Advanced Network Security: Project 7
Report Overshadowing - Group 13

Laura Kolijn - s1025724
Tom Koning - s1020020
Jesse Ravensbergen - s4573560
Denise Verbakel - s1018597

December 2021

1 What is overshadowing?

An overshadowing attack is a form of attack which exploits specific fixed transmission timings of LTE subframes. The LTE subframes are "overshadowed" by the attacker whom will send their own malicious subframe to replace the subframe that was sent by the legitimate cell. In essence, all an attacker needs to do is send out the message on a stronger signal than the cell. Overshadowing subframes can easily be done with a popular SDR, which can be purchased for relatively cheap. However, there are also other methods to accomplish overshadowing, which we will see when describing different overshadowing attacks.

2 Different overshadowing attacks

Thus far, three different variants of the overshadowing attack are already known. The first attack, which was a novel primitive attack in this area of research, is called the SigOver attack [12]. This research was done by Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim and Yongdae Kim and is from August 14-16 2019. Following this research, two other (independently found) overshadowing attacks based on the SigOver attack appeared:

1) At June 9 2021, Simon Erni, Patrick Leu, Martin Kotuliak, Marc Röschlin and Srdjan Čapku introduced the AdaptOver attack [3];

2) At June 28 2021, Norbert Ludant and Guevara Noubir presented the SigUnder attack [5].

In the next three sections, we are going to describe the idea behind the different attacks and the feasibility of them in practice. We will also look into what other attacks are enabled by using the overshadowing attacks, what the limits of these attacks are and if there are known mitigations. Finally, we will also talk about interesting tests to perform with SigOver, AdaptOver or SigUnder and what the possible consequences of a successful execution of these attacks are.

3 SigOver

The first overshadowing attack we will discuss is called SigOver. The SigOver attack exploits the so-called fixed transmission timing of LTE subframes: the malicious attacker injects a self-made subframe in such a way that the original subframe is exactly and flawlessly overshadowed [12]. This concept is also depicted in Figure 1. As we can see, five legite subframes (in blue) were sent from the base station to the UEs. The attacker has made a malicious and stronger subframe (in brown) which they also send to the UEs. When these signals are timed perfectly and the frequency matches, the UEs will use the stronger signal of the

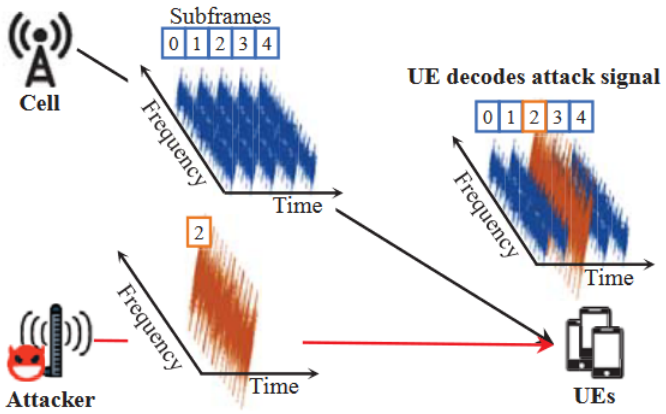

Figure 1: Visual representation of the SigOver attack [12]

attacker for subframe 2 instead of the legit subframe 2. This way, the UEs will decode the attack signal inside the other legit subframes instead of the original signal/message.

As we can see from the explanation above, the SigOver attack can be split into three steps. We will elaborate upon them in general below:

1) *Crafting a malicious subframe*
The first step the attacker takes is making a malicious subframe that they will use in the SigOver attack. This activity is divided into two parts: (i) the communication configuration matching and (ii) the subframe structuring and injection. In this step, the attacker used the knowledge that the subframes sent from the base station to the UE are decoded independently and thus that the other subframes the attacker does not overshadow are not affected [12].
In part (i) the attacker needs to get to know the physical configuration of the base station to which the UEs are connected. This is needed to determine the structure of the subframe the attacker needs to make in order to match it with the legitimate signal. All information needed about the physical configuration can be seen by the attacker when they connect to the same base station as the UEs and includes for instance the channel bandwidth and the transmission scheme or number of antenna ports [12].
In part (ii) the attacker should make sure that the UE will decode its subframe appropriately. When a UE receives a broadcast message, it will decode the CFI (Control Format Indicator), the DCI (Downlink Control Information) and the RBs (Resource Blocks). In order to do a successful SigOver attack, the attacker thus needs to make a subframe that contains the right information for these three elements.

2) *Synchronization of time and frequency*
The second step consists of synchronizing: the attacker should make sure that both the time and frequency of their maliciously crafted subframe is matching with the original subframe they want to overshadow.
The time synchronization is important to overshadow the original subframe because the attacker needs to know when that particular subframe begins and what frame number belongs to that subframe [12]. The frequency synchronization of the the signal in the subframe is also important in order to keep the offset below the oscillation level in the UE [12].

3) *Overshadowing by the malicious synchronized subframe*
The third and last step of the SigOver attack is done by the (unknowing) victim UE: it will decode the stronger signal of the attacker instead of the original signal of the base station whenever the attacker has done steps 1) and 2) properly. But why does this step happen at the side of the UE? As stated in [12]: "in principle, the SigOver attack leverages the capture effect, wherein the stronger signal is decoded when multiple simultaneous wireless signals (i.e., legitimate and crafted subframes) collide in the air". The capture effect [10] thus states in simple words that the stronger signal will always be

decoded instead of other weaker signals. This phenomenon already occurs at a small power difference of 3 dB [6] and thus can easily be exploited as done in the last step of the SigOver attack.

Note that we mentioned 'the attacker' multiple times above. In this attack it is assumed that (i) the attacker is not aware of the LTE key of the victim UE and (ii) the attacker can eavesdrop on the downlink broadcast messages (messages from the base station to the victim UE) [12].

3.1 Follow-up attacks and possible consequences

The SigOver attack as described above can be used to exploit two broadcast messages, namely SIB (System Information Block) and paging [12]. Knowing this, we can describe two attacks using SIB injection and three attacks exploiting paging messages.

First, we will briefly discuss the two types of attacks via SIB injection:

1) *Signaling storm*
   Simply said, a signaling storm is an attack that overloads the bandwidth between the UE and the base station by, for instance, repeatedly sending messages [4]. Such a signaling storm can be achieved at the moment the UE moves to another area such that the UE should connect to a new base station. The SigOver attack exploits this by repeatedly triggering invalid TAU (Tracking Area Update) resulting in too much messages send on the bandwidth between the UE and the base station [12].

2) *Selective DoS*
   To achieve a selective DoS using SigOver, the attack exploits a feature that determines how many UEs can access the network at the same time [12]. If by overshadowing, this number is changed into a 0, no UEs are able to connect to the network. This means that "an attacker can restrict all data traffic and signaling from the UE" [12]. Since only a number of UEs is affected, this obviously leads to a selective DoS attack.

After having described the follow-up attacks using SIB injection, we will show what the three types of attacks via paging messages are:

1) *DoS attack*
   In order to perform a DoS attack using paging messages, the attacker exploits a 3GPP standard. This standard states that when a paging messages that contains the IMSI is received, the UE should terminate all service sessions and initiate the registration procedure with the identifier set as the received IMSI [1]. An attacker can thus overshadow such paging message by injecting the IMSI of the victim UE. This results in an detached UE from the cellular network services, which thus indicates a DoS at the UE [12].

2) *Network downgrading*
   Another method an attacker could use is to force the victim UE to downgrade to the 3G network. The attacker could overshadow a paging message by injecting a Circuit Switched (CS) notification to initiate the transit to the 3G network [12].

3) *Location tracking*
   The SigOver attack can also be used to estimate the current location of a certain victim UE when an attacker knows the S-TMSI of the victim. The idea is that the attacker overshadows a paging message by injecting the known S-TMSI. After this, the attacker eavesdrops on the Connection setup messages transmitted from the original base station: whenever the attacker sees the S-TMSI they injected, the attacker can confirm (by sniffing the downlink messages) that the victim UE is somewhere in the range of that particular base station [12].

So, briefly stated, the follow-up attacks of SigOver consist of two different ways of achieving a DoS attack, a signaling storm, network downgrading to 3G or tracking the approximate location of a victim UE.

3.1.1 Possible consequences

The possible consequences of a successful overshadowing attack depend on how an attacker uses the SigOver attack. There are two ways to use this attack: use SigOver as a stand-alone attack or perform one of the follow-up attacks as described in subsection 3.1 (so using SigOver as part of an overarching attack).

If SigOver is used as a stand-alone attack, some maliciously crafted subframe is inserted in some legitimate signal, resulting in a malicious signal that will be received by the victim UE. The possible consequences of this attack is then that the signal received will be decoded as some gibberish communication or even a totally fake communication when the overshadowing attack is executed perfectly. Broken data integrity is thus the main consequence of this way of using the SigOver attack.

If the SigOver attack is used as a part of an overarching follow-up attack as introduced in subsection 3.1, there could be a lot more possible consequences. Firstly, if the overshadowing attack results in a DoS attack, an evident consequence is that legitimate users cannot use their device in a normal way without a working connection. Another potential consequence of this is information loss during the DoS attack. Secondly, when an attacker performs the signaling storm properly, a possible consequence would be unavailability (as also happens when a DoS attack is performed). Thirdly, when the attacker forces the victim UE to downgrade to the 3G network, a logical consequence is a slower connection for the victim UE. Last but not least, when the attacker tracks the approximate location of a victim UE, a consequence that cannot be avoided is private information leakage (such as the victim UEs location).

3.2 Feasibility in practice

The Sigover attack is feasible in practice ('in the wild') as has been demonstrated in [12]. This attack has been mounted against a legitimate base station and several commercially available smartphones. The researchers did this in two ways: the first experimental setup had the victim UE and the attacker in the same room, separated by a distance of 2 meters; the second experimental setup had the victim UE and the attacker in different rooms, separated by a wall and a distance of 10 meters.

Since this attack was conducted 'in the wild', the three ethical considerations were taken during this experiment [12]. The first one was that the researchers used a downward-facing dome-shaped antenna to minimize upward interference for normal users (such that they are not affected by the experiment). The second consideration was that the researchers performed the experiments in the basement, again to minimize upward interference. The last ethical consideration that was thought of was to run the signaling storm in a carrier's shielded testbed network in order to not DoS the operational network. This way, the SigOver attack could be safely performed in practice without facing any legal consequences.

3.3 Limitations

Compared to the FBS (Fake Base Station) attacks and the MitM (Man in the Middle) attacks, SigOver does not have any limitations regarding stealthiness, power efficiency and sustainability as examined in [12]. However, later research as described in [3] has found two limitations for this overshadowing attack:

1) *The DoS caused by SigOver is not persistent*
   The selective DoS attack (achieved by using SIB injection) has no persistence: the victim UE will immediately try to re-attach to the base station. In comparison to the selective DoS attack, the 'normal' DoS attack (achieved by using paging messages) has a persistence of around 9 minutes [3]. This is not considered as a very strong DoS attack.

2) *Need predictable scheduling for the synchronization*
   In order to get a working SigOver attack, we need to know the underlying physical configuration of the base station, such as the scheduling (as described earlier). The attack thus only works on a single base station at the same time. "In reality, however, the UE is rarely in a situation with only one cell [base station] in reach, so it immediately switches over to the next available cell, requiring the attacker to mount the attack on all base stations in the vicinity of the victim as otherwise the DoS attack does not impact a UE in a real-world setting" [3].

3.4 Mitigations

In [12] it is mentioned that there are two different mitigation techniques, namely digitally signing broadcast messages and leveraging the channel diversity. Below we will briefly describe what these mitigations entail. Note that next to these mitigations, [5] also stated that their found mitigations for the SigUnder attack work also against the SigOver attack. For these mitigations we refer to subsection 5.4.

The first mitigation discussed by the researchers is employing integrity protection in the messages using a digital signature scheme [12]. This is a proper way to defend against the overshadowing attack since SigOver takes advantage of the lack of integrity protection. This lack of protection can naturally be mitigated by digitally signing messages: in this way data integrity is guaranteed.

The second mitigation is about channel diversity. Knowing that wireless communication can be depicted by waves, channel diversity is the variation of wavelengths on a certain channel. When a SigOver attack happens, a slight change in these wavelengths occurs due to changing the legitimate subframe with a malicious subframe. Detecting these slight changes can mitigate the impacts of such overshadowing attack.

3.5 Interesting tests

The first test that would be interesting to perform with these attacks that comes into mind is testing on which scale the SigOver attack could be successful. We saw in subsection 3.2 that the SigOver attack could be performed in practice, but to what extent can we overshadow all the UEs on a single network? Since this has a lot of ethical considerations, this would probably not be the best test.

However, a sensible next step in the overshadowing research area is to tweak the test variables of the SigOver attack as described in subsection 3.2. Here, we will exclude the variables that are changed and tested in AdaptOver and SigUnder such as size of the size overshadowed part of the signal (no whole subframes).

An interesting test would be to see what the effect is of a UE connecting to a different base station. In the experiment conduced in [12] it is namely the case that all the smartphones camp on a legitimate base station with a 20MHz bandwidth. What would the effect be of 'moving' smartphones that change from one base station to another? And how does the amount of Hertz affect the experimental results? What happens when we change the bandwidth from 20MHz to for instance 19MHz and then back to 20MHz? How effective would the SigOver attack then be?

Another interesting test would be to see how much the variable distance affects the SigOver attack. In the conducted experiments, the researchers used a distance of 2 meters and a distance of 10 meters (the latter with a wall in between the attacker and victim UE). But what would happen if we doubled, tripled, or even made this distance much larger? Does this prevent SigOver from working, or does this adjusted variable just make the attack more difficult? And what would happen if we take the same distance of 10 meters, but instead of 1 wall between the attacker and victim, have a barrier with a thickness of 5 walls in between the attacker and victim?

Both these experiments could be conducted in approximately the same way and using the same ethical considerations as was done before by the researchers of SigOver in [12].

4 AdaptOver

AdaptOver is a new LTE signal overshadowing attack that allows an adversary to reactively and adaptively overshadow any downlink message between the network and the user equipment (UE). We consider the following attacker: (i) No knowledge of any keys and no physical access to components of the operator or the user equipment (UE). (ii) Capability to receive the downlink communication from the base station to the UE; no ability to decipher encrypted messages. (iii) Capability to send LTE signals to the UE such that the power of the attacker's signal at the UE is 3dB higher than the power of the signal transmitted by the base station. This can be achieved either by adjusting the transmission power or the location of the attacker's device.

The AdaptOver form of attacking exploits the way the UE's are supposed to interact with base stations. More specifically, the interaction that is required to establish a connection, regain a connection or transmit data. The UE devices are configured in such a way that they generally listen to the message with the highest

power, also known as the loudest message. This is easily exploited by sending the same message a basestation would send, but then 'louder', meaning that a potential attacker would send a more powerful signal.

From AdaptOver paper: *They accomplished this by overshadowing parts of the signal with their attacker signal that achieves a higher power at the UE. Although these two signals collide, the stronger signal will still be decoded. This phenomena is called the capture effect.*

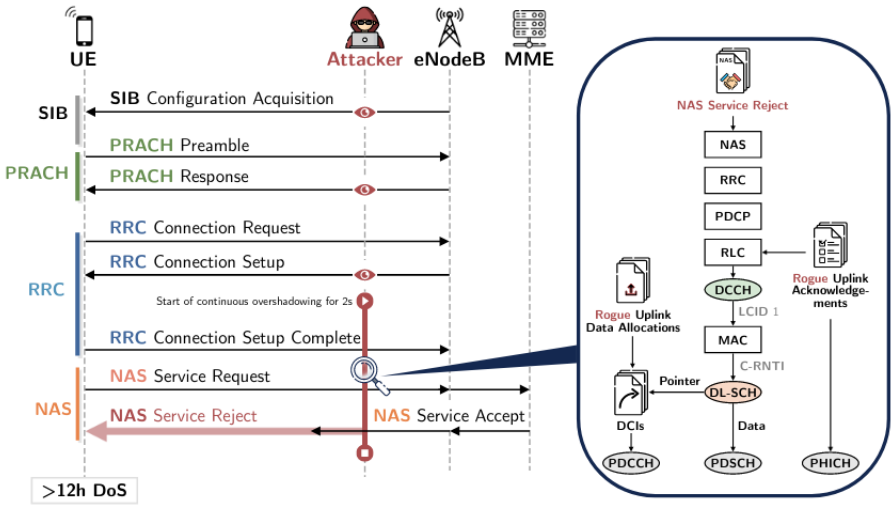

Figure 2: AdaptOver explained using Service Reject Attack. The attacker listens for the RRC Connection Setup message to start the attack. The attacker sends the NAS Service Reject on every subframe for 2 seconds, overshadowing the Service Accept with a Service Reject, causing a >12h DoS at the UE. During the attack, the attacker includes rogue uplink allocations and acknowledgments to allow the UE to send the NAS Service Request.

4.1 Follow-up attacks and possible consequences

The AdaptOver attack enables near endless possibilities for DoS attacks. The greatest feature of this attack is the amount of time that it can deny the service of any victim UE.

4.2 Feasibility in practice

This attack is far more feasible in practice than other attacks, but only whene executed properly. The only limit is the knowledge of the attacker, meaning that if they do not understand what they are doing (read, what they are trying to overshadow) it will not be feasible at all. The hardware required for this particular attack is really easy to come by as well.

4.3 Limitations

The power required to set up and execute the attacks mentioned in the AdaptOver paper is one of the slight limitations of the attacks. Take note of the word slight, as it genuinely is not that big of a problem to get the proper amount of power required. The attack range of a signal with strength 20dB is already more than enough to overshadow the usual 40 dB transmissions of an eNodeB.

The main limitation of setting up an attacker system would be the amount of time spend researching the exact timings the eNodeB is transmitting messages that are potentially targetable for overshadowing. The paper mentions a service reject attack, an attach reject attack and an authentication reject attack. All of which should be looked into in order to find what messages should be overwritten.

4.4 Mitigations

Even though it is not possible to guarantee availability in LTE, it is always possible to disturb the wireless channel such that communication is impossible. The best way to counter an attack such as the attacks described in the AdaptOver paper, is by implementing detection mechanisms. Detecting the AdaptOver attack on lower level layers is not difficult (continuous overshadowing the downlink with identical information to blank out any legitimate downlink traffic) presenting a highly identifiable characteristic.

On higher levels in the protocol, the separation of legitimate and false rejections could be done by identifying the absence of a message authentication code.

The integrity of the messages that are sent over the wireless interface can be easily achieved by sending over a message authentication code to the messages send. Assuming an attacker does not have access to the shared secret key between the UE and the base-station, there is no way for an attacker to replicate such a MAC.

4.5 Interesting tests

As a first test, it would be interesting to figure out to what extend we can check whether a message sent over the wireless interface was created with malicious intent. As mentioned by the paper, the way to test that would be by setting up an eNodeB, which sends along a MAC with the more important messages such that the UE can check whether the messages have been tampered with or not. Such a test would also allow researchers to see how much of an impact sending along MAC's would have to the overall speed and efficiency of the protocols.

Another interesting test would be building a framework that allows for signals of different strength to attempt and overshadow legitimate eNodeB messages. Instead of continuously sending out a 20dB signal, one could then try to send messages at a lower or even higher power level in order to see how the effectiveness of the attacks change. By playing around with the power levels it might be possible to figure out a cheaper way of attacking UE's

5 SigUnder

The last overshadowing attack that we will discuss is the SigUnder Attack [5]. This attack is a subcarrier-selective overshadowing attack, which means that the difference between target and PBCH symbols is transmitted in a subcarrier basis.

For this attack there are two models that need to be described: the communication model and the adversarial model. For the ***communication model***, it is assumed that a 5G base station (gNodeB) with a fixed position operates at a frequency within Frequency Range 1 (frequencies lower than 6GHz). The base station periodically transmits Synchronization Signal Block (SSB) signals in order for 5G capable devices (UEs) to be able to initially access the network. The UEs follow the standard initial access procedure to connect to the network.

With regards to the ***adversarial model*** there are a few assumptions that are made. The first assumption is that the attacker is positioned within the coverage of the gNodeB station and is thus able to record and process RF samples from 5G bands. Next to this, it is assumed that the attacker can generate and inject 5G signals at any time they wish. Lastly, the attacker is assumed to be capable of processing the Synchronization Signal Block signals and maintaining time and frequency synchronization with the gNodeB.

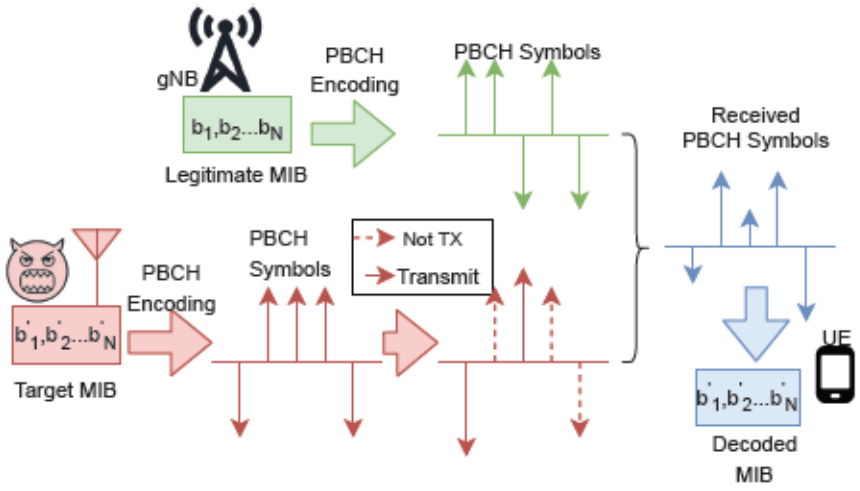

Figure 3: Visual representation of the SigUnder attack [5]

For the actual attack, the attacker will position themselves in the direct neighborhood of the gNodeB and start listening to the SSB signals that the gNodeB sends. The attacker then proceeds to perform the necessary steps to connect to the base station, synchronizing in time as well as frequency with the base station and storing the Master Information Block (MIB) that is received in the process. This Master Information block contains information with regards to the network configuration that is needed to establish a connection with the core network. To spoof the Synchronization Signal Block, the attacker chooses what the target Master Information block should be and encodes this signal using the PBCH (Physical Broadcast CHannel) encoding. The legitimate Master Information Block that was stored during the process of connecting to the network is also PBCH encoded. The attacker than identifies exactly which PBCH symbols differ between the target MIB and the legitimate MIB. When the gNodeB sends the SSB signal that the attacker wants to spoof, the subset of PBCH symbols that differ are transmitted at a slightly higher power level. The difference in power is precisely enough to cancel out the legitimate symbol and flip it to the symbol that the attacker wants to have there once the signals get added over the air.

5.1 Follow-up attacks and possible consequences

The difference in power between the signal that the attacker sends and the legitimate signal is significantly smaller for the SigUnder attack than for previous overshadowing attacks. This means that the SigUnder attack enables a more stealthy and lower-power version of previous DoS and overshadowing attacks.

Next to this, the SigUnder attack also enables some completely new attacks, using specific fields in the Master Information Block. The first example of such an attack is blocking UEs from this particular cell by setting the `cellBarred` field in the MIB. If the `cellBarred` field is set, there is another field that the attacker can tamper with, namely the `intraFreqReselection` field. This bit indicates whether or not intra-frequency cell selection is allowed when the current cell is barred, so if this field is set, the UE will not select any cell in the same frequency as the barred cell.

Secondly, the `pdcch-ConfigSIB1` field can be set, which allows an attacker to specify where a UE should look for the System Information Block 1 (SIB1). This means that the attacker is able to specify their own part of the spectrum where the victim will look for SIB1. This allows an attacker to perform different follow-up attacks, one of which is forcing the target UE to transmit the so-called Random Access preamble with high power by setting a specific field in SIB1. This in turn allows an attacker, among other things, to identify the UE's that are nearby.

5.2 Feasibility in practice

In the paper the performance of the attack is evaluated using "both software simulations and over the air measurements" [5]. A real channel was used for the over the air measurements as is described in section 4.3 of [5]. The experiments that have been conducted have revealed a number of technical challenges, that will be described in the next section. Apart from these challenges it does seem like it is possible to use the attack in practice. However, it is not clear from the description in the article whether the channel used was fully under the control of the researchers and whether the conditions under which the tests were conducted fully matched a channel in the real world (e.g. multiple UEs on the channel). In case the channel did not match a real-world channel at all, there could be even more limitations and even more things that would have to be almost perfectly aligned for the attack to work, making it a huge challenge at best to use the attack in practice.

5.3 Limitations

There are a few different challenges when the SigUnder attack is to be performed in a real-world setting. The first of these problems has to do with synchronizing the timing of the spoofed signal and the legitimate signal. Since the legitimate and forged PBCH symbols need to be added to end up with the desired symbol for the attacker, the signal that the attacker sends needs to be synchronized with the signal that is sent by the gNodeB. The Cyclic Prefix that is included in the 5G New Radio waveform does allow for some offset between the two signals. If the offset between the two signals is less than the duration of the Cyclic Prefix, the signals do still add up correctly. The CP length thus limits the range over which the attack works.

The next limitation we face is that the attacker needs to align the phases of the two signals. To be able to do this, the phase offset of the gNodeB needs to be tracked and the offset needs to be maintained constant in order for the attack to be successful.

Lastly, channel estimation needs to be in place. Without channel estimation, the attack does work in some cases, but there is a large decrease in performance compared to when channel estimation is used.

5.4 Mitigations

There are a few ways to mitigate this attack. The first of these mitigations is so-called Successive Interference Cancellation (SIC). The idea behind SIC is that a signal that is decoded by the receiver is subtracted from the signal that was received and the resulting signal is again decoded. This traditional scheme does not work optimal for the SigUnder attack, since in this attack it is possible to only overshadow a subset of subcarriers. This would cause the subcarriers left untouched by the attacker to be zeroed out after the received signal was subtracted, requiring some adjustments to the original scheme.

There are two ways to adjust the original scheme, namely using Partial SIC or Equalized SIC. With Partial SIC the subtraction is not done with the decoded signal at full strength but with a scaled-down version of the signal. This prevents subcarriers that were not targeted by the attacker from being zeroed out.

Using Equalized SIC there is an even bigger probability that the original signal will be recovered. With Equalized SIC a metric of choice (e.g., Error Vector Magnitude) is used to determine which set of subcarriers were targeted by the attacker. Subsequently the original SIC scheme is applied to this set of modified subcarriers only. This significantly increases the probability of recovering the legitimate signal, especially when the attacker uses very low-power signals to overshadow the legitimate signal.

The second mitigation mentioned in the paper is integrity protection. One possible solution that is suggested is the use of signatures such that the UE is able to verify whether or not the MIB for example is legitimate. However, since the MIB has a very limited size it would not be feasible to include a signature to the MIB itself without significantly changing the entire SSB. Therefore, the authors propose to include the signature of both the MIB and the SIB1 with the SIB1. This can be implemented relatively straightforward since there exists specific kind of field that can be added to existing 5G messages. Because this is an already existing field, the gNodeB would be backwards compatible with systems that were deployed before this change would be implemented.

5.5 Interesting tests

As already mentioned in section 5.2, it is not fully clear to what extent the channel that the over the air measurements were performed on, represented a channel in the real world. Assuming that the researchers had full control over certain conditions on the channel that cannot be controlled in practice, it would be interesting to test how feasible this attack actually is in practice.

Moreover, a logical next step would be to investigate what techniques other than SIC can be used to reconstruct the original signal and thus to mitigate the SigUnder attack. In particular, looking at the results of the experiments with the different extensions of SIC when using a DeModulation Reference Signal (DMRS), we see that the probability of reconstructing the original MIB is only greater than random chance in the case of a rather weak signal from the attacker. It would be interesting to investigate whether there is a technique to be able to significantly increase the success rate even when the attacker uses more powerful signals.

6 Comparison SigOver, AdaptOver and SigUnder

In this section, we will discuss three main differences between the aforementioned overshadowing attacks. We will talk about the differences concerning what parts of a signal are overshadowed, signal strength and possible follow-up attacks:

1) *Differences in parts of a signal that are overshadowed*
   For the attack described first, namely the SigOver attack, it is necessary to overshadow an entire subframe or even multiple subframes of the particular signal the malicious user wants to attack. In the two newer attacks described thereafter, this has been improved and thus these do not require an entire subframe to be overshadowed.
   The AdaptOver attack requires the attacker to only overshadow the part of a subframe where the target message is located. In [3] the target message described is the Service Accept message: the Service Reject attack they researched required an attacker to change the Service Accept message into a Service Reject message. Note that the attacker might need to overshadow the Service Accept message (in the case of a Service Reject attack) in multiple subframes.
   In the SigUnder attack a malicious user overshadows multiple subcarrier(s) in the SSB (a total of at most 3 Orthogonal Frequency-Division Multiplexing symbols [5]) instead of a whole subframe. Thus, the SigUnder attack requires for even less subcarriers to be overshadowed compared to the AdaptOver attack, resulting in a more power-efficient attack (see the second difference).

2) *Differences in signal strength (in dB)*
   The first overshadowing attack described used a signal strength of 3 dB over the legitimate signal, which was quite an improvement over the fake base station attacks used previously (which operate with a signal difference of 35 dB). The AdaptOver and SigUnder overshadowing attacks both improved this in their own different ways.
   The researchers that introduced AdaptOver came up with the idea to make the signal even less powerful: their overshadowing attack uses signals that are just 1.8 dB over the legitimate signal. Despite being less powerful compared to the SigOver attack in terms of number of dBs needed to overshadow the legitimate signal, this overshadowing attack still performs well.
   The third attack, the SigUnder attack, took another approach for determining the signal strength to be used. In this attack, the signal is 3.4 dB *under* the legitimate signal instead of *over*. As we can see, this signal strength is way lower than the previously mentioned attacks. However, if we look at the absolute value of the amount of dB used, we see that SigUnder actually uses the strongest signal to achieve an overshadowing attack (but it is the hardest to discover, see the third difference).
   Note that the results given in all three research papers can differ in practice. This is because part of the differences in dB can be attributed to variances in the setup of an experiment.

3) *Differences in possible follow-up attacks*
   In subsection 3.1 we described some follow-up attacks that are made possible by the SigOver attack. These attacks are made more persistent and stealthy over time as described by the two other overshadowing attacks.
   AdaptOver has made the overshadowing attack better in terms of persistence. As we have seen, a DoS attack can now continue for >12 hours instead of the maximum duration of 9 minutes with the SigOver attack, making the consequences of the attack a lot more persistent.
   SigUnder has made another improvement in comparison to the SigOver attack, namely with regard to stealthiness. The follow-up attacks made possible by this overshadowing attack are much more difficult to detect and thus go unnoticed more often. Besides this, another outcome of the SigUnder attack is that new attacks are made possible by overshadowing specific fields in the MIB (contained in the SSB).

7 Similar attacks to overshadowing attacks

The concept of overshadowing is not unique to LTE, or indeed any mobile network. In fact, as long as data is transferred wireless (i.e. over the air), it is possible to interfere with the physical integrity of the message. Most simply, a legitimate message m can be destroyed by another message m' sent at the same time, so long as they are each others exact inverse. This is called destructive interference, and is of course a much more primitive attack than overshadowing as presented for LTE [9]. Of course, challenges here are similar to those of LTE Overshadowing. To send such a message m', one must know what m will look like. Furthermore, it must be sent at (almost) the exact same time as m, which similarly causes issues of timing.

However, there are more subtle attacks. Relying on much the same properties as LTE Overshadowing, for many wireless interfaces it is possible to interfere with specific parts of a message in order to flip bits or otherwise replace parts of a message. One such interface is IEEE 802.15.4, which we will discuss in more detail later. Again, this encounters the same problem as its LTE equivalent – timing. Furthermore, many wireless interfaces are now encrypted. This means at best we can flip bits at random, which is not particularly useful. Indeed, while there may be a physical property that allows us to overshadow (parts of) a message, this does not immediately mean it is exploitable.

7.1 Distance Enlargement/Reduction in IEEE 802.15.4

IEEE 802.15.4 is a protocol that establishes the operation of wireless personal area networks (WPAN). Most commonly, this protocol is used by a variety of IoT devices to communicate with one another, such as RFID readers, smart home appliances, or autonomous vehicles.

In a simple test setup, Wilhelm et al. demonstrated that they were able to overwrite a specific part of an IEEE 802.15.4 frame [11]. It relied on the same property as LTE Overshadowing: when signals collide, only the stronger of the two is received. Again the timing is very precise ($< 1\mu s$ in IEEE 802.15.4), and so far this has not been translated into a practical attack.

More interesting are a variety of attacks that provide distance enlargement or reduction between devices. IEEE 802.15.4 implements a distance bounding protocol, which allows devices to communicate their distance to one another. This protocol is far more accurate than traditional locating methods such as GPS, providing an accuracy of up to 10 cm and 10 m, respectively [7]. The protocol itself is simple. If an RFID reader wants to know the distance to an RFID tag it is communicating with, the reader will send a message to the tag. The longer it takes for the RFID tag to reply, the further away it is. One might see how this can be exploited.

It is not difficult to relay the communication between an RFID tag and an RFID reader, so there is no need for them to be physically close to each other. However, the distance bounding protocol is meant to ensure that the RFID tag is physically within the vicinity of the reader. If we respond before the legitimate RFID tag responds and our broadcast is louder than that of the RFID tag, our response will be considered the legitimate one and we will have overshadowed the legitimate response. This will make it seem like the tag is close to the reader, and thus we might gain access to e.g. a secured area.

Practically however, this is difficult. If the expected response is e.g. some typical challenge-response scheme, then it is likely we cannot actually respond before the legitimate RFID tag responds. As such, this attack is well-defended against and challenging to execute. However, we can also enlarge the apparent distance between two devices in a similar way [8]. Consider two autonomous vehicles that communicate with one another in order to avoid a collision. They too use the distance bounding protocol in order to ensure they keep a proper distance from one another. Here, we can intercept the response message and replay it at a later time. We might cancel out the legitimate response through destructive interference, or we might simply send our reply over the legitimate response, but louder (overshadowing) [2]. In either case, our response now took longer than the legitimate signal. The two vehicles will now believe they are at a safe distance from one another, while in reality they are on a collision course.

This is much more difficult to defend against, as we now don't need to know some cryptographic secret to execute the attack. Such distance enlargement attacks are far easier to execute, and could potentially be very problematic for e.g. autonomous vehicles. In both cases we rely on the property of louder messages being considered legitimate, very similar to that of LTE Overshadowing. Notably, in these practical examples, timing is less of an issue. Our response only needs to be fast (or slow) enough to get the distance we want, but we do not need to precisely time our response to a legitimate signal.

References

[1] 3GPP. 2017. Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS). Technical Specification (TS) 24.301. Stage 3. 3rd Generation Partnership Project (3GPP). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1072.

[2] Alberto Compagno, Mauro Conti, Antonio Alberto D'Amico, Gianluca Dini, Pericle Perazzo, and Lorenzo Taponecco. 2016. Modeling enlargement attacks against uwb distance bounding protocols. *IEEE Transactions on Information Forensics and Security*, 11, 7, 1565–1577.

[3] Simon Erni, Patrick Leu, Martin Kotuliak, Marc Röschlin, and Srdjan Capkun. 2021. AdaptOver: Adaptive Overshadowing of LTE signals. (June 2021). https://arxiv.org/pdf/2106.05039.pdf.

[4] Erol Gelenbe, Omer H. Abdelrahman, and Gokce Gorbil. 2016. Detection and mitigation of signaling storms in mobile networks. In *2016 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, (February 2016), 1–5. DOI: 10.1109/iccnc.2016.7440686. https://doi.org/10.1109/iccnc.2016.7440686.

[5] Norbert Ludant and Guevara Noubir. 2021. SigUnder: a Stealthy 5G Low Power Attack and Defenses. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, (June 2021). DOI: 10.1145/3448300.3467817.

[6] John R. Moberg, Mattias Löfgren, and Robert S. Karlsson. 2000. Throughput of the wcdma random access channel. In *Proceedings of IST Mobile Communication Summit*. (October 2000). https://www.semanticscholar.org/paper/Throughput-of-the-WCDMA-Random-Access-Channel-Moberg-L%5C%C3%5C%B6fgren/fc052fb6eb24b1902b2e7bd7300be11b4c4a33d5.

[7] Niloofar Orouji and Mohammad Reza Mosavi. 2020. Novel secure positioning method in ultra-wide band framework based on overshadowing attack probabilistic model. *IET Communications*, 14, 21, 3778–3783.

[8] Mridula Singh, Patrick Leu, AbdelRahman Abdou, and Srdjan Capkun. 2019. Uwb-ed: distance enlargement attack detection in ultra-wideband. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 73–88.

[9] Nils Ole Tippenhauer, Kasper Bonne Rasmussen, and Srdjan Capkun. 2016. Physical-layer integrity for wireless messages. *Computer Networks*, 109, 31–38.

[10] Kamin Whitehouse, Alec Woo, Fred Jiang, Joseph Polastre, and David Culler. 2005. Exploiting the Capture Effect for Collision Detection and Recovery. In *The Second IEEE Workshop on Embedded Networked Sensors (EmNetS-II)*. IEEE, (May 2005), 45–52. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.67.3968.

[11] Matthias Wilhelm, Jens B Schmitt, and Vincent Lenders. 2012. Practical message manipulation attacks in ieee 802.15.4 wireless networks. In *MMB & DFT 2012 Workshop Proceedings*, 29–31.

[12] Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. 2019. Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, (August 2019), 55–72. ISBN: 978-1-939133-06-9. https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon.