB** is an LTE base station, which provides a wireless connections for UEs to receive services enabled at the LTE network. A single eNB covers multiple sites (referred to as cells in LTE), which are identified by a Physical layer Cell Identity (PCI).

An **EPC network** is responsible for control functions such as authentication, mobility and session management, and user plane services. For mobility management, a Mobility Management Entity (MME) in the EPC network manages a set of Tracking Areas (TAs), each of which contains several eNBs.

2.2 LTE Physical Layer Initial Access

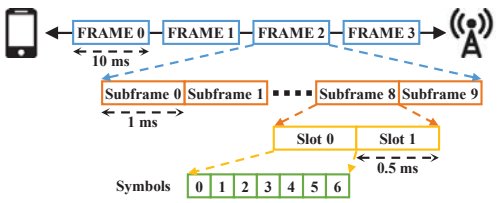


Figure 2: LTE frame structure type 1 [2]

LTE frame. The UE and eNB communicate with each other based on the radio frame structure, as shown in Figure 2[2].

[2] The LTE-Frequency Division Duplex (FDD) mode was employed in this study, as used by the majority of operators in the world [18].

Each frame has a duration of 10ms and comprises 10 subframes, each of which has a duration of 1ms. A single subframe is further divided into two slots of equal duration and each slot comprises seven Orthogonal Frequency Division Multiplexing (OFDM) symbols.

Downlink Scheduling. In LTE, radio resources are allocated in the unit of the Physical Resource Block (PRB) [2] that contains 12 subcarriers (each with a bandwidth of 15 KHz) and consumes one slot in time (0.5ms). The number of available PRBs in a frequency band is determined by the system bandwidth. Depending on the size of the data, an eNB allocates PRBs within a subframe (1ms), which is the smallest scheduling time interval.

Channel estimation. When a signal travels through a wireless channel, the signal gets distorted due to several factors, e.g., attenuation, phase-shift, and noise. To accommodate those factors, wireless devices estimate the channel using the following equation: $Y(k) = H(k)X(k)$, where $Y(k)$, $H(k)$ and $X(k)$ represent a signal received by a UE, the channel coefficient, and the signal transmitted by an eNB, respectively. In LTE, a UE performs channel estimation based on the Reference Signal (RS) transmitted by the eNB. The UE calculates $H(k)$ from $H(k) = \frac{Y(k)}{X(k)}$ as it already knows $X(k)$ and $Y(k)$ value of RS. To minimize the effects of noise in the channel estimation, $H(k)$ of RS is averaged using an averaging window.

Cell search. When a UE is turned on, it has to find a suitable cell to establish radio connections. To this end, it first attempts to measure the Received Signal Strength Indication (RSSI) of the candidate frequency channels. The UE selects the channel with the highest RSSI based on the measurement. Thereafter, the UE obtains time synchronization on a subframe basis and the PCI of the cell by listening to a Primary Synchronization Signal (PSS) and a Secondary Synchronization Signal (SSS). The UE then decodes the Master Information Block (MIB) to acquire the System Frame Number (SFN) and other physical channels.

System information acquisition. After completing the cell search procedure, the UE decodes a Physical Control Format Indicator CHannel (PCFICH) and a Physical Downlink Control CHannel (PDCCH) to decode downlink data. The UE knows the number of OFDM symbols used to carry the PDCCH at each subframe through the PCFICH. The UE then decodes the PDCCH that contain the information on the resource blocks that the data and the demodulation scheme required by the UE. After decoding the two channels, the UE decodes the other system information broadcasted through a Physical Downlink Shared CHannel (PDSCH). There are 22 System Information Blocks (SIBs), each of which contains different cell-related system information [3]. Among them, SIB1 and SIB2 are essential for a UE to connect to a cell. The availability of other SIBs is indicated in SIB1.

Random access. A UE performs a Random Access CHannel (RACH) procedure to establish a radio connection with the eNB. To this end, the UE randomly chooses a Random Access (RA) preamble sequence and transmits it to the eNB. Unless the same preamble sequence is simultaneously transmitted from a different UE, the UE successfully completes the RA procedure.

2.3 Mobility Management

Radio Resource Control (RRC). When all the steps above have been completed, the UE carries out a connection establishment procedure with the eNB (called RRC connection establishment procedure). Upon the completion of the procedure, the UE enters the *RRC Connected* state in which it can communicate with the eNB. When there are no incoming and outgoing data for a certain time period, the radio connection between the UE and eNB is released, and the UE enters the *RRC Idle* state, to reduce battery consumption.

Non-Access Stratum (NAS). NAS is a network layer protocol between the UE and MME for mobility and session management. To register with the LTE network, the UE carries out an ATTACH procedure. After the UE is successfully registered with the LTE network, the MME knows the TA to which the UE belongs and provides the UE of a list of TA identifiers (TAIs). This TAI list is used by the UE to report its location to the MME.

Idle state behavior. In the *RRC Idle* state, the UE periodically wakes up to read paging messages and SIB 1. When there is incoming message to the UE, the MME that tracks the UE sends a paging to all eNBs in the entire TAs assigned to the UE, and those eNBs broadcast a paging message to inform the UE of the arrival message. The paging message contains either the temporary or permanent identity of the UE. If the UE receives the paging message, it sends a `RRC connection request` and a `Service request` message to the LTE network. Paging is also used to notify the system information change or provide emergency alerts such as the Earthquake and Tsunami Warning System (ETWS) and Commercial Mobile Alert System (CMAS). The UE also reads the SIB1 to identify the current TA. If the UE enters into a new TA that is not in the TAI list, the UE sends a `Tracking Area Update (TAU) request` to the MME to report its location. In addition, the UE periodically measures the power and quality of the serving cell and neighboring cells by calculating the Reference Signal Received Power (RSRP) and Reference Signal Received Quality (RSRQ). When the RSRP of a neighboring cell is higher than that of the serving cell by a certain threshold, the UE selects new cell and camps on it (i.e., cell re-selection).

2.4 Establishing Security Context

When a UE establishes a wireless connection with an eNB, it registers with the LTE network to achieve a full connection with the network (this behavior is called ATTACH) by providing its permanent identity, IMSI. Then, the MME and the UE mutually authenticate each other and carry out a key

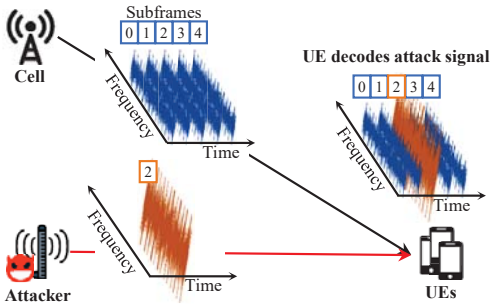


Figure 3: Overshadowing attack at a glimpse: By exploiting the fixed transmission timings of LTE subframes, the attacker injects a crafted subframe (in brown) that precisely *overshadows* the legitimate subframe (in blue) without errors.

agreement procedure to create a *security context* (i.e., NAS security context) for encryption and integrity protection. After the Authentication and Key Agreement (AKA) procedure, most messages between the UE and the MME are encrypted and integrity protected with cryptographic primitives. On the other hand, all initial procedures before establishing a security context in the AKA procedure are not encrypted and integrity protected by design. Those unprotected messages include paging, SIBs and several network layer initial messages specified in the LTE standard [5].

3 Overshadowing LTE Broadcast Message

In this section, we present the attack model, followed by a description of the `SigOver` attack. The `SigOver` attack is demonstrated by using an SDR that is widely used today (i.e., Universal Software Radio Peripheral (USRP) [16]). Lastly, we compare the `SigOver` attack with typical FBS attacks to show the effectiveness of the former.

3.1 Attack Model

We assume an active adversary with minimum privilege. The proposed attack model can be described as follows: (i) The adversary does not know the LTE key of the victim UE. (ii) The adversary is able to eavesdrop on the downlink broadcast messages transmitted from the legitimate LTE cell to the victim UE(s). However, as the victim key is unavailable, the encrypted messages cannot be decrypted. Note that (ii) is trivially achievable because messages are transmitted through the open medium. 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 Section 3.5, we discuss the fundamental differences between the proposed attack model and typical FBS attacks [21, 22, 36, 37, 39].

3.2 `SigOver` Attack Overview

This section briefly outlines the design of the `SigOver` attack. As discussed in Section 2, the LTE downlink is scheduled in a subframe granularity with a duration of 1ms. Each subframe is encoded separately by the base station, and is therefore decoded accordingly by the UE. Under this frame structure, Figure 3 conceptually illustrates the `SigOver` attack, where the attacker injects a crafted subframe (brown color) that precisely *overshadows* the legitimate subframe (blue color). Since the subframes are decoded independently from one another, the legitimate (non-overshadowed) subframes are generally not affected. At the same time, the injected subframe is crafted such that the UEs that have received and decoded the subframe behave based on the included information, which typically yields an abnormal or malicious behavior - an intended behavior by the attacker. The inherent vulnerability of LTE broadcast messages enables an attacker to launch various types of attacks using legitimately-looking messages (i.e., insidiously).

In principle, the `SigOver` attack leverages the capture effect [51], wherein the stronger signal is decoded when multiple simultaneous wireless signals (i.e., legitimate and crafted subframes) collide in the air. This is true for signals with a slight power difference of 3 dB [29]. Two technical challenges to launch the `SigOver` attack are (i) carefully crafting the overshadowing message to be decoded by the victim UEs (Section 3.3), and (ii) the stringent requirement of the transmission timing and frequency for precise overshadowing (Section 3.4).

3.3 Crafting a Malicious Subframe

Here we illustrate how to craft a subframe that can be successfully decoded at the victim UE for a successful attack.

Communication configuration matching. For the `SigOver` attack, the attacker must first identify the physical configuration of the legitimate cell on which the victim UEs are camping, to determine the structure of the attack subframe. The necessary physical configuration information for valid subframe construction includes the PCI, channel bandwidth, PHICH configuration, and transmission scheme (or the number of antenna ports); all of which are available to the attacker once the attacker camps on the same legitimate cell. In particular, PCI is calculated from the PSS/SSS, and the remaining information is obtained from the MIB. Furthermore, the attacker must synchronize with the SFN of the legitimate cell, which is also available in the MIB, to determine the injection time of the attack subframe.

Subframe structuring and injection. In LTE, when a UE reads a broadcast message, it decodes the following information from a subframe: i) a Control Format Indicator (CFI) that contains the control channel structure, ii) Downlink Control Information (DCI) that contains the allocated resource (i.e., resource blocks) for the message, and iii) the resource blocks (RBs) that contain the message itself. The CFI and DCI are

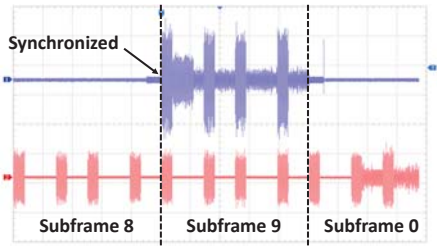


Figure 4: Oscilloscope snapshot showing precise time synchronization between a legitimate (in red) and a crafted signal (in blue).

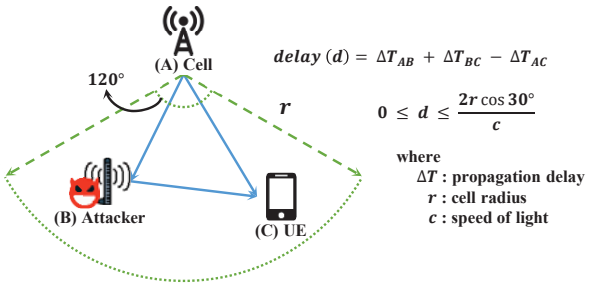


Figure 5: Propagation delay in the 3-sector cell configuration according to the location of the victim UE and the attacker. The attacker and victim UE are assumed to be within a cell coverage (the green sector form)

transmitted over the PCFICH and PDCCH respectively; and the message is transmitted over the PDSCH. Therefore, to inject a subframe, the attacker needs to craft a subframe that contains the PCFICH, PDSCH and PDSCH. However, the injected subframe containing those values may not be decoded correctly at the UE due to a channel estimation error. Note that the UE estimates the channel from the RS transmitted by the legitimate eNB, yet the estimation result may be inappropriate to decode the injected subframe correctly. To address this issue, the RS is included in the subframe for the `SigOver` attack, which significantly increases the robustness of the `SigOver` attack.

The last technical challenge related to the decoding of the crafted subframe is with respect to wireless channel estimation and equalization, for recovery from the signal distortion due to the channel. In the `SigOver` attack, the channel is estimated either dominantly (even solely depending on the paging occasion) from the crafted subframe (*RRC Idle*), or it is averaged from consecutive subframes (*RRC Connected*) along with multiple legitimate subframes. In the former, a single injection is sufficient for the attack (i.e., decoding of the crafted subframe). In the latter, repeated injections are needed to effectively reflect the wireless channel between the attacker and the victim UE. According to our measurement (Section 4) which injected one subframe for every SFN, `SigOver` attack reaches over 98% success rate in less than a second while maintaining reliable communication for legitimate subframes. In Appendix A, we present empirical results showing that legitimate communication is minimally affected by `SigOver` attack using several services including web browsing and streaming.

3.4 Accurate Overshadowing

Overshadowing requires the crafted subframe to overlap the legitimate signal precisely in both the time and frequency domains. This subsection discusses how this is achieved.

Time synchronization. To precisely overshadow legitimate subframes, an attacker needs to know the subframe timing (to determine when a subframe starts) and SFN (to determine when to inject the subframe with respect to the frame number) from the legitimate cell. The attacker obtains the subframe timing from the synchronization signals (i.e., PSS/SSS) and the SFN from the MIB of the legitimate cell. The attacker continuously obtains the subframe timing and the updated SFN, as the values vary over time depending on the channel condition. With the knowledge of the subframe timing and the SFN, the `SigOver` attack precisely synchronizes the transmission time of the crafted subframe with that of the target broadcast message (see Figure 4).

As shown in Figure 5, however, the crafted subframe transmitted at the acquired subframe timing may still arrive at the UE with a slight timing offset (with reference to the legitimate subframe) due to the propagation delay. Although the delay (d) is unavoidable (as the propagation delay is immeasurable by the attacker), its impact is minimal. This is because the baseband processor in the UE is designed to compensate the delay due to mobility and environmental effects [48]. Since the maximum delay that can be compensated is dependent on the baseband processor of the UE, we perform the following experiments to measure the delay. We assumed the typical three-sector cell configuration wherein the transmission angle of the cell is 120° [10]. The delay (d) is maximized when the attacker and the victim UE are located at both ends of the arc. This translates to $d = 8.66\mu$s under a typical cell radius of approximately 1.5km in urban environments. We measured the offset tolerance on two devices with different basebands (Qualcomm and Exynos), and the tolerance was larger than the maximum delay (i.e., 8.66μs) (see Section 4 for detailed experimental results).

Frequency synchronization. The operating frequency of a radio device is determined by the oscillator, where it inevitably suffers from a device-specific offset that is randomly imposed during manufacturing and generated during operation due to environmental effects (e.g., temperature). Such an imperfection in the oscillator is reflected in the radio signal as carrier frequency offset. In LTE, there are a number of readily available techniques [27, 50] to compensate for offsets up to a certain level (e.g., Up to ±7.5KHz for PSS based compensation in the LTE 15KHz subcarrier spacing [38]). Therefore, for the reliable implementation of the `SigOver` attack, the offset should be maintained below that level in the UE, at all times.

The LTE standard defines the minimum frequency accu-

Table 1: Comparison of the SigOver, FBS and MitM Attacker

	Stealthiness	Power efficiency	Attack sustainability
FBS	Low	Low	Low
MitM	Limited*	Low	Limited*
SigOver	High	High	High

* "Limited" means that the attack works in an limited environment

racy of a base station of ±50 ppb [1] for macro base stations. To satisfy the requirement, eNBs are equipped with highly accurate oscillators and further augmentation techniques such as a precision time protocol and GPS. In contrast, the SigOver attack was run on a typical, inexpensive SDR with an inaccurate oscillator (±2500 ppb for the USRP X310 [16]). A GPS disciplined oscillator (GPSDO) was employed, namely, an oven-controlled crystal oscillator (OCXO) to reduce the frequency offset to an appropriate level. The GPSDO provides a sufficient accuracy of ±25 ppb [14, 32] and is highly stable (±1 ppb when the GPS locked). This indicates a frequency offset of up to ±270Hz (at 3.6GHz with an offset of 75 ppb), within the LTE FDD frequency range of 460MHz-3.6GHz [6]. Our experiment confirms that all 10 devices (listed in Section 5) can compensate such small frequency offset to enable a reliable SigOver attack.

3.5 Comparison of SigOver, FBS and MitM Attacks

Although the FBS and Man-in-the-Middle (MitM) attacks can be used for broadcast message manipulation in LTE, only the former has appeared in the literature. In this section, we extensively analyze the FBS and MitM attacks in comparison with the SigOver attack with respect to stealthiness, power efficiency, and sustainability (see Table 1).

3.5.1 Attacks using FBS

The FBS attack is one of the most commonly used attacks against cellular networks [21, 22, 26, 36, 39, 40]. In an FBS attack, the attacker (i.e., the FBS) attracts victim UEs to camp on itself by transmitting a stronger signal than legitimate cells. The attacker then injects unprotected yet legitimate-looking messages to the victim UE. The FBS attack has the following limitations when compared with the SigOver attack.

Power Efficiency. In general, a UE selects the cell that transmits signals with the highest power. However, it has not been well investigated how much stronger signal the FBS should transmit than a legitimate base station to attract nearby victim UEs. This is an important question to be answered for the attacker, as higher power increases the chance of attracting the UE at a greater risk of being detected through power measurements (e.g., RSRP, RSRQ). According to the experimental measurements, the FBS attack reaches 100% success at 40 dB, whereas the SigOver attack was 98% successful at 3 dB (see Table 2). In particular, the FBS requires a power consumption greater than that of the SigOver attack by a factor of 5000, to achieve a comparable attack success rate.

(a) FBS attack (b) SigOver attack

Figure 6: Signaling messages during FBS and SigOver attack

Stealthiness. In general, an FBS is configured to masquerade as a legitimate base station as presented in previous studies [21, 22, 39, 40]. For example, the FBS broadcasts the same MIB and SIB1/2 messages as those of the legitimate cell and may use the same PCI to make itself indistinguishable from the legitimate ones. Nevertheless, the FBS inevitably carries several unique and clear signatures for detection [25, 30, 33, 49, 53]. First, as discussed earlier, an FBS attack uses ×10,000 stronger power (cf. ×2 for SigOver attack) than a legitimate cell, which is a clear indicator of the FBS. Second, when an FBS attracts a victim UE camping on a legitimate cell, the victim must undergo a cell re-selection process, where the victim UE reads the MIB and SIB1/2 messages from the FBS (Figure 6a). Third, the operation of the FBS may be very different from the legitimate ones due to its limited physical capabilities compared to the real base station[3]. Such operational characteristics include a relatively low paging rate, in addition to different RF properties such as a large frequency offset due to the low cost hardware. Finally, the FBS cannot establish a secure connection with the UE or transport protected NAS messages between the UE and the network (i.e., MME), which results in a denial of service to the UE. Hence, it is highly probable that a UE is able to detect an FBS. On the other hand, the mechanism of the SigOver attack is to precisely overshadow a specific broadcast message without interfering the synchronization between the victim UE and current cell. Therefore, as shown in Figure 6b, the UE does not carry out cell re-selection or reconfigure any cell-specific parameters. The UE subject to the SigOver attack maintains secure signaling connections with the legitimate eNB and MME.

Sustainability. If a victim UE camps on an FBS, it cannot receive the service via the FBS. This can be used by the UE as a potential FBS detection mechanism as mentioned above. To avoid such detection, the FBS may take the following strategy: it injects a malicious message to the UE, and releases a connection (e.g., by causing a radio link failure or triggering cell re-selection at the UE) so that the victim UE returns to a legitimate cell. Under this scenario, however, the injected

[3] A state-sponsored attack with unlimited resource and capabilities was not considered.

message should be selected such that the attack sustains even if the UE makes a cell change (e.g., `TAU Reject` [39]) or has an immediate impact on the UE (e.g., emergency warning message [21]). Thus, it is not an appropriate attack vector to exploit broadcast messages (e.g., SIB messages) that are refreshed when the serving cell changes. This makes the FBS attack either limited in terms of attack scope (as exploitable messages are very limited) or less sustainable in its duration.

3.5.2 MitM attacks

Recently, a new type of FBS attack referred to as the aLTEr [37] attack was discovered. This is an MitM attack that employs an FBS with eNB and UE capabilities. The eNB component of the FBS impersonates a legitimate eNB by relaying the messages from the eNB to a victim UE. In addition, the UE component of the FBS impersonates the victim UE by relaying the messages from the UE to the eNB. By sitting between the victim UE and the eNB, the MitM attacker manipulates user plane messages since the messages are not integrity-protected in LTE. The MitM attack inherits two aforementioned limitations of the FBS attack, namely, a high power consumption and low stealthiness, since the MitM attacker should attract the victim UEs in the same manner. Meanwhile, in principle, the MitM attack does not affect the connection between the victim UE and the eNB, thereby making the attack sustainable. However, we noticed that it is non-trivial to implement an MitM attacker for various reasons. First, to maintain the connection with a victim UE, the MitM attacker should relay all uplink and downlink messages exchanged between the victim UE and the eNB. To this end, the attacker must know the UE's radio resource settings configured by the eNB and configure the radio resource for the UE accordingly. Otherwise, the radio connection between the UE and the eNB may become unstable or fail. However, since the message that contains the radio resource setting (i.e., `RRC reconfiguration`) is encrypted, the attacker cannot properly configure the UE's radio resource. We note that the `RRC reconfiguration` contains a large number of PHY, MAC, RLC, and PDCP configurations for the UE.

To address this issue, the aLTEr attack used the radio configuration in a heuristic manner under the following conditions: (i) a victim UE receives the service using the *default radio configuration*, and (ii) the default radio configuration of an operator is stable. That is, only a few parameters (e.g., scheduling request (SR) and channel quality indicator (CQI) configuration) are changed for each radio configuration; whereas the others are the same. Thus, the attacker only needs to guess the CQI and SR configurations. However, in the real world, the eNB frequently changes the UE's radio configuration depending on the service that the UE is using and/or the current channel condition (e.g., initiating carrier aggregation, starting a Voice/Video call service, service priority, or channel quality change due to mobility). We observed that when a UE watched a YouTube video for 2 minutes under a bad channel condition, it received 9 `RRC reconfiguration` messages from the eNB, where the length of each message varied from 18 bytes to 109 bytes. Note that, as the attacker is only able to know the message length and the sequence of message delivery, it may not correctly guess the configuration. We also observed that 8 out of 9 messages have different CQI configurations which also need to be guessed.

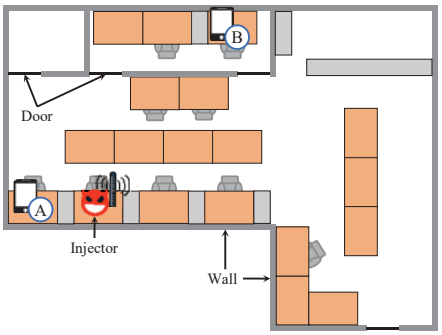


Figure 7: Experiments are conducted at two UE locations, A and B: A is 2m away from the attacker with line of sight. B is 10m away from the attacker, separated by a wall (i.e., non-line of sight). We refer to the former and the latter as LOS and NLOS, respectively.

These limitations apply to all MitM attacks, even when the attacker attempts to manipulate the broadcast message. However, the `SigOver` attack does not suffer from such limitations, as it only utilizes a persistent radio configuration acquired from the MIB of the legitimate cell (see Section 3.3).

4 Real World Experiment

In this section, we perform `SigOver` attack in the wild, and analyze the reliability of the attack.

4.1 Experimental Setup

We implement the `SigOver` attack based on the *pdsch_enodeb*, which contains a basic transmission function as part of srsLTE [43]. We add a custom-built receive function for time synchronization with the legitimate cell. The subframes were crafted using the srsLTE library. Moreover, an USRP X310 [16] equipped with a UBX [15] daughter board and GPSDO [14] 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 [28], if needed. Victim UEs are commercial smartphones that camp on a legitimate LTE cell with a 20MHz bandwidth. In addition, the diagnostic monitor tools (e.g., SCAT and XCAL [8, 42]) were used for the analysis of the transmitted and received messages at the UE.

Figure 7 illustrates the two locations within a university office, where two sets of experiments were conducted, as follows: (LOS) The victim UE and the attacker were in the same room, separated by a distance of 2m. (NLOS) The victim UE and the attacker were in different rooms separated by a

wall and distance of 10m. These two environments were used for experiments throughout the study.

Implementation details. An attacker acquires the information of the target benign cell (PCI, MIB) using *pdsch_ue* or diagnostic tools [8, 42]. She acquires time synchronization with the target cell (mimicking the procedure for a benign UE to camp on a cell by getting the PSS/SSS and MIB). After she obtains the arrival timing and SFN information of the LTE frame transmitted by the benign cell, she transmits the malicious message to the target SFN. Thereafter, she continuously receives the PSS/SSS (every 5ms) and MIB (every 10ms) transmitted by the benign cell and updates the synchronization information. Self-interference may cause synchronization problems, because Rx and Tx are in the same frequency. However, due to the precise overshadowing, the `SigOver` attack can minimize the effects on the legitimate PSS/SSS and MIB (there was no case of losing synchronization due to the self-interference).

As a minor issue, the USRP X310 generated an unintended high peak signal at the beginning and end of the signal when carrying out a burst transmission which `SigOver` attack does. This is due to the state change of the front-end components of the SDR. When there was no transmission, it was in the idle state. When transmission occurred, the transition to the transmitting state caused unwanted noise. We resolve this problem by simply padding zero to the front and back ends of the signal to separate the unwanted noise from the original signal, and by compensating the delay due to the zero padding during transmission.

Ethical considerations. As the attacker, we use a downward-facing dome-shaped antenna to minimize upward interference. In addition, we perform the experiments on the first basement level, which is the lowermost floor of the building. The basement floor was restricted during the experiments to prevent normal users from receiving the crafted signal. The experimental results with respect to the impact of the crafted signal revealed that the users upstairs and outside the building normally communicate with the legitimate base station without being affected by the signal. The signaling storm attack explained in Section 5.1.1 was run in a carrier's shielded testbed network, since the attack may cause a DoS on an operational network.

4.2 Practicality

In this section, we evaluate the practicality and robustness of the `SigOver` attack in the LOS/NLOS environment. We use an LG G7 ThinQ smartphone with SnapDragon845, which is the latest Qualcomm LTE chipset. We inject a paging message with the S-TMSI[4] intentionally set as an invalid value of `0xAAAAAAAA`, to differentiate the injected subframe from the legitimate subframes.

[4] S-TMSI is the shortened form of GUTI.

Table 2: Success rate of `SigOver` and FBS* attack

Relative Power (dB)	1	3	5	7	9
`SigOver`	38%	98%	100%	100%	98%
Relative Power (dB)	25	30	35	40	45
FBS attack	0%	0%	80%	100%	100%

* The FBS sets the same freq. band, PCI, MIB and SIB1 to the legitimate cell. If the victim UE camped on the FBS within 10s after it operates, the attack was considered a success. The FBS experiment was run 10 times for each power level. The `SigOver` experiment was performed with 100 paging messages for each power level.

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

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

Power cost. The `SigOver` attack exploits the capture effect, where it injects a stronger signal to overshadow the legitimate signal, which is at a lower power level. Moreover, we inject 100 paging messages into a victim UE in the *RRC Idle* state, and measure the success rate of the attack depending on the relative power between the injected and legitimate signals in the LOS environment. Table 2 shows that the `SigOver` attack achieves the success rate of 98% at 3 dB.

Attack robustness. Table 3 summarizes the success rates of the `SigOver` attack for different combinations of experimental settings (LOS/NLOS) and RRC states (Idle/Connected). Each measurement was an average of 120 injected paging messages. In the *RRC Idle* state, we inject a paging message at the exact paging occasion (e.g., Subframe 9) and paging frame (e.g., SFN%256 = 144) of the victim UE. As discussed in Section 3.3, in the *RRC Idle* state, the channel estimation is carried out solely on the injected signal; whereas in the *RRC Connected* state, the average of the channel estimated from a set of the injected and legitimate signals is considered. In other words, in the *RRC Idle* state, injected signals are individually decoded without the impact of the legitimate signals; thus successful attacks (i.e., correct decoding) can be achieved with a single injection. 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 occasion/frame of the victim UE. Simultaneously, we also inject a subframe with RS at every SFN, to reflect the channel of the injected signal and enable a successful attack. As shown in Table 3, the `SigOver` attack maintained a success rate greater than 97% in different RRC states and the LOS and NLOS setups, thus validating the robustness of the `SigOver` attack with respect to operating modes and environmental factors (e.g., multi-path). Finally, during the experiments the victim UE neither reported any radio link failures nor initiated radio connection re-establishment (i.e., `RRC Reestablishment request`). This implies that the `SigOver` attack is non-disruptive to the victim UE and its service. Furthermore, we verify that the `SigOver` attack maintains 100% success rate for over 100 SIB 1 and SIB 2 messages in the *RRC Idle* state and LOS setup.

Table 4: Time tolerance of two smartphones.

Time (μs)	LG G7 (Qualcomm)	Galaxy S9 (Exynos)
Min.	-2.93	-2.60
Max.	9.77	8.46
Max. tolerance*	12.7	11.06

* Note that the `SigOver` attack succeeds if $d <$ Max. tolerance, regardless of the cell radius; where d is defined in Section 3.4

Attack coverage. As described in Section 3.4, a crafted subframe may arrive at victim UE with a slight timing offset due to the propagation delay of the injected signal from the attacker to the victim UE. The decoding of the crafted subframe requires the offset to be bounded within the tolerance range of the UE LTE chipset. Hence, the largest tolerable offset determines the maximum propagation delay; or equivalently, the maximum distance between the attacker and the UE (i.e., the attack coverage). The attack coverage was experimentally evaluated, wherein the propagation delay between the attacker and the UE was emulated by time-shifting the transmission timings of the crafted subframes. We gradually changed the shift in the unit of 10 samples (=0.33μs at 30.72Msps), until the crafted subframes were not decoded; which indicates the maximum delay tolerance. Table 4 presents the tolerance measured from two smartphones with different basebands – LG G7 (Qualcomm), and Galaxy S9 (Exynos). The tolerance offset was consistently higher than 8.66μs across all the devices. With reference to the tolerance-distance relationship discussed in Section 3.4, the results indicate that the `SigOver` attack can cover the entire urban cell (typical radius of 1.5 km) at all times, irrespective of the relative positions of the UE and attacker.

5 Attack Scenarios and Implications

This section presents several attack scenarios using the `SigOver` attack, in addition to their practical implications. The `SigOver` attack can be used to exploit two broadcast messages; SIB and paging. All the attacks were run in the LOS setup presented in Section 4, with the exception of the signaling storm attack. To validate the proposed attacks on the various baseband chipset types, ten LTE capable smartphones were employed: one Intel (iPhone XS), six Qualcomm (Galaxy S4/S8/S9, LG G2/G6/G7), and three Exynos (Galaxy S6/S8/S9) chipset equipped smartphones.

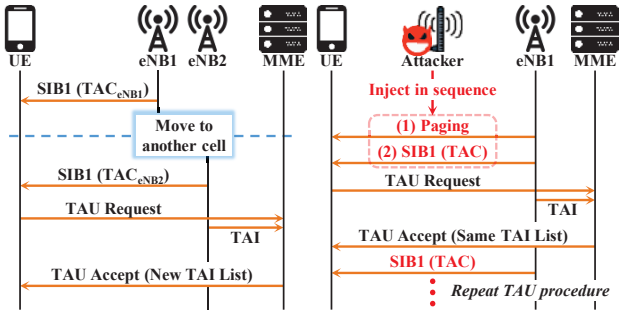
5.1 Attacks Exploiting SIB

In this section, a discussion on two types of attacks via SIB injection, namely, signaling storm and selective DoS, is presented.

5.1.1 Signaling Storm

Attack mechanism. When a UE moves to a new cell, the UE retrieves the Tracking Area Code (TAC[5]) contained in the SIB1 from the new cell and validates it using the TAI list in the

[5]TAC is the shortened form of TAI.



(a) Normal TAU (b) SigOver TAU

Figure 8: Normal and attack case for TAU procedures

UE. If the TAC is not included in the list of TACs on the UE, the UE initiates a TAU procedure to notify the LTE network of the updated TAC. The `SigOver` attack incurs the signaling storm by repeatedly triggering invalid TAU. Figure 8 illustrates the attack process when compared with the normal (i.e., without attack) operation. The attacker first overshadows a paging message with the `system_Info_Modification` field set as true, thus forcing the UEs to read SIB1. The SIB1 is then overshadowed using a spoofed TAC, thus leading to the TAU. It should be noted that the TAU request messages are directed to the legitimate eNB, because the `SigOver` attack preserves the radio connection between the victim and the legitimate eNB. Repeating this procedure results in the signaling storm on the LTE network. On the contrary, under normal circumstances, the TAU is performed only once each time the UE moves to another TA not included in the TAI list.

Validation. This attack was validated using a carrier's testbed LTE network with nine LTE devices[6] registered to the testbed network. Each device was running the diagnostic monitor tools (e.g., SCAT, XCAL [8, 42]) for the analysis of the UE-side signaling messages throughout the attack. Figure 9 reveals that a single UE carries out an average of seven TAU procedures per second, which is unlikely under the normal conditions without the attack. Moreover, the UE-side signaling messages were analyzed to better understand the behavior of the network under the attack. When the victim UE carries out the TAU with the spoofed TAC (irrespective of the validity of the TAC value), the network returns the same list of TACs previously provided during the legitimate registration. This is because the serving cell is unchanged. That is, the list of TACs still does not include the victim UE's spoofed TAC. Hence, the victim UE repetitively carries out the TAU upon receiving the SIB1 message from the attacker. Nokia reports [31] that a UE generates approximately 45 service requests[7] during a peak busy hour. However, the signaling storm via the `SigOver` attack induces a more significant network traffic, e.g., an attacker is able to trigger an average of 25,200 TAUs per UE per

[6]The iPhone was excluded because our monitoring tool does not support it

[7]UE sends a `Service request` during the connection initiation to the LTE network.

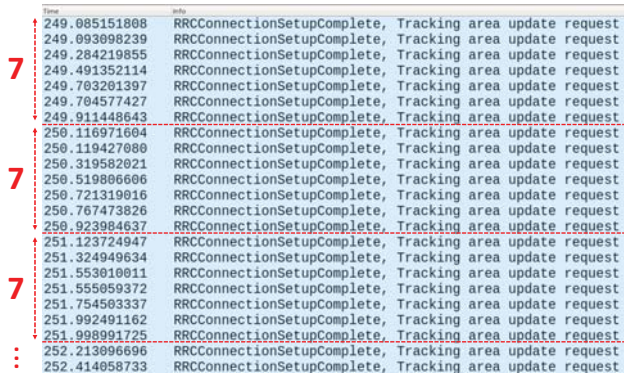


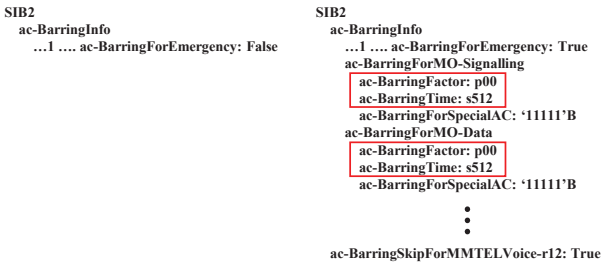
Figure 9: Wireshark snapshot of `TAU Request` messages generated by the SIB1 spoofing.

hour. Given that the number of signaling messages generated through the TAU and service request is similar, the attacker can generate more traffic than that generated during a peak hour by a factor of 560. This clearly demonstrates the significant impact of the signaling storm attack, which imposes a heavy signaling load on the network and causes severe battery drainage for the UE.

Boosted impact of Qualcomm chipset. A sustained signaling storm attack requires the attacker to continually inject SIB1 messages. However, the smartphones equipped with the Qualcomm baseband (e.g., Galaxy S4/S8/S9, LG G2/G6/G7) malfunctioned, thus generating TAUs indefinitely after a single SIB1 injection. In particular, the UE continued to perform the TAU procedure, even after the attacker stopped injecting SIB1[8]. The malfunctioning UE exhibits a normal behavior to the user, which indicates that the data/call service can be used without disrupting the user. Although the malfunction can be fixed by setting the UE in airplane mode, the user is unlikely to do so without noticing any problems. This indicates that the attack is sustained, even with the low-cost efforts to further strengthen its impact.

Infeasibility of the FBS or Rogue UEs. The signal storm attack seems to be achievable with an FBS. However, the injection of malicious SIB1 (containing the spoofed TAC) via the FBS does not lead to the signaling storm attack. This is because under the FBS, the `TAU request` from the victim UE is directed to the FBS, instead of the legitimate LTE network. In other words, the signals do not reach the LTE network; thus, the signaling storm attack is inherently unachievable for the FBS. Moreover, exploiting a number of rogue UEs may induce the signaling storm on the network. However, this approach is limited with respect to its scalability, wherein it requires multiple radio devices and SIM-cards for each device, to induce the same effect as the `SigOver` attack. On the other hands, the `SigOver` attack uses a single radio device that covers an entire cell and forces several authentic users camping on the cell to initiate the TAU procedure.

[8]The root cause of this malfunctioning is the implementation logic of the Qualcomm LTE chipset, which did not read the SIB1 after completing the TAU. As a result, they could not recognize the legitimate SIB1 that contained correct TAC, and the TAU was carried out until the legitimate SIB1 was re-read.



(a) Original SIB2 (b) Malicious SIB2

Figure 10: Access control feature in SIB2 message

5.1.2 Selective DoS through Access Barring

Attack mechanism. The cellular network has control over the number of UEs that can access the network. This feature is to manage the amount of traffic and maintain the stability of the network under specific conditions, e.g., a disaster. The control is realized using the *BarringFactor* parameter in SIB2, which is exploited by the `SigOver` attack to block the victim UE. By setting *BarringFactor* as 0 (via overshadowing), an attacker can restrict all data traffic and signaling from the UE (i.e., mobile originating)[9], which leads to DoS.

Figure 10 presents the configuration of the malicious SIB2 in the crafted subframe in comparison with the original SIB2 in a legitimate subframe. To maximize the impact of the attack, the `SigOver` attack sets the *BarringTime* to 512s, which is the maximum value as per the standard. Note that *BarringTime* can be refreshed if the attacker repeats the attack within the remaining *BarringTime*; thus, a persistent DoS can be achieved. To properly inject the crafted subframe (similarly to the signaling storm), the attacker first overshadows a paging message with `system_Info_Modification`. Thereafter, she overhears the legitimate SIB1 to extract the SFN, from which the attacker can obtain the schedule of the next SIB2 for overshadowing. A potential extension of this attack is service-specific DoS to *selectively* block only the targeted services (e.g., voice call, video conference, and SMS). This leverages a new service-specific barring feature introduced in 3GPP specifications [7].

Validation. This attack was validated using 10 different smartphone models. Upon the successful `SigOver` attack (i.e., injected paging and SIB2 are received); entire data services, which include web browsing and video streaming were blocked on all 10 devices. From the analysis of the device logs, it was found that all the devices failed to initiate any connection when applications made multiple connection requests. This confirms the feasibility of the barring via the `SigOver` attack. Moreover, the service-specific DoS was validated using

[9]The attacker can also block the mobile terminating traffic by overshadowing the paging channel of the victim UE.

the Samsung Galaxy S9 based on the Exynos chipset.

Comparison with the FBS. An FBS can also inject malicious SIB2. However, the attack is only valid when the FBS is turned on, and immediately stops when the FBS is turned off. This is because the victim UE connects to the legitimate cell shortly after disconnection from the FBS. During the connection to the legitimate cell, the victim UE reads the legitimate SIB2, which recovers UE services. Conversely, the services of the victim UE remain blocked after `SigOver` attack stops, as this does not incur cell reselection. Furthermore, the FBS cannot achieve the service-selective DoS, as it cannot provide the LTE service.

5.2 Attacks Exploiting Paging

In this section, we present three attacks through the `SigOver` attack on the paging message: DoS attack, network downgrading, and location tracking.

5.2.1 DoS Attack by Overshadowing Paging with IMSI

Attack mechanism. When the GUTI of the UE is unavailable, the network sends paging message with IMSI as an identifier of UE. As defined in the 3GPP standards, upon receiving the paging that contains the IMSI, the UE terminates all service sessions and initiates the registration procedure using the IMSI as the identifier [5]. This implies that the DoS attack can be realized by injecting the paging message with IMSI[10]. Specifically, the attacker injects a paging message that contains the IMSI of the victim UE at the paging occasion/frame of the victim UE. This attack detaches a UE from the cellular network services, which include voice call and data services, thus indicating a DoS at the UE. As the registration procedure (which follows the service termination) automatically recovers the services, the attack is sustained by the repeated injection of the paging message.

Validation. This attack was validated using 10 different smartphone models in two different operation states (*RRC Idle* and *RRC Connected*). Specifically, in the *RRC Idle* state, we confirmed that the UEs successfully received the overshadowed paging message. Furthermore, the internal logs in the UEs confirmed the expected impact of the attack, i.e., detachment from the network followed by the registration procedure, thus leading to DoS.

For following experiment, we launched the attack on the UE in the *RRC Connected* state. Note that the `SigOver` attack enables the attacker to convey the crafted message to the UE on the existing radio connection between the UE and the eNB. We first make a voice call on the victim UE to force the UE to enter the *RRC Connected* state. We then transmitted the paging message with IMSI to the UE. Interestingly, we observed that not all UEs handled the paging messages in the *RRC Connected* state. In particular, the Samsung Galaxy S8/S9, LG G6/G7 (Qualcomm), Samsung Galaxy S8/S9 (Exynos), and Apple iPhone XS (Intel) properly handled the paging message with IMSI, after which the call was immediately aborted (service termination). Meanwhile, the Samsung Galaxy S6 (Exynos), and Galaxy S4, LG G2 (Qualcomm) did not respond to the attack in the *RRC Connected* state.

The inconsistencies between the devices stem from the ambiguity of the 3GPP standards. The mechanism used to handle paging in the *RRC Connected* state is loosely defined, without specific direction on paging with IMSI, e.g., only information on paging with the system information notification or CMAS/ETWS [3] is provided. In summary, by injecting the paging message with IMSI , the `SigOver` attack can realize a DoS on the victim UE in *RRC Idle* and *RRC Connected* states, depending on the device.

Comparison with the FBS. This attack scenario was extensively discussed in the previous work [21, 35] leveraging the FBS. Although the impact and the attack vectors are equivalent, the applicability of the existing attacks is limited when compared with the `SigOver` attack. This is because the `SigOver` attack uniquely enables the attacker to deliver the paging message to the UE which has an active radio connection with the network, whereas other works are only applicable to UEs that use no services; thus indicating the wider applicability of the `SigOver` attack.

5.2.2 Network Downgrading Attack via CS Paging

Attack mechanism. In this attack, an attacker injects a paging message with a Circuit Switched (CS) notification (with the S-TMSI of the victim UE) to intentionally downgrade victim UEs to the 3G network. Upon the reception of the CS paging, the UE initiates the Circuit Switched Fall-Back process and transits to the 3G network. That is, the `SigOver` attack enables the attacker to force the UE to a slower connection.

Validation. We experimentally confirmed that the victim UE in the *RRC Idle* state immediately switched to the 3G network when the attacker's CS paging was received, after which it soon reverted back to the LTE network because there was no actual service in the 3G network. The attack was effective for the state-of-the-art smartphones, e.g., the Samsung Galaxy S8/S9, LG G6/G7 (Qualcomm), and Samsung Galaxy S8/S9 (Exynos), as they were able to respond the CS paging message the both *RRC Idle* and *RRC Connected* states. However, similar to the paging attack with IMSI, some smartphones did not respond to the CS paging in the *RRC Connected* state, and were therefore immune to the attack. Interestingly, when the Samsung Galaxy S8 (Qualcomm) dropped to the 3G network due to the attack, the LTE connection was never restored while using data service.

Comparison with the existing attack. Tu *et al.* demonstrated the throughput degradation attack against an victim UE by invoking the CS paging, which is similar to our attack [47]. However, in this study, the network was driven to send the paging message on behalf of the attacker, by establishing a

[10] Acquiring IMSI is extensively discussed in the previous work [11, 44]

call with the UE in the 3G network. It should be noted that, in the SigOver attack, the paging message is directly transmitted by the attacker. This attack inherently exposes the attacker's phone number, thus making the attack easily detectable by the operator. In comparison, the SigOver attack silently transmits the CS paging to the victim UE. Furthermore, the existing work cannot downgrade the victim UEs in the *RRC Connected* state to the 3G network, since the network does not send a paging message to the victim UE in the *RRC Connected* state; whereas the SigOver attack can deliver the paging message.

5.2.3 Coarse-grained Tracking of a UE

Attack mechanism. As explained in Section 2, following the completion of the RA procedure, the UE attempts to establish an RRC connection by sending a Connection request (containing UE identity) to the cell. If the UE holds the previously assigned temporary identity (i.e., S-TMSI), this identity is included in the Connection request as well. Otherwise, a random value is selected. Upon the receipt of the UE's request, the cell replies with the Connection setup that contains the UE's identity (the S-TMSI or the random value). By checking this identity, each UE is able to recognize if its RA procedure was successful. If the procedure fails, the UE retries the RA procedure. The abovementioned procedure used to resolve connection conflicts is referred to as a *contention resolution*.

In this attack, an attacker exploits the contention resolution technique to perform coarse-grained location tracking of the target victim. First, the attacker with the knowledge of the S-TMSI of the victim UE injects a paging message with the S-TMSI[11]. The attacker then eavesdrops on the Connection setup messages transmitted from the legitimate cell[12]. When the Connection setup message that contains the S-TMSI of the victim UE is received, the attacker confirms that the victim UE resides within the coverage of the cell by sniffing the downlink messages.

Validation. We validated this attack using all the smartphone models in this work. We confirmed that the attacker is able to identify the presence of the victim UE by injecting a single paging message and eavesdropping on the Connection setup message sent to the victim UE.

Comparison with the FBS. An FBS can achieve the same results by monitoring the IMSI in Identity Response message. However, the FBS requires an active connection to the target victim to transmit the message. Therefore, the attack is limited by the FBS with respect to its stealthiness and power efficiency. In a previous study, it was reported that RNTI-TMSI mapping can be applied to passively monitor the victim's TMSI [37]; however, the SigOver attack provides an active method by which the victim can be located.

[11] Due to the space limit, a detailed discussion on how an attacker acquires the S-TMSI of the target UE was omitted. However, this has been extensively investigated in previous studies [19, 22, 23, 37].

[12] Since the RRC connection procedure is not encrypted, the attacker can eavesdrop on any downlink messages during the connection procedure of the UEs.

6 Defending Against SigOver Attack

In this section, we present an outline of two possible defense strategies against the SigOver attack. We start the feasibility of the fundamental solution as a prevention measure, in which all the broadcast signals were digitally signed by adopting the Public Key Infrastructure (PKI). We then discuss a short-term solution for the detecting SigOver attack, which leverages the changing nature of the physical signal during the processing of the overshadowing signal.

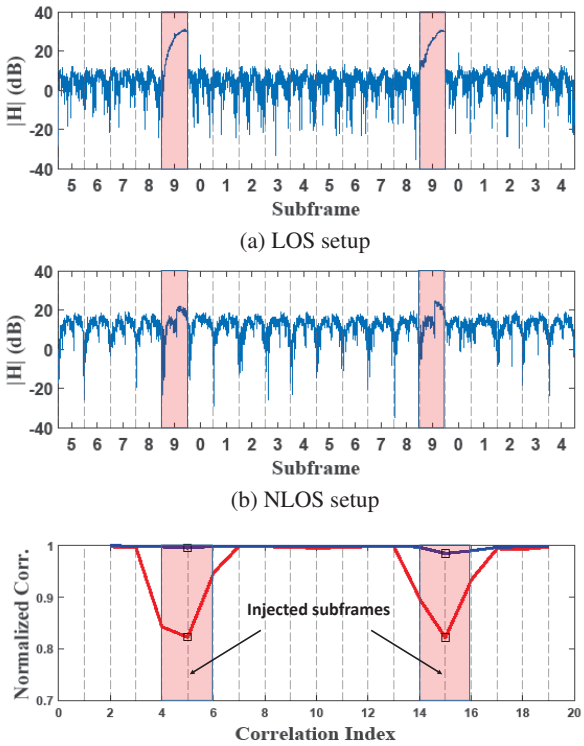
6.1 Digitally Signing Broadcast Messages

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 (e.g., self-signed one by the operator) to verify the certificate of the base station. However, this natural defense has at least several deployment and technical challenges.

Deployment challenges: In 5G, the 3GPP introduced a public key encryption for IMSI in the initial registration, to provide privacy protection for the permanent identifier. For this, each UE is provisioned with its home operator public key, thereby it was assumed that a public key provisioning mechanism to the UE is in place. This provisioning mechanism could also be used to provision a public key (or a signing certificate) for base station certificate verification. However, in roaming scenarios, the UE need to acquire the public key of the visited network operator, which is trusted by the home operator. This essentially requires a PKI for the global cellular networks that span the world and non-trivial trust relationships among multiple operators in different jurisdictions. Furthermore, managing certificate revocation lists are another obvious burden.

Technical challenges: 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 (e.g., using a new SIB) would result in a higher power consumption at the base station. Similarly, from UE's perspective, verifying certificate and signature would require additional power consumption, resulting in a faster battery drain. Such a power consumption may be prohibitive to low-power Internet of Things devices that need to survive many years without battery replacements.

An ID-Based Signature scheme (IBS) [9, 41] can be considered as a cost-effective alternative, as it has substantially low key management overhead and eliminates the certificate broadcast and verification overhead. However, the IBS requires UEs to get synchronized with the public parameters from KMS [17]. This is problematic to UEs that do not have a



(a) LOS setup

(b) NLOS setup

(c) Normalized cross-correlation on LOS (Red line) and NLOS (Blue line)

Figure 11: Fluctuation of the channel estimation magnitude after the `SigOver` attack: Sudden magnitude changes could be used for detection metric.

subscription as they may not be able to get the public parameters from the network. Note that the unsubscribed devices are also supposed to receive the ETWS or CMAS messages as long as they have cellular capabilities.

6.2 Leveraging the Channel Diversity

According to communication theory, a wireless channel varies significantly with a displacement of only a quarter of the wavelength, which is 3.57cm for 2.1GHz LTE [46]. This is referred to as the channel diversity, and it is highly applicable to the attacker and victim UE, which are expected to be at different locations – i.e., the wireless channel between the attacker and UE is likely to be disparate from that between the eNB and UE. Therefore, the injection of the attack signal, which reflects the channel between the attacker and UE, naturally forces the channel information recovered at the UE to deviate from when only the legitimate subframes are present (without attack). In other words, the detection of such a variance in the channel could serve as a defense technique.

The wireless channel can be conventionally represented as H [46] in complex representation. The magnitude $|H|$ uniquely defines different wireless channels depending on how efficiently the signal power is delivered. Hence, an abrupt change in $|H|$ is an effective metric to detect `SigOver` attack.

Figure 11a presents $|H|$ of the injected (Subframe 9) and legitimate signals measured during the experiment in LOS setup, where the attacker is located 2m away from the victim UE. This clearly demonstrates the severe fluctuation of $|H|$ when the attack occurs, indicating effortless detection.

Despite its effectiveness, the robustness of leveraging the channel is problematic. In particular, the general application of the technique to various scenarios is not trivial, due to the various factors that have a potential influence on H. Figure 11b shows a detection failure example in NLOS setup, when the power of the injected signal was low. That is, the impact of the attack signal to H gradually fades out as the energy decreases, down to the point where it is difficult to detect. Figure 11c clearly demonstrates this challenge, wherein the drop in the correlation was fuzzy in NLOS setup, unlike in the LOS setup (strong injection signal). In summary, leveraging the channel is a potential solution, where we leave the design of robust techniques as future work.

6.3 Discussion on Potential Solutions

Both approaches discussed in the previous sections present challenges to be addressed and/or limitations. However, we note that the exploits demonstrated in Section 5 are only a few examples rather than an exhaustive list. The effects of the `SigOver` attack would be broader and more damaging if the cellular network is utilized for critical domains, e.g., vehicular networks and industrial systems. Therefore, in principle, the intrinsic broadcast vulnerabilities of the cellular system should be addressed. Meanwhile, it is recommended that critical services should have their own security protection instead of relying on those of other protocol layers. For example, the issue of the ETWS or CMAS may be better addressed at the application level[13], instead of being based on SIB protection, since the SIB is only a transport mechanism for those critical application messages.

7 Related Work

In this section, we describe previous work that exploits the signal overshadowing concept. We then present the signaling storm, in addition to attacks that exploit the non-integrity protection.

Signal overshadowing in wireless channel. The signal overshadowing attack, which exploits the use of an open medium and the capture effect, has been widely conducted in the wireless systems such as GPS [20, 45] and Low-Rate Wireless Personal Area Networks (LR-WPANs) [52]. Pöpper *et al.* presented a symbol flipping attack on the Additive White Gaussian Noise (AWGN) channel [34], with a fine-grained overshadowing of the signal at the symbol level. However, it requires exact information with respect to the timing, amplitude, and phase, which is difficult to achieve in the real

[13] The 3GPP already conducted a study on the security aspects of Public Warning System (PWS) [4].

world. Similar to this study, Wilhelm et al. demonstrated the possibility of signal overshadowing and its impact on IEEE 802.15.4 [52]. In comparison, the SigOver attack is the first comprehensive study in which the signal overshadowing attack on the LTE was realized, in addition to the validation of its practicability. Moreover, we present the novel attack scenarios by leveraging the SigOver attack.

Message manipulation in LTE. The LTEInspector [21] conducted a paging channel hijacking attack and paging message injection attack, which seems similar to this study. However, this study has two key differences: 1) the definition of the injection attack and 2) its realization method. First, the SigOver attack silently injects the victim with malicious messages while making the victim keep being synchronized with the legitimated eNB. As a result, during the SigOver attack, the uplink response message of the victim naturally goes to the legitimated eNB. However, the victim UE in LTEInspector transmitted its uplink response message to the malicious eNB after receiving the manipulated message, which is the general response action for the attack with the FBS. Thus, it is more similar to existing attacks using FBS. Second, the SigOver attack overwrites the target signal with malicious signals without requiring a connection to the malicious base station. To this end, we investigate various requirements of the SigOver attack as described in Section 3. Despite other requirements, LTEInspector only considered the paging cycle and its occasion, which are the part of timing synchronization requirements.

Attacks exploiting non-integrity protection. Extensive research has been conducted on the manipulation of messages with no/weak-integrity protection [21, 22, 26, 36, 39, 40]. As discussed in Section 3.5, such attacks mainly leverage an FBS. Although they exploited the broadcast messages in LTE, but the attacks have limited implications. This is because their operational logic inevitably produces limitations with respect to stealthiness, power efficiency, and attack sustainability.

8 Concluding Remarks and Future Work

Signal overshadowing is an intuitive method for the manipulation of LTE broadcast messages with no integrity protection, which was not addressed in previous studies. In this paper, 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 feasibility and effectiveness of SigOver attack was demonstrated in five novel attacks, and an extensive analysis of the relative advantages of the SigOver attack over those of the FBS and MitM attacks was carried out. The key features of the SigOver attack are stealthiness, power-efficiency, and sustainability, which have not been achieved simultaneously by previous attacks. The evaluation revealed that the SigOver attack achieves a 98% success rate with low power cost.

Finally, two potential approaches to defending against the SigOver attack were proposed, which leveraged the digital signature and channel diversity. As acknowledged, both approaches have challenges and limitations to be addressed; however, they can be used as a basis for the development of a reliable and robust solution.

The cellular industry is rapidly transitioning to the 5G network of cellular systems equipped with advanced radio technologies and enhanced security features. However, the fundamental broadcast security issues discussed in this paper have not addressed in design. Considering significant changes made in the 5G New Radio (NR), it is left as a future study to evaluate 5G NR against the SigOver attack. As this paper turns on the spotlight on the security of broadcast messages, we believe that 3GPP standard body and cellular network community need to consider the design of broadcast messages seriously.

Acknowledgments

We sincerely thank Dr. Soo Bum Lee for his detailed and valuable comments on the earlier version of the draft. In addition, we would like to thank the anonymous reviewers for their insightful comments. This work was supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (2018-0-00831, A Study on Physical Layer Security for Heterogeneous Wireless Network).

References

[1] 3GPP. ETSI TS 36.104. Base Station (BS) radio transmission and reception, 2017.

[2] 3GPP. ETSI TS 36.211. Physical channels and modulation, 2011.

[3] 3GPP. ETSI TS 36.331. RRC Protocol specification, 2017.

[4] 3GPP. TR 33.969. Study on Security aspects of Public Warning System (PWS), 2014.

[5] 3GPP. TS 24.301. Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3, 2017.

[6] 3GPP. TS 36.101. User Equipment (UE) radio transmission and reception, 2017.

[7] 3GPP. TS 36.331. Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification, 2017.

[8] ACCUVER. XCAL. http://accuver.com/acv_products/xcal/.

[9] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Annual international cryptology conference*, pages 213–229. Springer, 2001.

[10] Bruno Clerckx and Claude Oestges. *MIMO wireless networks: channels, techniques and standards for multi-antenna, multi-user and multi-cell systems*. Academic Press, 2013.

[11] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. IMSI-catch me if you can: IMSI-catcher-catchers. In *Proceedings of the 30th annual computer security applications Conference*, pages 246–255. ACM, 2014.

[12] Sebastian Egger, Tobias Hossfeld, Raimund Schatz, and Markus Fiedler. Waiting times in quality of experience for web based services. In *Quality of Multimedia Experience (QoMEX), 2012 Fourth International Workshop on*, pages 86–96. IEEE, 2012.

[13] Juanita Ellis, Charles Pursell, and Joy Rahman. *Voice, video, and data network convergence: architecture and design, from VoIP to wireless*. Elsevier, 2003.

[14] Ettus. GPSDO OCXO. https://www.ettus.com/product/details/GPSDO-MINI.

[15] Ettus. UBX 160MHz Board. https://www.ettus.com/product/details/UBX160.

[16] Ettus. USRP X300/X310 Spec Sheet. https://www.ettus.com/content/files/X300_X310_Spec_Sheet.pdf.

[17] Michael Groves. Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI). *RFC6507*, 2012.

[18] GSA. Evolution from LTE to 5G: Global Market Status. Aug. 2018.

[19] Byeongdo Hong, Sangwook Bae, and Yongdae Kim. GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2018.

[20] Todd E Humphreys, Brent M Ledvina, Mark L Psiaki, Brady W O'Hanlon, and Paul M Kintner. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Radionavigation Laboratory Conference Proceedings*, 2008.

[21] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In *Proceedings of the Network and Distributed Systems Security (NDSS)*, 2018.

[22] Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. In *IEEE Symposium on Security & Privacy (SP)*. IEEE, 2019.

[23] Denis Foo Kune, John Koelndorfer, Nicholas Hopper, and Yongdae Kim. Location leaks on the GSM Air Interface. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2012.

[24] Younes Labyad, Mohammed MOUGHIT, Abderrahim Marzouk, and Abdelkrim HAQIQ. Impact of Using G. 729 on the Voice over LTE Performance. *International Journal of Innovative Research in Computer and Communication Engineering*, 2(10), 2014.

[25] Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu. FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. In *NDSS*, 2017.

[26] Huang Lin. LTE REDIRECTION: Forcing Targeted LTE Cellphone into Unsafe Network. In *Hack In The Box Security Conference (HITBSecConf)*, 2016.

[27] Konstantinos Manolakis, David Manuel Gutiérrez Estévez, Volker Jungnickel, Wen Xu, and Christian Drewes. A Closed Concept for Synchronization and Cell Search in 3GPP LTE Systems. In *2009 IEEE Wireless Communications and Networking Conference*, pages 1–6, April 2009.

[28] minicircuit. ZVE-2W-272. https://www.minicircuits.com/WebStore/dashboard.html?model=ZVE-2W-272%2B.

[29] Johan Moberg, Mattias Löfgren, and Robert S Karlsson. Throughput of the WCDMA Random Access Channel. In *IST Mobile Communication Summit*, 2000.

[30] Peter Ney, Ian Smith, Gabriel Cadamuro, and Tadayoshi Kohno. SeaGlass: enabling city-wide IMSI-catcher detection. *Proceedings on Privacy Enhancing Technologies*, 2017(3):39–56, 2017.

[31] David Nowoswiat. Managing LTE Core Network Signaling Traffic. https://www.nokia.com/blog/managing-lte-core-network-signaling-traffic/.

[32] OPENBTS. Ettus Research USRP. http://openbts.org/w/index.php?title=Ettus_Research_USRP.

[33] Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, Andrew Martin, and Jean-Pierre Seifert. White-Stingray: Evaluating IMSI Catchers Detection Applications. In *USENIX Workshop on Offensive Technologies (WOOT). USENIX Association*, 2017.

[34] Christina Pöpper, Nils Ole Tippenhauer, Boris Danev, and Srdjan Capkun. Investigation of Signal and Message Manipulations on the Wireless Channel. In *Proceeding of the European Symposium on Research in Computer Security (ESORICS)*, 2011.

[35] Muhammad Taqi Raza, Fatima Muhammad Anwar, and Songwu Lu. Exposing LTE Security Weaknesses at Protocol Inter-Layer, and Inter-Radio Interactions. In *International Conference on Security and Privacy in Communication Systems*, pages 312–338. Springer, 2017.

[36] David Rupprecht, Kai Jansen, and Christina Pöpper. Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness. In *10th USENIX Workshop on Offensive Technologies (WOOT)*, 2016.

[37] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. Breaking LTE on Layer Two. In *IEEE Symposium on Security & Privacy (SP)*. IEEE, 2019.

[38] Stefania Sesia, Matthew Baker, and Issam Toufik. *LTE-the UMTS long term evolution: from theory to practice*. John Wiley & Sons, 2011.

[39] Altaf Shaik, Ravishankar Borgaonkar, N Asokan, Valtteri Niemi, and Jean-Pierre Seifert. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2016.

[40] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks. In *WISEC*, pages 75–86, 2018.

[41] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques*, pages 47–53. Springer, 1984.

[42] Signaling Collection and Analysis Tool (SCAT). https://github.com/fgsect/scat.

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

[44] Daehyun Strobel. IMSI catcher. *Chair for Communication Security, Ruhr-Universität Bochum*, 14, 2007.

[45] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 75–86. ACM, 2011.

[46] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[47] Guan-Hua Tu, Chi-Yu Li, Chunyi Peng, and Songwu Lu. How voice call technology poses security threats in 4g lte networks. In *Communications and Network Security (CNS), 2015 IEEE Conference on*, pages 442–450. IEEE, 2015.

[48] Jan-Jaap Van de Beek, Magnus Sandell, and Per Ola Borjesson. ML estimation of time and frequency offset in OFDM systems. *IEEE transactions on signal processing*, 45(7):1800–1805, 1997.

[49] Thanh van Do, Hai Thanh Nguyen, Nikolov Momchil, et al. Detecting IMSI-catcher using soft computing. In *International Conference on Soft Computing in Data Science*, pages 129–140. Springer, 2015.

[50] Qi Wang, Christian Mehlfuhrer, Christian Mehlführer, and Markus Rupp. Carrier frequency synchronization in the downlink of 3GPP LTE. In *21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 939–944, Sep. 2010.

[51] Kamin Whitehouse, Alec Woo, Fred Jiang, Joseph Polastre, and David Culler. Exploiting the capture effect for collision detection and recovery. In *Embedded Networked Sensors, 2005. EmNetS-II. The Second IEEE Workshop on*, pages 45–52. IEEE, 2005.

[52] Matthias Wilhelm, Jens B Schmitt, and Vincent Lenders. Practical message manipulation attacks in IEEE 802.15. 4 wireless networks. *Proceedings of MMB & DFT*, 2012.

[53] Zhou Zhuang, Xiaoyu Ji, Taimin Zhang, Juchuan Zhang, Wenyuan Xu, Zhenhua Li, and Yunhao Liu. Fbsleuth: Fake base station forensics via radio frequency fingerprinting. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 261–272. ACM, 2018.

Appendix

A Impact on Quality of Services

We measure the impact of the quality of services under the `SigOver` attack, where the malicious paging messages are transmitted at the every subframe 9. This implies that legitimate subframes at subframe 9 are overshadowed and lost, whereas non-overshadowed legitimate subframes may also be affected by crafted subframes. Specifically, the RS of the crafted subframes perturbs the channel estimation averaged among crafted and non-overshadowed legitimate subframes (in *RRC Connected* state), which may disturb the equalization and incur errors. Despite such factors, the impact of `SigOver` attack is validated to kept minimal, as demonstrated in this section under a range of common, but distinct services of voice call, web surfing, FTP download, and live streaming. We note that measurements were carried out under a reliable `SigOver` attack (>97% success rate) for the UE in the *RRC Connected* state.

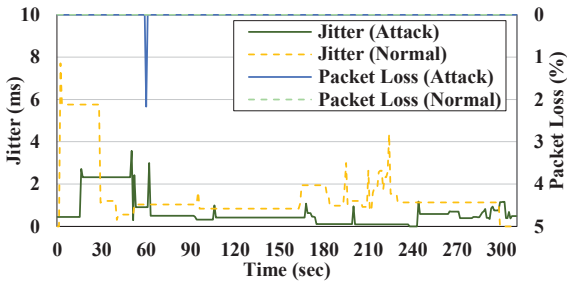


Figure 12: Call jitter and packet loss

Voice call. The UEs camping on LTE network use Voice over LTE (VoLTE) as a call service. We evaluate the impact of the `SigOver` attack on the key factors with respect to the VoLTE performance [13]; or equivalently, the call quality, e.g., data rate, jitter, and packet loss. Such metrics were measured before and after the attack for comparison. The data rate was kept stable after the attack, and omitted for brevity. Figure 12 illustrates the jitter and the packet loss. The jitter was consistently less than 10ms, and the packet loss is mostly kept as zero. Moreover, both were sufficient to support high quality call services [24]. This keeps the `SigOver` attack stealthy without degrading user experience.

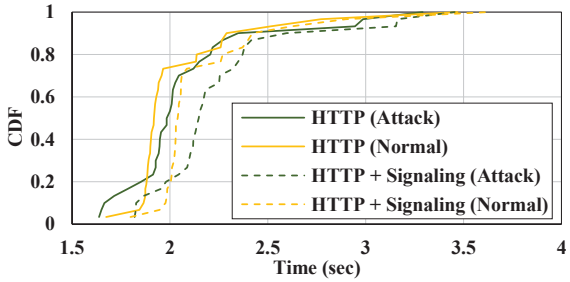


Figure 13: Webpage loading time

Web-browsing. We extend the measurements to web browsing, which is one of the most frequently used services. Specifically, the time required to load multiple identical web pages with and without the attack. Figure 13 presents the results, with 'HTTP' representing the total duration of HTTP data exchange for page loading. 'Signaling' is the time required for RRC connection establishment. Under the `SigOver` attack, the time from the RRC connection initiation to the web page downloading is delayed by an average of only 80ms when compared with the case without the attack. Previous studies [12] have shown that the impact of such lag on the quality of the experience is negligible.

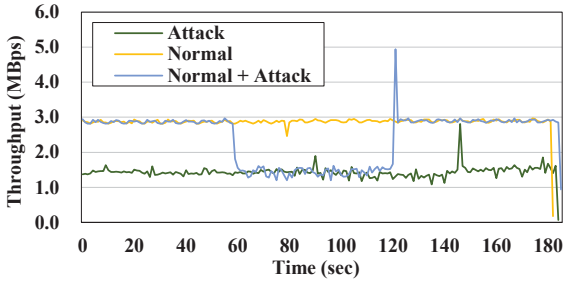


Figure 14: FTP throughput

FTP downloading. Figure 14 reveals that the FTP exhibited a significantly different performance under the `SigOver` attack. This is due to dynamically controlled modulation, to overcome the bit error in the communication. The `SigOver` attack incurs bit errors, which force the UE to use a robust modulation of QPSK, which has a limited throughput. Conversely, without the attack, the bit error is kept low. In this case, the UE used 64QAM which is less robust but supports higher throughput than QPSK. However, this impact is less likely to be experienced by the users and FTP rarely used on smartphones.

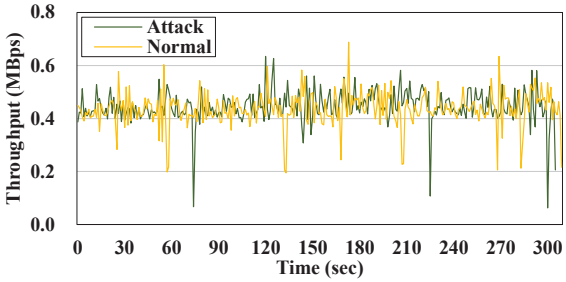


Figure 15: YouTube Live throughput: The average was 0.445 and 0.436MBps for attack and normal case, respectively.

Live streaming. Figure 15 shows the throughput of the YouTube live streaming at a resolution of 1080p. In summary, neither buffering nor interruption occurred under the `SigOver` attack during a 5-min video clip. The result of the live streaming differs from that of the FTP downloads, as streaming throughput was not as high as that of the FTP.

B ACRONYMS

3GPP	Third Generation Partnership Project
AKA	Authentication and Key Agreement
AS	Access Stratum
CFI	Control Format Indicator
CMAS	Commercial Mobile Alert System
CQI	Channel quality indicator
CS	Circuit Switched
DCI	Downlink Control Information
eNB	Evolved Node B
EPC	Evolved Packet Core
ETWS	Earthquake and Tsunami Warning System
FBS	Fake Base Station
FDD	Frequency Division Duplex
GPSDO	GPS disciplined oscillator
GUTI	Globally Unique Temporary Identity
IMSI	International Mobile Subscriber Identity
LOS	Line of sight
LTE	Long Term Evolution
MIB	Master Information Block
MME	Mobility Management Entity
NAS	Non Access Stratum
NLOS	Non-line of sight
OFDM	Orthogonal Frequency Division Multiplexing
PCFICH	Physical Control Format Indicator CHannel
PCI	Physical layer Cell Identity
PDCCH	Physical Downlink Control CHannel
PDSCH	Physical Downlink Shared CHannel
PHICH	Physical HybridARQ Indicator CHannel
PRB	Physical Resource Block
PSS	Primary Synchronization Signal
RA	Random Access
RACH	Random Access CHannel
RB	Resource Block
RRC	Radio Resource Control
RS	Reference Signal
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
SAE	System Architecture Evolution
SDR	Software Defined Radio
SFN	System Frame Number
SIB	System Information Block
SSS	Secondary Synchronization Signal
S-TMSI	SAE Temporary Mobile Subscriber Identity
TA	Tracking Area
TAI	TA identity
TAU	Tracking Area Update
UE	User Equipment