Don’t hand it Over: Vulnerabilities in the Handover Procedure of Cellular Telecommunications

Evangelos Bitsikas
New York University Abu Dhabi
Abu Dhabi, UAE
eb173@nyu.edu

Christina Pöpper
New York University Abu Dhabi
Abu Dhabi, UAE
christina.poepper@nyu.edu

ABSTRACT

Mobility management in the cellular networks plays a significant role in preserving mobile services with minimal latency while a user is moving. To support this essential functionality the cellular networks rely on the handover procedure. Most often, the User Equipment (UE) provides signal measurements to the network via reports to facilitate the handover decision when it discovers a more suitable base station. These measurement reports are cryptographically protected. In this paper, we examine the cellular specification and illustrate that this crucial functionality has critical security implications. To the best of our knowledge, this is the first work on cellular Man-In-The-Middle attacks based on the handover procedure. In particular, we demonstrate a new type of fake base station attacks in which the handover procedures, based on the encrypted measurement reports and signal power thresholds, are vulnerable. An attacker who sets up a false base station mimicking a legitimate one can utilize the vulnerabilities in the handover procedure to cause Denial-Of-Service attacks, Man-In-The-Middle attacks, and information disclosure affecting the user as well as the operator. Therefore, users’ privacy and service availability are jeopardized. Through rigorous experimentation, we uncover the vulnerable parts of the handover procedure, a comprehensive attacker methodology, and attack requirements. We largely focus on the 5G network showing that handover vulnerabilities remain unmitigated to date. Finally, we assess the impact of the handover attacks, and carefully present potential countermeasures that can be used against them.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**; **Security protocols**; **Denial-of-service attacks**.

KEYWORDS

5G, LTE, Handovers, Denial-Of-Service, Man-In-The-Middle, False base stations

ACM Reference Format:
Evangelos Bitsikas and Christina Pöpper. 2021. Don’t hand it Over: Vulnerabilities in the Handover Procedure of Cellular Telecommunications. In *Annual Computer Security Applications Conference (ACSAC ’21), December 6–10, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3485832.3485914

1 INTRODUCTION

The 5$^{\text{th}}$ Generation (5G) of mobile telecommunications is gradually transforming the world. By the end of 2020 over 1 billion people, or 15 percent of the world’s population, were living in areas with 5G coverage [25]. 2G and 3G generations are in a process of progressive phaseout, since carriers need to re-use spectrum to enhance their networks and provide faster, more responsive technology to their customers. This means that newer networks will rely on the coexistence between 4G and 5G technologies.

One of the most critical elements of the cellular telecommunications is the mobility management and a principal part of it is the handover procedure. *Cellular handover* in mobile networks is a mechanism that retains the current session of the mobile terminal when a transition is required from one radio cell to another. It is a vital part of the Mobility Management with a goal to maintain Quality of Service, to not drain the UE battery power, and to provide service continuity with minimal handover latency. To facilitate this process, operators and organizations, such as the 3rd Generation Partnership Project (3GPP), introduced the Measurement Report (MR), which is a message containing frequency and power metrics to assist the network on deciding if a handover is necessary and which is the most suitable handover target station. The UE sends these messages to the serving base station when required or instructed. As a consequence, the handover procedure is heavily dependent on the content of the MR to assess the mobility status of a UE.

In terms of security, the MR messages are protected by the Access Stratum (AS) security context. Similarly, exchanged messages during a handover procedure are security protected, thus an attacker cannot manipulate or modify the messages directly. However, the content of the MR messages are never verified by the network to prove their legitimacy. Instead, they are considered trusted and the network proceeds with their evaluation. Consequently, if an attacker manipulates the content of the MR by including his/her measurements, then the network will process the bogus measurements. This is possible by imitating a legitimate base station and replaying its broadcast messages. So, when the UE is in the coverage area of the attacker, the rogue base station has high enough signal power to "attract" the UE and trigger a MR, then the attacker has very good chances of forcing the victim UE to attach to his/her rogue base station abusing the handover procedure. Once, the UE is attached to the attacker it could either enter in a camped mode due to a Denial-Of-Service (DoS) attack and become unresponsive,

ACSAC ’21, December 6–10, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8579-4/21/12…$15.00
https://doi.org/10.1145/3485832.3485914

or the attacker could establish a Man-In-The-Middle (MitM) relay building the basis for other advanced exploits. It is noteworthy that the attack has impact on the network side as well, as we will elaborate on later.

Recently, Shaik et al. [46] and the 3GPP's technical report [8] have briefly tackled handover implications in Self-Organizing Networks (SON) [10, 15]. They illustrate the idea that an attacker could potentially launch successful handover attacks against Long Term Evolution (LTE)'s X2 and 5G's Xn handover procedures, respectively. However, both works address this issue with limited levels of details and rather vague results, and they merely report two handover cases. Furthermore, the two works disagree when it comes to the Random Access Channel (RACH) completion that is required during a malicious handover: whether the RACH can be successfully completed or not.

In this paper, we tackle the fact that the security implications of the cellular handover are under-explored. We present the first comprehensive study of vulnerabilities in the cellular handover procedure. In particular, we explore the security weaknesses of the handover procedure in the presence of a rogue base station, we present a comprehensive attack methodology that can impact the cellular network in various ways, we experiment thoroughly to uncover the extent of affected handover cases, and reveal what types of attacks are feasible. In conclusion, we discuss potential detection and prevention handover countermeasures.

In more details, our contributions are as follows:

(1) We present a comprehensive security study on the handover procedure evaluating different handover types and presenting their similarities in terms of security. As far as we know, this is also the first study that investigates rogue base station effects on handover security in such depth.
(2) We demonstrate that vulnerabilities in the handover procedure are not limited to one handover case only but they impact all different handover cases and scenarios that are based on unverified measurement reports and signal strength thresholds. We also illustrate that the problem affects all generations since 2G (GSM), remaining unsolved so far.
(3) We perform an experimental validation for 4G (LTE), 5G Non-Standalone and 5G Standalone handover cases, where we evaluate the Intra- and Inter-Base station handovers and provide a detailed description of the experimental setup, the exact attack steps needed, and the achieved results. In addition, we describe and interpret the behavior of the UE and the network during a handover exploitation, taking into account a diverse range of cellular services and UE models.
(4) We specifically show that handover exploitation can lead to MitM attacks and sensitive data extraction, such as IMSI, apart from the usual DoS attacks. Furthermore, we clarify the impact of such attacks on the UE as well as on the network.

To the best of our knowledge, our work is the first study on the security of the handover procedure presenting experimental results for 5G from an advanced 5G Standalone and Non-Standalone setup.

Finally, we have discussed the vulnerability disclosure with GSMA as our work was submitted under the assigned tracking number CVD-2021-0051. GSMA is planning to use our results to improve the existing 3GPP specifications, remedy any inaccuracies and bolster 3GPP's security study against false base stations.

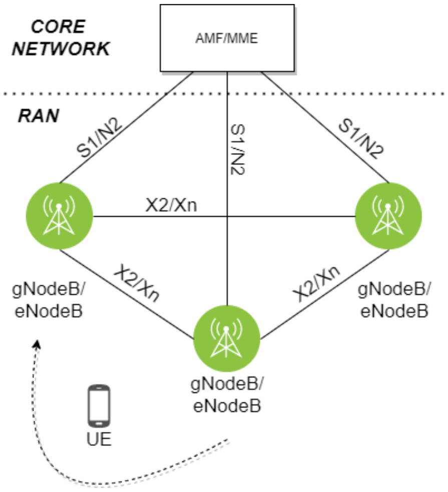


Figure 1: Abstract RAN architecture in LTE and 5G

2 PRELIMINARIES: MOBILE HANDOVER

Normally, the UE collects radio measurements based on two states: *idle* and *connected*. In idle state mode, the measurements are used for cell selection and cell re-selection. In connected state mode, the measurements are used for handover and redirection scenarios. In general, the UE is instructed to occasionally transmit measurement report messages to its source/serving base station.

Measurement reports consist of collected power and frequency measurements about proximal base stations. All the necessary information needed for the UE to conduct the measurements are accessible through the broadcasted System Information Block (SIB) and Master Information Block (MIB) messages of the base station. Upon receiving the messages, the serving base station evaluates them and decides if a handover procedure is necessary. In particular, if the link to the serving cell is getting degraded and/or another reported neighboring cell at a different frequency is getting better than the serving cell, the network may possibly move the mobile terminal connection from the serving cell to that neighboring cell, so the mobile terminal will get better radio conditions and consequently the operator will offer a greater user experience. This decision is actually based on mathematical calculations involving a triggering threshold [2, 3, 6, 18] that corresponds to an *Event*. Therefore, if the UE's values in the measurement report exceed the associated threshold, then a handover will be initiated by the source base station. Additionally, the measurements (RSRP, RSRQ, SINR etc.) may also facilitate inner-network processes and may be used for other calculations such as base station resource allocation. Figure 1 shows the UE's transition from one base station to another as the handover procedure takes place.

Trigger Events: The decision whether a mobile device will move to another station or not is made by the serving base station based on measurement reports from the mobile device. This holds for any technology so far (i. e., 2G, 3G, 4G, 5G). In ideal cases, a base station shall allow UE to report serving cell and neighboring cell signal quality and trigger the handover with a single measurement, but in practice it can create overload conditions due to unnecessary ping-pong handovers [26, 50]. As solution to avoid such situations, 3GPP specifications have proposed a set of predefined measurement report mechanisms, called *Events*, to be performed by the UE. The type of event a UE has to report is specified by the Radio Resource Control (RRC) signaling message sent by the base station. Section A (Appendix) illustrates these events in LTE and 5G.

Handover Phases: Before the handover procedure takes place, the UE is attached to the source base station with its established radio bearers. It is in RRC-Connected state (and registered state) and uplink/downlink data are relayed normally between the UE and the network. Then, the handover procedure consists of three phases:

(1) The *preparation phase* corresponds to the decision of handover, information exchange and resource reservation. The preparation phase begins when the decision is taken to execute a handover procedure after the UE's measurement reports.
(2) The *execution phase* corresponds to the mobile connection to the target eNodeB/gNodeB. It begins with the source base station sending the RRC Reconfiguration message to the UE.
(3) The *completion phase* consists of the establishment of final bearers and the release of the old resources. It starts when the UE transmits the RRC Reconfiguration Complete message.

2.1 Handover Classification

According to the specifications [5, 17], cellular handovers can be classified according to three primary factors, detailed as follows:[1]

Intra- and Inter-Base Station Handover: Base stations may be a gNodeB, eNodeB or BSS/RNC including their sub-types (en-gNodeB, ng-eNodeB, etc). Handovers can then be classified as *Inter-Base Station*, where the UE relocates to a cell belonging to a different base station, or *Intra-Base Station*, where the UE relocates to a different cell but operated by the same base station. Intra-Base Station handovers comprise a simple exchange of reconfiguration messages between the UE and the serving base station without adhering to the regular handover procedure. Also, this process lacks the need of a target base station, so we can completely distinguish it from Inter-Base Station. On the contrary, Inter-Base Station handovers follow the normal handover procedure. Inter-Base Station handovers need to be classified further in order to determine the target system that will handle the connection after the handover. Therefore, all the types below are mainly applicable to them.

Intra- and Inter-Core Network Handover: Core Network entities that handle authentication and sessions may also need to change leading to *Inter-Core Network* handovers. For example, the serving Access and Mobility Function (AMF in 5G) or Mobility Management Entity (MME in LTE) may need to change because the target base station belongs to another AMF or MME. *Intra-Core Network* handovers do not demand Core Network relocations because the target base station is under control of the current network, while *Inter-Core Network* handovers perform relocations because the target base station belongs to a different Core Network entity.

Core Network relocations always require the relocation of the entity that manages the access and mobility (such as AMF and MME) and controls the target base station. For instance, a relocation from a 5G Core Network to another is characterised as Inter-AMF handover because of this AMF shift. In fact, the terms Intra/Inter-Core Network are not necessary when we know the relocation state of the AMFs/MMEs/SGSNs. In cases where a Core Network may have more than one authentication and mobility management entity, it is possible for a UE to shift between them according to network needs. This means that an Intra-Core Network handover could also be Inter-MME or Inter-AMF.

Besides that, it is common for a UE to also change its assigned user-plane gateway and function. This may happen inside the same network or when the Core Network changes. For example, if the UE is assigned a new UPF within the same 5G network then we can define this handover as Intra-AMF Inter-UPF. This is applicable to any generation. Worth mentioning is the fact that this kind of relocation is neither transparent to the UE nor will it require any additional steps from UE's side during the handover, as the authentication and mobility management entity will complete this appointment directly. Exactly the same is applicable to the SMF function in 5G.

Intra- and Inter-RAT Handover: Finally, based on a distinction due to the Radio Access Technology, *Intra-RAT* refers to a handover destined for a target network entity that uses the same radio technology as the source network, while the *Inter-RAT* refers to a handover destined for a network entity that uses a different radio technology. For instance, an Inter-RAT handover is the EPS fallback from a 5G connectivity.

2.2 Special Handover Types

In addition to the presented normal handovers, the following special – subsumed – handover types exist, with related security concerns as we will demonstrate.

Conditional Handovers. According to release 16 [10] a Conditional Handover (CHO) is a handover that is executed by the UE when one or more handover execution conditions are met. The source base station sends the execution condition(s) to the UE through the RRC Reconfiguration and then the UE starts evaluating them. Once one of the conditions is fulfilled, a handover is executed. Also, after sending the RRC Reconfiguration message, the source base station prepares all potential handovers by sending handover requests to the candidate cell(s). The CHO configuration contains the configuration of the CHO candidate cell(s) generated by the candidate base stations and execution condition(s) generated by the source base station. The UE determines the best candidate based on the threshold using the typical signal metrics (e. g., RSRP, RSRQ, RSSI, SINR). Also, a candidate cell may be operated by the source or candidate base stations. Finally, an execution condition may consist of one or two trigger condition(s) (CHO events A3/A5, as defined in [7]).

CU-DU gNodeB Handovers (5G). In the 5G RAN architecture, the gNodeB has been split into smaller specialized units, the Centralized Unit (CU) and the Distributed Unit (DU). The CU is

[1] To make our evaluation more coherent, in this paper we also group the legacy technologies (2G and 3G) together as one unified system with a 2G/3G SGSN, MSC, BSS and RNC stations, especially due to their current phase out. Otherwise, these two generations hold different but connected Core and RAN networks.

Table 1: Inter-Base Station handover types.

		Target Network			
		Within the Source Network	5G RAN	E-UTRAN	UTRAN / GERAN
Source Network	5G RAN	Intra-RAT Intra/Inter-AMF Xn or N2	Intra-RAT Inter-AMF N2	Inter-RAT (with or w/o N26 interface)	Inter-RAT through SRVCC (Call only)
	E-UTRAN	Intra-RAT Intra/Inter-MME X2 or S1	Inter-RAT (with or w/o N26 interface)	Intra-RAT Inter-MME S1	Inter-RAT (with or w/o SGW relocation, direct or indirect tunneling)
	UTRAN/ GERAN	Intra/Inter RAT Intra/Inter SGSN A/Gb or Iu mode	—	Inter-RAT (with or w/o SGW relocation, direct or indirect tunneling)	Intra/Inter RAT Inter SGSN A/Gb or Iu mode

a logical node that includes gNodeB functions such as user data transfer, mobility control, radio access network sharing, positioning, session management etc., except from those allocated exclusively to the DU. In addition, the CU controls the operation of DU(s) over the front-haul interface. Contrariwise, the DU (also known as RRH/RRU/RE/RU) is a logical node that includes a subset of the gNodeB functions depending on the functional split option.

According to 3GPP [6] a handover may be Intra-gNodeB (Intra-CU) Intra/Inter-DU or Inter-gNodeB (Inter-CU) Inter-DU. This means that the target DU is either controlled by the same gNodeB or by a neighboring gNodeB, thus a CU relocation may be needed too.

3 THREAT MODEL

We consider an adversary that has the capacity to establish a MitM relay, which in turn may allow him/her to eavesdrop, drop, modify and forward messages transmitted between benign participants (e. g., genuine user equipment and base stations) in the public channel while adhering to the cryptographic assumptions. In addition, we consider an active adversary who can install and operate a base station with the same capabilities as a legitimate one. Specifically, the fake station can impersonate a legitimate base station and thus force a victim's device to connect to it by broadcasting MIB and SIB messages in the victim UE's frequency with a higher signal strength than the legitimate base station. We also make the assumption that the attacker is able to capture the MIB and SIB messages by eavesdropping the public channels. He/She may utilize any available equipment to carry out attacks. Finally, we assume that the adversary cannot physically tamper the SIM card, base station, or the Core Network to obtain the sensitive information, e. g., cryptographic session keys, and we consider side-channel and signal jamming attacks as out of scope.

4 OVERVIEW OF THE ATTACK

In this section we describe the holistic view of our attack. We propose a methodology that focuses not only on exploiting the handover procedure, but also on avoiding easy detection. First, we define all possible handover cases that an attacker should take into consideration while preparing for the attack. Then, we specify the necessary steps to complete the attack.

4.1 Defining the Handover Cases

In Sections 2.1 & 2.2, we described the types of handover and clarified in which each handover can be classified according to its relocation, radio access technology, etc. In this section, we go one step further and determine the concrete cases resulting from the classification. An attacker can make use of these cases to have a better understanding of the victim network. Thus, by putting the classification into practice, beginning from the latest radio access technology to the earliest, we identify the primary Inter-Base station handover cases as presented by Table 1.

Moreover, the selection of interface that is based on the Core Network's involvement during the handover is essential. If a direct communication between the source and target base station can be utilized (X2 in LTE and Xn in 5G), then the Core Network will not be involved. However, when a direct connection is not enabled (or due to failures or Inter-AMF/MME handovers), the authentication and mobility management entity of the Core Network must manage the handover. Therefore, base stations must communicate through the authentication and mobility management entity (S1 in LTE, N2 in 5G). Figure 5 shows very briefly how the interface decision is made based on the specifications [2, 7, 10, 14]; Figure 1 illustrates the established interfaces between network entities in LTE and 5G.

Finally, apart from the Intra-Base Station handovers that belong to another distinct category, we also take into account the conditional and the Intra/Inter-DU handovers from Section 2.2 that may apply to either Intra- or Inter-Base station handovers.

4.2 Attack Steps

1. Initial Reconnaissance. Gathering sufficient intelligence in the cellular environment is possible through passive sniffers that collect broadcast messages as well as UE traffic. An attacker that aims to exploit the handover procedure must be able to capture the MIB and SIB messages of the network (e. g., using inexpensive hardware like USRPs). An additional way to boost network scanning is to use the publicly available IMSI-catcher detection applications. Thus, an attacker may utilize his/her smartphone device to collect data related to nearby legitimate stations and use them to configure a rogue base station, thus reversing the applications' intended purpose.
2. Determining the Network Structure. Knowledge about the network composition allows to choose the most suitable target to attack. Thus, through the collected traces the attacker is able to locate

the legitimate base stations and determine their parameters. To create an adequate representation of the network structure we deem important to use the location, Cell Identifier, Tracking Area Identity (TAI) which includes the Mobile Country Code (MCC), Mobile Network Code (MNC) and Tracking Area Code (TAC), Absolute Radio Frequency Channel Number (ARFCN), the associated operators/providers and the supported services like 5G and LTE for each available base station. The attacker may continuously scan the network for configuration changes in order to remain updated.
3. Selecting the Target. Given sufficient information about the network, the attacker can decide which base station to imitate. We separate this process into three phases. Since the attacker's objective is to lure UE victims to connect to a rogue base station and disconnect them from their source/serving base station, as a first phase, the attacker will determine which source/serving base station and cell to impact. Second, the attacker will construct its potential neighboring list based on the obtained network data. To form a more accurate neighboring list the attacker may also leverage his/her malicious UE to participate in one or multiple UE-assisted Automatic Neighbor Relation (ANR) processes, which is a feature of the Self-Organising Networks [10, 15]. Finally, the attacker will choose to emulate a base station that is included in the estimated neighboring list of the serving base station. The benefit of preferring a base station from this neighboring list is that the adversary uses a legitimate base station with right parameters and close-to correct location. Alternatively, invalid parameters like wrong Cell Ids, excessive X2/Xn connections and abnormal locations may hamper the handover attack. In such a case, either the source/serving base station will not be able to complete the preparation phase of the handover or detection becomes easier.
4. Configuring the False Base Station. Before executing any handover attack the adversary needs to set up his/her base station correctly. The false base station should be able to replay the latest MIB and SIB messages of the emulated station and cell. Nonetheless, replaying just the broadcast messages is not enough. In fact, the attacker must configure the malicious base station appropriately based on the Cell Identifier, TAI, dl_ARFCN (downlink), PRACH Root Sequence Index and type of service.

Then, the attacker will gradually increase the signal power of his/her station to "attract" the UEs and force them to report bogus measurements to the network. If these false measurements eventually succeed in triggering a handover event, then the attacker can cease increasing the signal power and focus on the handover exploitation itself. Finally, the false base station should also have the capability to normally interact with the victim UEs meaning that it should be able to receive and respond to RACH, RRC and NAS messages using open or closed source software.
5. Handover Exploitation. The attacker's decision on selecting the most convenient base station to mimic determines also the handover cases that he/she can exploit. For instance, the choice to mimic a legitimate LTE eNodeB limits the exploited cases to the LTE domain for Intra/Inter Base station handovers. Of course, a more powerful attacker could leverage more false base stations covering multiple services and generations, thus increasing the number of affected handover cases and the impact. Nevertheless, it is prudent for the attacker to always pay attention to unsupported services, since they can expose him/her to the operator.

In our work, we provide evidence that the defined cases in Section 4.1 are vulnerable. All of them share the same security weaknesses; thus an attacker that adheres to the aforementioned attacking methodology can potentially launch successful handover attacks. The attacker's main objective is to make UEs attach to his/her malicious cell with detrimental results. The next sections cover the vulnerabilities and the handover exploitation comprehensively.

4.3 Identifying the Vulnerabilities

We next explore the handover security flaws and deficiencies based on the specifications. Our approach is sequential, starting from the pre-handover, concluding with post-handover weaknesses. In addition, vulnerabilities A to D are mainly inherent to the specifications, whereas E and F are primarily operator-specific.
A. Insecure Broadcast Messages: The SIBs and MIB of a base station that are necessary for the UEs in order to connect to the network are broadcasted without encryption, integrity-protection, and authentication. As a consequence, anyone with the proper equipment can intercept and replay broadcasted traffic related to legitimate base stations. The lack of a Public Key Infrastructure scheme [30] that could be used to sign these messages gives the attacker the chance to setup a false base station and exploit the handover procedure.
B. Unverified Measurement Reports: MRs include signal information of nearby stations. These measurements are evaluated by the source/serving base station to determine if a handover is required. Even though the MR is an RRC message protected by the AS security context, its content is never verified by the network. To be precise, the source base station is unable to detect abnormal values in the measurement report meaning that in case of false Cell Identifiers, incorrect Tracking Area Codes, incorrect PLMNs, unsupported services, and wrong network topology, the source base station will still accept the MR. Consequently, a malicious handover remains undetected during the handover decision at the preparation phase. Furthermore, the MR lacks extra values that could be used for security purposes, such as MIB/SIB hashes and location coordinates.
C. Missing Cross-Validation in Preparation Phase: The preparation phase incorporates also the communication between the source and the target base station that is needed to arrange the handover. This can either be fulfilled through a direct channel interface or through a Core Network interface. However, regardless of the interface, the procedure lacks a cross-validation of the values included in the MR. In fact, there is no way for the the target base station to verify if the handover derives from itself (a legitimate entity). Instead, the source base station immediately sends the Handover Request (or Handover Required) and the target base station goes through the process of admission control. A cross-validation mechanism could be used to detect inconsistencies in the values reported by the UE compared to the real values of the target base station, mostly if extra security values are going to be included in the MR.
D. RACH Initiation without Verification: Once the preparation phase is completed, the source base station immediately instructs the UE to connect to the target base station by sending the RRC

Connection Reconfiguration message. The UE blindly initiates the RACH procedure and attempts to send the RRC Connection Reconfiguration Complete to finalise the new attachment. These messages that belong to the execution phase can lead to malicious attachments since the UE's perspective of the target base station is different from the network's. Therefore, besides of the unsubstantiated measurement reports, the problem is amplified by the fact that the network has the tendency to trust the UE without acknowledgements or supervision. In addition, the RRC Connection Reconfigurations are not designed to inform the UE that the target base station is legitimate.

E. Missing Recovery Mechanisms: The network functions lack a proper recovery mechanism so the UE can safely connect back to the legitimate base station in case of a failure. When a UE is maliciously camped, it periodically tries to reconnect to the network through the rogue base station using the RRC Connection Reestablishment messages, Service Requests and Attach requests. This means that in cases of failure, the UE is not intended to validate its serving base station. Hence, the real network can only wait for the UE to reconnect and rely on its post-failure Radio Link Failure (RLF) reports. On top of that, the malicious base station has the ability to ignore, reject or forward messages to the legitimate network when the UE attempts to reconnect.

F. Difficulty of Distinguishing Network Failures from Attacks: Finally, the specifications do not include any dynamic post-detection mechanism that would leverage the network topology, its configurations, the UE RLF and measurement reports, missing RRC and NAS responses and network failures (X2/Xn connection errors, timer error, etc) in order to reveal potential malicious activities. In fact, the network is not sufficiently designed to distinguish failures caused by security issues from prevalent network causes. Therefore, it incorrectly invokes regular recovery and optimization functions (e. g. OAM) to solve security issues, which may lead to additional damages.

5 EXPLOITING THE HANDOVER

Dependence on measurement reports and signal strength started from the early legacy technologies with 2G and 3G [1, 10, 13], meaning that the problem is not new and remains unmitigated. Surprisingly, not only LTE, but also 5G is affected even though it is considered more secure. In this section, we present our findings regarding the handover exploitation, by illustrating how handover attacks can take place.

5.1 Intra-Base Station Handovers

In this part we describe the general form of the Intra-Base station attack which applies to LTE and 5G, see Figure 2. The figure also shows the exploited weaknesses represented in red circles according to Section 4.3.

Initially, the UE transmits and receives traffic as normal while being in an RRC-Connected state. Normal traffic is related to a service that could be a voice call, data, SMS exchange, etc. The duration in which the UE remains in the RRC-Connected state varies and it chiefly depends on the configured RRC inactivity timer. Furthermore, the source and target cells belong to the same eNodeB/gNodeB. An attacker that emulates the target cell tries to disrupt the normal traffic and execute a handover attack that will make the UE attach to the malicious cell.

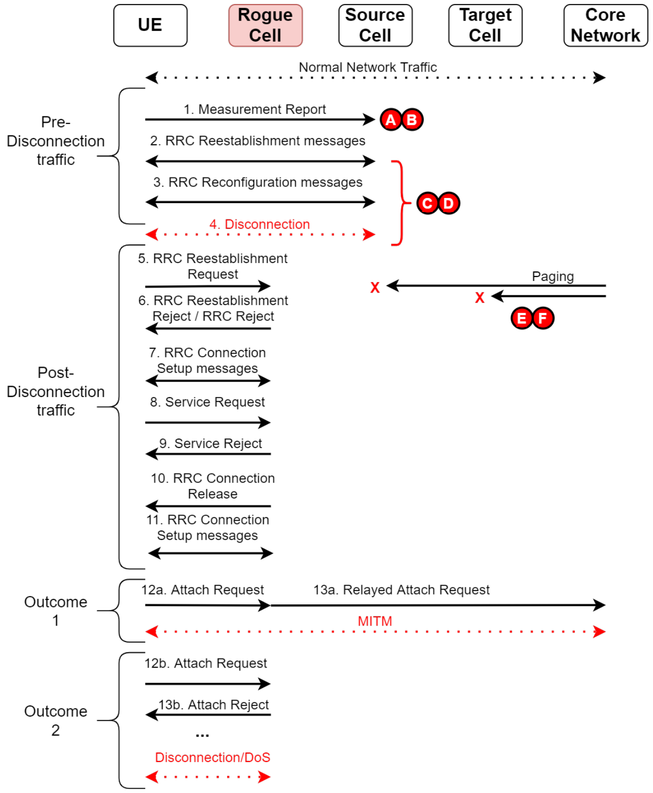

UE
Rogue Cell
Source Cell
Target Cell
Core Network
Normal Network Traffic
Pre-Disconnection traffic
1. Measurement Report
A
B
2. RRC Reestablishment messages
3. RRC Reconfiguration messages
C
D
4. Disconnection
Post-Disconnection traffic
5. RRC Reestablishment Request
6. RRC Reestablishment Reject / RRC Reject
Paging
X
X
E
F
7. RRC Connection Setup messages
8. Service Request
9. Service Reject
10. RRC Connection Release
11. RRC Connection Setup messages
Outcome 1
12a. Attach Request
13a. Relayed Attach Request
MITM
Outcome 2
12b. Attach Request
13b. Attach Reject
...
Disconnection/DoS

Figure 2: Intra-Handover attack

Once the MR is sent to the source cell containing false measurements about the target cell, the source cell will wrongly accept it and initiate a series of RRC Reconfiguration messages and possible RRC Reestablishment messages to synchronization purposes as presented in steps 2 and 3. The reason behind this potentially lengthy exchange of RRC messages is that the attack destabilizes the connection and the transition from the source cell to the bogus cell becomes turbulent. Ideally, to synchronize to a target cell in Intra-Base station handovers, a single exchange of RRC Reconfiguration and RRC Reconfiguration Complete messages is adequate. Finally, the UE will disconnect from the source cell and initiate a connection to the false cell. The disconnection happens immediately after the UE receives an RRC Reconfiguration message, which signifies the lack of cross-validations on the network side. Then, the source cell may notify the MME/AMF about the abnormal disconnection of the user by sending a UE Context Release with cause "Radio Connection with UE lost", as also shown in Figure 8. It should be specified that in most cases the RAN network may experience a handover *T_RELOC_OVERALL* timer expiry close to the moment of disconnection too.

Thereafter, the UE will begin the attachment with an RRC Reestablishment Request (step 5). The reestablishment cause is usually a *handoverFailure* or *otherCause* since the UE cannot properly attach to the rogue cell, especially through the intended RACH procedure.

Figure 6 shows such an RRC Reestablishment Request. In this case, an RRC Reestablishment Reject/RRC Reject (step 6) can make the UE begin a new RRC Connection Setup (step 7) normalizing the connection. On the side of the Core Network, the UE appears to be deregistered in an abnormal way, therefore paging messages may be sent from the Core Network to all available cells, in order to locate the user. However, these messages will fail since the UE is attached to the attacker. Once the new RRC connection is ready, the UE attempts to quickly recover the disrupted service because of the attack by transmitting one or multiple Service Request messages (step 8). The attacker must reject the service (step 9), since not only Service Accept messages are security protected and the attacker does not possess the UE Security Context, but also he/she cannot offer legitimate services to the users.

Moreover, considering that the attacker would want to achieve a stable and exploitable connection with the UE, after a series of failed service recoveries, he/she can leverage a compelling RRC Connection Release with *waitTime* 1 second in order to make the UE connect anew (step 9). Consequently, in all of our experimental attempts, we noticed that the UE promptly reconnects with an RRC Connection Setup and sends an NAS Attach Request to the attacker (steps 11 and 12). The UE believes that the Attach Request will be received by the legitimate Core Network through a legitimate base station, but this is not the case.

Given the above steps, the attacker has two options based on his/her goals: Either forward the Attach Request and all the following downlink and uplink traffic in order to establish a MitM relay, or perform a DoS attack by responding with an Attach Reject. According to our assessment, the UE enters into a DoS mode after a few attach rejections without recovering. A reboot or airplane mode is necessary, even though the UE also needs to "escape" the attacker's coverage. Finally, it should be mentioned that the UE-initiated messages are sent on the attacker's side along with sensitive data such as the IMSI, TMSI and UE capabilities. IMEI/PEI could also be exposed if the UE is instructed by the malicious network to authenticate with the equipment identifier. Therefore, user's private information are invaded too.

5.2 Inter-Base Station Handovers

Akin to the Intra-Base station cases, we now determine the general form of Inter-Base station handovers on LTE and 5G, see Figure 3. We include the S1/X2 (Intra-RAT), N2/Xn (Intra-RAT), and EPS fallback (Inter-RAT) handover cases. Once again, we start by having a UE in RRC-Connected state with a normal network communication. Nonetheless, the source and target cells now belong to different eNodeBs/gNodeBs. Thus in this scenario, the attacker emulates the target cell of a target eNodeB/gNodeB.

Upon receiving the fraudulent MR, the source cell checks if the measurements meet the handover trigger threshold, then the source eNodeB/gNodeB searches the Neighbour Cell Relation Table with the reported PCI, and finds the target cell of the target eNodeB/gNodeB. The source cell believes that this PCI applies to a legitimate base station and proceeds with the handover preparation phase in step 2, however the PCI is associated with the rogue cell from UE's viewpoint. The general structure of the preparation phase is very similar to the aforementioned cases, with few differences. In X2 and Xn, there is direct link of communication between the base stations; therefore a Handover Request and a Handover Acknowledgement are sufficient. In cases where there is no direct link, like in S1, N2 and EPS Fallback, the traffic goes through the MME/AMF, beginning with a Handover Required message. In any case, the source cell tries to prepare the target cell for the handover, and when ready it sends an RRC Reconfiguration message (HO Command) to the UE to force a handover (step 3). In spite of that, the UE disconnects from the source cell and connects to the false cell due to the lack of verification mechanisms. Additionally, it is possible that the source cell will send a UE Context Release due to disconnection like in Intra-Base station handovers. Finally, when the attack affects UE's communication and destabilizes it, the source cell may cancel the handover procedure during the preparation phase more than once. Once again, this is an indication that a smooth transition might not be conceivable leaving traces behind.

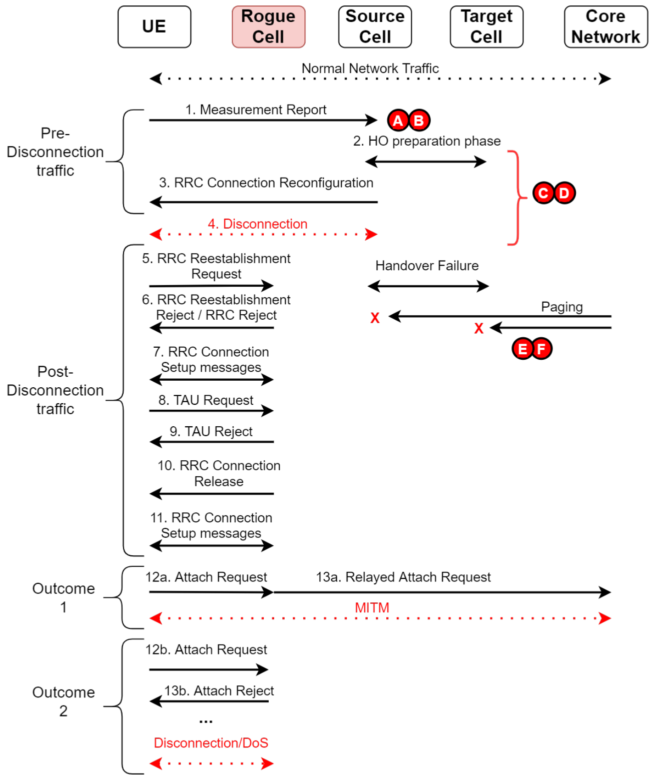


Figure 3: Inter-Handover attack

Similar to Section 5.1, the UE attempts a connection to the rogue cell with an RRC Reestablishment Request (step 5) and the attacker responds accordingly (step 6). Next, the UE initiates an RRC Connection Setup with the malicious cell to retain attachment (step 7). In LTE, the UE also sends two to three NAS TAU Requests that are declined by the attacker (steps 8 & 9). A rejection cause that can be used in TAU reject messages is the "UE cannot be derived by the network" which will force the UE to connect anew. To amplify this result an RRC Connection Release message *waitTime* 1 second is a suitable option as shown in step 10. The attacker should also reject any Service Requests sent by the UE, even though we did not detect any such message during our experimentation, since any service has been dropped by now. On the network side, a handover failure occurs because the real target cell did not complete the intended RACH procedure with the UE and the source cell did not receive the UE Context Release from the target cell. Eventually, the Core Network may transmit paging messages to locate the user who is missing, hoping for an RLF report that will match the registered handover failure but not until the UE reconnects to it.

Thereafter, the UE begins a new RRC connection with the rogue cell and sends a NAS Attach Request in order to freshly register (steps 11 and 12). Once again, the UE's false trust has consequences identical to Intra-Base station cases. The attacker can forward messages to establish a MitM relay or reject the attachment forcing a DoS attack. Similarly, privacy issues are still present as the UE sends sensitive information to the attacker during the whole process.

5.3 Special Handover Cases

Likewise, special handover cases are designed with the same security flaws. In CU-DU handover cases, the principal factor for a transition from a source CU/DU to a target CU/DU is once again the MR [6]. As a DU may control one or more cells and the handover procedure remains the same, we suspect that Intra/Inter-CU and Intra/Inter-DU handovers can be affected similar to the Intra- and Inter-Base Station handovers presented above.

Conditional handovers [10] rely on the UE to make the decision on which target cell it should attach to. The source base station provides the trigger events and thresholds to the UE via the RRC Reconfiguration message while it prepares the candidate targets for a potential handover. If the UE discovers a trigger event and a suitable cell based on its measurements, then it initiates the execution phase of the handover and establishes a connection. This means that this process is still based on MRs and signal power, therefore we believe that the attacks can be carried out in the same fashion as previously. The difference here is the UE which sends an RRC Reconfiguration Complete to the source cell right after receiving the RRC Reconfiguration message and before disconnection.

6 EXPERIMENTATION

6.1 The Setup

As Figure 4 shows, our setup consists of computer ① which is the Amarisoft Callbox Classic (equipped with SDRs) [19] with the EPC/5G Core Network and the eNodeB/gNodeB representing the legitimate network. In addition, we have computer ② with another legitimate Amarisoft eNodeB/gNodeB using a Lenovo Thinkpad T580 laptop with Ubuntu 20.04 and an Ettus B210 USRP [41]. The two computers are connected in the same network via Ethernet and their cellular interfaces are set according to Amarisoft documentation. For the UE, we used the Oneplus 6, Apple iPhone 5, Samsung S10 5G and Huawei Pro P40 5G with an Anritsu sim card. Furthermore, the attacker's machine comprises a Dell Latitude E5450 laptop with Ubuntu 20.04 and an Ettus B210 USRP with a total cost of 2k €. In our setup, the attacker can use srsLTE for LTE cases and Amarisoft software for the LTE and 5G cases with a Core Network and a single eNodeB/gNodeB. More details about our cellular network configurations are presented in Section D of the Appendix.

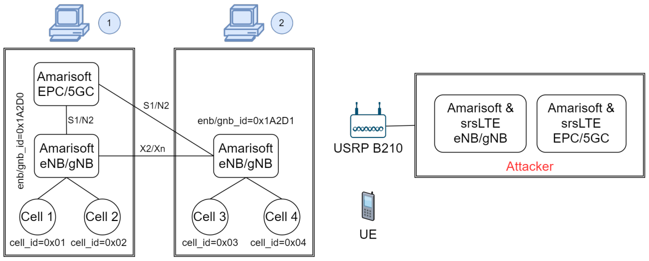


Figure 4: Our experimental setup

6.2 Requirements, Scenarios, Target Handovers

In our experimentation we emulated three scenarios where the UE is in RRC-Connected state and interacts normally with the network. The first one was a data transfer through iperf [34] as suggested by the Amarisoft documentation, while the second one was a regular IP Multimedia Subsystem (IMS) SIP call service and a third one was the Short Message Service (SMS). For iperf we had to initiate a server/receiver on the network side and a client/sender on the UE side while the mobile data were enabled. Moreover, IMS calls were possible through the IMS terminal by carrying out the *mt_call* command and SMS messages through the *sms* command.

We applied the above scenarios to LTE, 5G NSA and 5G SA, while using all four smartphones for LTE, Samsung S10 and Huawei P40 for 5G NSA, and Huawei P40 for 5G SA. Unfortunately, we were not able to experiment on Inter-RAT cases that involve 2G (GSM) and 3G (UMTS), and on the special handover cases described in Section 2.1, since the former would result in a very complex and unreliable Core Network interworking that includes 2G/3G, and the latter is not supported by any software so far.

Next, we will present our experimental details for Intra- and Inter-Base station cases. We assume that the attacker has completed the reconnaissance and proceeds to the actual exploitation.

6.3 Executing the Attacks

For Intra-Base station cases we used eNodeB/gNodeB 1 cell 2 as a target while the UE was stationed at eNodeB/gNodeB 1 cell 1 having a normal connection. Once we configured the malicious station as cell 2, we launched attacks based on the three distinct scenarios; data transfer, IMS SIP call, and SMS messages. The callbox was configured based on the Amarisoft software, while the attacker used srsLTE and Amarisoft for LTE and only Amarisoft for 5G. Using two different software whenever possible allowed us to have a more accurate understanding about UE's behavior during the attack.

At the moment of the attack, we increased the signal power of the false base station while the signal power of cell 1 was slightly decreased to imitate a handover procedure. To achieve this we used the command *cell_gain*. Immediately the UE, not been aware about the presence of a false cell 2, informed cell 1 through MRs about a strong signal coming from cell 2. Cell 1 wrongly accepted the measurements believing that they are related to the legitimate cell 2 and processed them. Figures 9 and 10 show examples of a malicious MR in LTE and 5G respectively containing false power measurements. Since the attack may achieve a discontinuous transition to the false cell in many cases, multiple MRs to the network with bogus measurements, RRC Reestablishment and Reconfiguration messages may be exchanged before the disconnection.

Eventually, the UE was forced to disconnect from the legitimate base station station and attached to the attacker. We configured the attacker to respond with reject messages whenever the UE was sending RRC Reestablishment Requests, TAU Requests or Service Requests, while allowing RRC Connection Setup Requests. Furthermore, an RRC Connection Release was used to force the UE into sending Attach Request without fully disconnecting from the attacker.

In the end, the UE attempted to attach to the false base station with an Attach Request. As a consequence, not only the UEs revealed sensitive information, but also there were indications of MitM attacks. Therefore, the attacker could establish a MitM relay between the UE and the Core Network. The way to perform this task is to have an SDR that emulates an eNodeB/gNodeB towards the affected UE and another SDR that emulates the UE towards the Core Network as presented in [44]. Alternatively, the attacker can still DoS the UE in this scenario as well by responding with NAS Attach Rejects. We observed that after a few NAS Attach Reject messages the UE was completely deprived of services remaining in a DoS state.

For Inter-Base station testing, we further separated this category into Intra-RAT and Inter-RAT handovers according to our prior classification in Section 2.1. The setup for Intra-RAT handovers, which consist of X2, S1, Xn and N2 types, contained the source and the target cell that were placed on different base stations, thus different computers. The UE was stationed in cell 1 and tried to transition from cell 1 to cell 3. Hence, the attacker tried to abuse the handover by emulating cell 3. Whereas for Inter-RAT handovers, Amarisoft software allowed us to run an LTE cell 1 and 5G NR cell 2 in computer ① without the need for computer ②. These cells had a separate virtual base station while an EPS fallback was possible through handover. The attacks were executed in the same manner as for Inter-Base station cases. Figure 11 shows the exploited EPS fallback on the Core Network and RAN.

6.4 Traffic Variations due to Service & UE Model

We tested the handovers on data transfer, IMS call and SMS scenarios and we observed varied UE behaviors. In theory, services with causes such as mo-VoiceCall, mo-Signaling, mo-Data, mo-SMS belong equally to a zero Access Identity (AI) which is below the Priority Access. However, an interrupted IMS SIP call was perceived more important by the UEs, since they immediately tried to recover the call by quickly attaching to the false base station. During the first RRC Setup messages (step 7 in Figures 2 and 3) UEs sent many RRC Setup Requests with cause mo-VoiceCall, while in other cases like data transfer with a cause mo-Data and SMS exchange with a cause mo-SMS a more relaxed behavior was observed. Figure 7 (Appendix) shows an RRC Setup Request with mo-VoiceCall as cause during the attack.

Table 2: Device Specifications and Results. All devices have IMS & Internet as configured APNs.

Device	Chipset	OS	Model	Release	MitM Susceptibility	DoS Susceptibility
Huawei P40 Pro 5G	Huawei Kirin 990 5G	Android 10	ELS-NX9	2020	High	High
One Plus 6	Snapdragon 855	Android 10	One Plus A6000	2019	High	High
Samsung Note 10 5G	Snapdragon 845	Android 10	SM-N976Q	2018	Medium	High
Apple iPhone 5	Apple A6 (32 nm)	iOS 10	A1428	2012	Medium	High

Likewise, through experimentation we realized that not all smartphones behave the same. Therefore, the attacks may not only depend on the service but also on the smartphone model. The next sections describe our equipment more thoroughly and Table 2 shows the smartphone specifications. Huawei P40 had a tendency to quickly establish a balanced connection during the attack (on LTE and 5G), especially in case of a voice call. Therefore, a MitM was more effective apart from an Attacker-initiated DoS. Oneplus 6 presented similar behavior, even though it produced a few unstable connections that made it susceptible to a UE-initiated DoS. Finally, Samsung S10 and iPhone 5 showed more instability since in every scenario they were more adamant to hold the connection with the source cell.

6.5 Countermeasures

There is a plethora of research works [23, 24, 36, 38–40, 51] that investigate the detection capabilities of the network and UE trying to determine the best indicators that when combined will reveal the presence of a false base station. However, these conventional detection mechanisms as mobile application or network listeners cannot prevent handover attacks, since the UE is not capable of enforcing security measures against malicious base station by itself and since the attack will probably be detected after its completion. On the contrary, the attacker can leverage these applications with his/her malicious UE to assist his/her network reconnaissance. On the other hand, we believe that a combination of enriched measurement reports [4, 8, 11, 37] by placing the detection at the preparation phase of the handover, Public Key Infrastructure to sign the broadcast messages [49] and encrypted system queries (they reveal if the current base station possesses the AS Security Context proving its legitimacy) [4] before every reconnection attempt constitute for a resilient handover procedure.

6.6 Ethical Considerations

Our experiments were carried out in an isolated environment without affecting other users, legitimate services, or real operators. Also due to the pandemic, the surrounding areas were empty, while the experimentation range was confined within 10 meters.

7 IMPACT OF THE ATTACK

The presented handover attacks can impact both the UE and the network. We elaborate on their impact as follows.

7.1 Impact on the UE

UE's inability to recognize a malicious from a genuine network, insecure broadcast messages and the unverified MRs give the attacker the chance to exploit the handover procedure. Taking this into account, the attacker has two options; either let the messages fail or respond with reject messages to DoS the user, or forward the messages to the real network to establish a MitM relay.

In the former case, the attacker can lock the UE in a complete DoS state while it will remain camped at the false cell. As a consequence, the user will lose its connection to the network and any available service (calls, internet connection, etc). Moreover, through the several attempts to recover the connection and due to state transitions (from Registered to Deregistered and vice versa, from RRC-Connected to RRC-Idle/Inactive and vice versa), its battery life will drain and its power consumption will increase.

On the other hand, the harmful effects of a MitM relay, in which UE traffic could be monitored and altered, has already been examined by past works. A MitM can lead to loss of confidentiality, integrity and to information leakage. For instance, an attacker may launch additional attacks by downgrading to a vulnerable 2G/3G connection or leveraging unprotected RRC and NAS messages to get sensitive data (e. g., IMSI, IMEI) as in [31, 35, 42]. Furthermore, modifying messages and manipulating the user-plane traffic [43, 44] might also be possible after UE reattachment to the genuine network. Of course, all these scenarios require the attacker to be able to sufficiently reach the UE while it moves and to have sufficient time to execute them.

It should also be noted that the attacker does not possess neither the AS nor the NAS Security Context, thus he/she cannot replicate legitimate services. Eventually, the UE will reattach to the network as normal and send an RLF report including the spoofed eNodeB/gNodeB IDs that caused the failure. Nevertheless, we consider handover attacks a highly critical security concern that may also have evident impact on the network as the next section explains.

7.2 Impact on the Network

The UE is not the only entity affected by the attacks, the impact is substantial for the network as well. The network wastes its resources if a malicious base station triggers a handover, because the UE will attach to the false base station and the network will wait for acknowledgement responses. Eventually, the timers will expire and the whole preparation will be rendered futile.

The ANR and the PCI optimization functions in LTE [16] are also impacted according to [46]. In the case of a handover attack, the genuine base station will be forced to search and get X2/Xn IPs in order to establish redundant X2/Xn connections between base stations, resulting in flooding scenarios that may lead to performance degradation.

In addition, the malignant use of PCIs that already exist will result in PCI collisions and confusions, and consequently to incorrect handovers and cell outages. Erroneous handovers not only can disrupt the network equilibrium at the moment of the attack, but may also have lasting effects for the afflicted base station. A base station that has a handover success rate lower than 95% may be disconnected (and blacklisted) from the network until it is recovered [46, 50]. Cell outages are possible because the PCI optimization procedure will be invoked to reboot the affected base station in order to renew its PCI. Similar functionalities can be observed in 5G networks [9, 12] which may introduce issues depending on the implementation.

7.3 Further Discussion

We report on further important details based on our experimentation.

Are forced/blind handovers affected by handover attacks? Forced/Blind handovers are used when the network needs to move the UE from one cell to another immediately without the use of an MR. Even though an attacker cannot manipulate this handover directly due to MR absence, he/she might block this handover from happening in the first place. According to our experiments, if the attacker's signal power is high enough even milliseconds before the handover takes place, he/she can impose malicious attachment causing handover failures on the network side. The results of such an attack could be similar to the typical handover cases. We were able to replicate the blind handovers by having the Intra-Base station setup as described earlier and by using *handover* command on the Amarisoft eNodeB/gNodeB terminal.

Does the UE fail to connect to the malicious base station during the initial HO RACH? Synchronization and successful RACH procedure are vital components of the handovers. Otherwise, the UE will not attach appropriately to its new base station or cell leading to errors. The attacker cannot offer the required smooth transition during the attack, even though he/she emulates the legitimate base station as precisely as possible. Nonetheless, we noticed that this issue does not affect the attack considerably, since the UE will still try to communicate and attach to the false cell. The attacker can DoS or perform MitM in most cases regardless of this initial abnormality.

Is there any real-time detection mechanism? Attachment to the malicious base station is not always as smooth as it is presented in theory. A handover attack may succeed but it is also likely to fail and most importantly leave traces related to abnormal traffic. One example is when the UE exchanges multiple RRC Reconfiguration messages with the source base station before disconnection. A detection mechanism placed in the RAN network can easily evaluate the traffic and easily identify inconsistencies (handover failures, timer expiration, unnecessary messages, etc), especially with the use of machine learning models. In addition, each eNodeB/gNodeB holds a record of temporary identifiers for each UE with the form: $\{RAN\_UE\ NGAP\ ID, AMF\_UE\ NGAP\ ID, Cell\ ID, RNTI\}$ in 5G and $\{eNB\_UE\ NGAP\ ID, MME\_UE\ NGAP\ ID, Cell\ ID, RNTI\}$ in LTE. We noticed that during an attack the list of records can be abused containing inconsistent values, short ID lifetimes and unnecessary records related to the affected UE due to traffic instability.

8 RELATED WORK

We have repeatedly witnessed serious vulnerabilities that affect 5G's predecessors [27, 31, 42, 44, 45], but also 5G itself [20, 47], even though its security baseline is more robust. Security flaws have been uncovered regarding various network components, such

Table 3: Overview of rogue base station attacks in academic literature.

Reference	Focus	Results/Impact	Generations	Year
Our Handover Attacks	General/Multiple Handover Procedures	MitM, DoS, Information Disclosure	2G-5G	2021
Shaik et al. [46]	X2 Handover Procedure	DoS	4G	2018
Rupprecht et al. [43, 44]	Layer-Two Protocols, User-Plane Exploitation	Privacy and Confidentiality issues, MitM	4G	2019/20
Borgaonkar et al. [21]	AKA hijacking	Privacy issues (User Localization)	3G-5G	2019
Shaik et al. [47]	Device Capabilities	Privacy issues (Device Identification), Service Downgrade, Battery Draining	4G-5G	2019
Hussain et al. [32]	Paging Procedure	Privacy issues, IMSI Cracking	4G-5G	2019
Hussain et al. [33]	RRC and NAS Protocols, Paging Procedure	Service Downgrade, DoS, MitM, User Tracking, Battery Draining	5G	2019
Kim et al. [35]	RRC and NAS messages	Privacy issues, DoS, MitM	4G	2019
Chlosta et al. [22]	Attach Procedure, Cryptogr. Misconfigurations	MitM, Impersonation	4G	2019
Hussain et al. [31]	Attach, Detach and Paging Procedures	Privacy issues, DoS, MitM	4G	2018
Shaik et al. [45]	Attach and TAU Procedures, Passive sniffing, Active Sniffing (MR and RLF)	Privacy issues (User Localization), MitM, DoS, Service Downgrade	4G	2016

as the authentication mechanism [21], the unprotected RRC and NAS messages [35], the insecure roaming protocols (e. g., Diameter and SS7) [29] and the unencrypted sensitive information (IMSI, IMEI, etc.) [24, 39]. Therefore, the system is vulnerable to an extensive number of attacks that can range from passive network scanning and IMSI catching to active exploitation. Furthermore, the capability of the attacker to setup false base stations using inexpensive hardware [45], transmit at cellular radio frequencies, replay legitimate broadcast messages, and interfere with unprotected cellular procedures makes it easier to discover and exploit weaknesses. Yang et al. [52] investigated the physical-layer exploitation of the pre-authentication traffic on LTE using mainly injections and signal overshadowing. For handover specifically, [46] and [8] have reported some elementary results on handover attacks indicating that an attacker can take advantage of the unverified measurement reports on X2 and Xn handover cases, respectively. Proper key management has been explored [28], but it remains inadequate since our proposed attacks circumvent LTE's and 5G's encryption and integrity-protection altogether like in the measurement report.

Table 3 presents false base station attacks, their focus and impact in the related academic work.

9 CONCLUSION

In this paper, we presented the attack methodology and the detailed steps for cellular handover exploitation. We identified the main security flaws related to the handover procedure which affect all generations and cases. We emphasize on the implications of the unverified measurement reports and insecure broadcast messages explicating the impact on both the UE and network. Finally, through a meticulous experimentation we were able to verify that DoS, MitM and information leakage are possible by using both open source and closed source software.

ACKNOWLEDGMENTS

This work was supported by the Abu Dhabi Award for Research Excellence (AARE) 2019 (#AARE19-236) and the Center for Cyber Security at New York University Abu Dhabi (NYUAD).

REFERENCES

[1] 3GPP. 2007. *Universal Mobile Telecommunications System (UMTS); Radio resource management strategies.* Technical Specification (TS) 125.922. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_tr/125900_125999/125922/07.01.00_60/tr_125922v070100p.pdf version 7.1.0.

[2] 3GPP. 2016. *LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification.* Technical Specification (TS) 36.331. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.00.00_60/ts_136331v130000p.pdf Version 13.0.0.

[3] 3GPP. 2016. *Universal Mobile Telecommunications System (UMTS); Radio Resource Control (RRC); Protocol specification.* Technical Specification (TS) 25.331. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/125300_125399/125331/13.01.00_60/ts_125331v130100p.pdf Version 13.1.0.

[4] 3GPP. 2017. *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14).* Technical Specification (TS) 33.899. 3rd Generation Partnership Project (3GPP). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045 Version 1.3.0.

[5] 3GPP. 2017. *Digital cellular telecommunications system (Phase 2+) (GSM); Packet-switched handover for GERAN A/Gb mode; Stage 2.* Technical Specification (TS) 143.129. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/143100_143199/143129/14.01.00_60/ts_143129v140100p.pdf version 14.1.0.

[6] 3GPP. 2018. *5G; NG-RAN; Architecture description.* Technical Specification (TS) 38.401. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/138400_138499/138401/15.02.00_60/ts_138401v150200p.pdf Version 15.2.0.

[7] 3GPP. 2019. *NR; Radio Resource Control (RRC); Protocol specification.* Technical Specification (TS) 38.331. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/138300_138399/138331/15.06.00_60/ts_138331v150600p.pdf Version 15.6.0.

[8] 3GPP. 2020. *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Study on 5G Security Enhancement against False Base Stations (FBS) (Release 17).* Technical Specification (TS) 33.809. 3rd Generation Partnership Project (3GPP). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539 Version 0.12.1.

[9] 3GPP. 2020. *5G; Management and orchestration; 5G end to end Key Performance Indicators (KPI).* Technical Specification (TS) 128.554. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/128500_128599/128554/16.06.00_60/ts_128554v160600p.pdf version 16.6.0.

[10] 3GPP. 2020. *5G; NR; NR and NG-RAN Overall description; Stage-2.* Technical Specification (TS) 38.300. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/138400_138499/138401/16.03.00_60/ts_138401v160300p.pdf version 16.3.0.

[11] 3GPP. 2020. *5G; Security architecture and procedures for 5G System).* Technical Specification (TS) 33.501. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf Version 16.3.0.

[12] 3GPP. 2020. *5G; Self-Organizing Networks (SON) for 5G networks.* Technical Report 128.313. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/128300_128399/128313/16.00.00_60/ts_128313v160000p.pdf version 16.0.0.

[13] 3GPP. 2020. *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Handover procedures.* Technical Specification (TS) 123.009. 3rd Generation Partnership Project

(3GPP). https://www.etsi.org/deliver/etsi_ts/123000_123099/123009/16.00.00_60/ts_123009v160000p.pdf version 16.0.0.

[14] 3GPP. 2020. *LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2.* Technical Specification (TS) 38.300. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/136300_136399/136300/16.02.00_60/ts_136300v160200p.pdf version 16.2.0.

[15] 3GPP. 2020. *Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Automatic Neighbour Relation (ANR) management; Concepts and requirements* . Technical Specification (TS) 132.511. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/132500_132599/132511/16.00.00_60/ts_132511v160000p.pdf version 16.0.0.

[16] 3GPP. 2020. *Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Self-Organizing Networks (SON); Concepts and requirements.* Technical Specification (TS) 32.500. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/132500_132599/132500/16.00.00_60/ts_132500v160000p.pdf Version 16.0.0.

[17] 3GPP. 2021. *5G; Procedures for the 5G System (5GS).* Technical Specification (TS) 123.502. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/123500_123599/123502/16.07.00_60/ts_123502v160700p.pdf version 16.7.0.

[18] K. Alexandris, N. Nikaein, R. Knopp, and C. Bonnet. 2016. Analyzing X2 handover in LTE/LTE-A. In *2016 14th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt).* 1–7. https://doi.org/10.1109/WIOPT.2016.7492906

[19] Amarisoft. [n.d.]. *Amarisoft Callbox Classic.* https://www.amarisoft.com/products/test-measurements/amari-lte-callbox/

[20] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. 2018. A Formal Analysis of 5G Authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18).* Association for Computing Machinery, New York, NY, USA, 1383–1396. https://doi.org/10.1145/3243734.3243846

[21] Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park, and Altaf Shaik. 2019. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. *Proceedings on Privacy Enhancing Technologies* 2019 (07 2019), 108–127. https://doi.org/10.2478/popets-2019-0039

[22] Merlin Chlosta, David Rupprecht, Thorsten Holz, and Christina Pöpper. 2019. LTE Security Disabled: Misconfiguration in Commercial Networks. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (Miami, Florida) *(WiSec '19).* Association for Computing Machinery, New York, NY, USA, 261–266. https://doi.org/10.1145/3317549.3324927

[23] A. Dabrowski, G. Petzl, and E. Weippl. 2016. The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection. In *RAID.*

[24] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. 2014. IMSI-Catch Me If You Can: IMSI-Catcher-Catchers. In *Proceedings of the 30th Annual Computer Security Applications Conference* (New Orleans, Louisiana, USA) *(ACSAC '14).* Association for Computing Machinery, New York, NY, USA, 246–255. https://doi.org/10.1145/2664243.2664272

[25] Ericsson. [n.d.]. Ericsson Mobility Report. https://www.ericsson.com/en/mobility-report/reports.

[26] K. Ghanem, H. Alradwan, A. Motermawy, and A. Ahmad. 2012. Reducing ping-pong Handover effects in intra EUTRA networks. In *2012 8th International Symposium on Communication Systems, Networks Digital Signal Processing (CSNDSP).* 1–5. https://doi.org/10.1109/CSNDSP.2012.6292642

[27] Nico Golde, Kévin Redon, and Jean-Pierre Seifert. 2013. Let Me Answer That for You: Exploiting Broadcast Information in Cellular Networks. In *Proceedings of the 22nd USENIX Conference on Security* (Washington, D.C.) *(SEC'13).* USENIX Association, USA, 33–48.

[28] Shubham Gupta, Balu L. Parne, and Narendra S. Chaudhari. 2018. Security Vulnerabilities in Handover Authentication Mechanism of 5G Network. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC).* 369–374. https://doi.org/10.1109/ICSCCC.2018.8703355

[29] S. Holtmanns, S. P. Rao, and I. Oliver. 2016. User location tracking attacks for LTE networks using the interworking functionality. In *2016 IFIP Networking Conference (IFIP Networking) and Workshops.* 315–322. https://doi.org/10.1109/IFIPNetworking.2016.7497239

[30] Russell Housley, W. Polk, W. Ford, and D. Solo. 2002. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. (04 2002).

[31] S. R. Hussain, Omar Chowdhury, Shagufta Mehnaz, and E. Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In *NDSS.*

[32] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. 2019. Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. In *Proceedings 2019 Network and Distributed System Security Symposium.* Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2019.23442

[33] Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino. 2019. 5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19).* Association for Computing Machinery, New York, NY, USA, 669–684. https://doi.org/10.1145/3319535.3354263

[34] iPerf. [n.d.]. *iPerf - The ultimate speed test tool for TCP, UDP and SCTP.* https://iperf.fr/

[35] H. Kim, J. Lee, E. Lee, and Y. Kim. 2019. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. In *2019 IEEE Symposium on Security and Privacy (SP).* 1153–1168. https://doi.org/10.1109/SP.2019.00038

[36] Z. Li, W. Wang, Christo Wilson, Jian Jhen Chen, C. Qian, T. Jung, L. Zhang, K. Liu, Xiangyang Li, and Y. Liu. 2017. FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. In *NDSS.*

[37] Prajwol Kumar Nakarmi, Mehmet Akif Ersoy, Elif Ustundag Soykan, and Karl Norrman. 2021. Murat: Multi-RAT False Base Station Detector. *CoRR* abs/2102.08780 (2021). arXiv:2102.08780 https://arxiv.org/abs/2102.08780

[38] Peter Ney, Ian Smith, Gabriel Cadamuro, and Tadayoshi Kohno. 01 Jul. 2017. SeaGlass: Enabling City-Wide IMSI-Catcher Detection. *Proceedings on Privacy Enhancing Technologies* 2017, 3 (01 Jul. 2017), 39 – 56. https://doi.org/10.1515/popets-2017-0027

[39] Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, Andrew Martin, and Jean-Pierre Seifert. 2017. White-Stingray: Evaluating IMSI Catchers Detection Applications. In *11th USENIX Workshop on Offensive Technologies (WOOT 17).* USENIX Association, Vancouver, BC. https://www.usenix.org/conference/woot17/workshop-program/presentation/park

[40] Cooper Quintin. 2021. Detecting Fake 4G LTE Base Stations in Real Time. USENIX Association, Presentation.

[41] Ettus Research. [n.d.]. *USRP B210 SDR Kit - Dual Channel Transceiver (70 MHz - 6GHz).* https://www.ettus.com/all-products/ub210-kit/

[42] David Rupprecht, Adrian Dabrowski, Thorsten Holz, Edgar R. Weippl, and Christina Pöpper. 2018. On Security Research Towards Future Mobile Network Generations. *IEEE Commun. Surv. Tutorials* 20, 3 (2018), 2518–2542. https://doi.org/10.1109/COMST.2018.2820728

[43] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2020. IMP4GT: IMPersonation Attacks in 4G NeTworks. In *IMP4GT: IMPersonation Attacks in 4G NeTworks (Proceedings of the 27th Annual Network and Distributed System Security Symposium (NDSS)).* The Internet Society.

[44] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper. 2019. Breaking LTE on Layer Two. In *2019 IEEE Symposium on Security and Privacy (SP).* 1121–1136. https://doi.org/10.1109/SP.2019.00006

[45] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2016. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In *23rd Annual Network and Distributed System Security Symposium (NDSS 2016).* Internet Society, United States. https://doi.org/10.14722/ndss.2016.23236 NDSS 2016 Volume: Proceeding volume: ; Network and Distributed System Security Symposium ; Conference date: 21-02-2016 Through 24-02-2016.

[46] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2018. On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (Stockholm, Sweden) *(WiSec '18).* Association for Computing Machinery, New York, NY, USA, 75–86. https://doi.org/10.1145/3212480.3212497

[47] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2019. New Vulnerabilities in 4G and 5G Cellular Access Network Protocols: Exposing Device Capabilities. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (Miami, Florida) *(WiSec '19).* Association for Computing Machinery, New York, NY, USA, 221–231. https://doi.org/10.1145/3317549.3319728

[48] Neil Sinclair, David A. Harle, Ian A. Glover, James M. Irvine, and Robert C. Atkinson. 2013. *Parameter optimization for LTE handover using an advanced SOM algorithm.* IEEE, 1–6. https://doi.org/10.1109/VTCSpring.2013.6692692 IEEE 77th Vehicular Technology Conference ; Conference date: 02-06-2013 Through 05-06-2013.

[49] Ankush Singla, Rouzbeh Behnia, Syed Rafiul Hussain, Attila Yavuz, and Elisa Bertino. 2021. Look Before You Leap: Secure Connection Bootstrapping for 5G Networks to Defend Against Fake Base-Stations. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security* (Virtual Event, Hong Kong) *(ASIA CCS '21).* Association for Computing Machinery, New York, NY, USA, 501–515. https://doi.org/10.1145/3433210.3453082

[50] Huawei Technologies. 2016. *eRAN TDD MRO Feature Parameter Description.* Technical Specification (TS) 01. HUAWEI TECHNOLOGIES CO. https://www.honorcup.ru/upload/iblock/164/7.pdf

[51] Thanh van Do, Hai Thanh Nguyen, Nikolov Momchil, and Van Thuan Do. 2015. Detecting IMSI-Catcher Using Soft Computing. In *Soft Computing in Data Science,* Michael W. Berry, Azlinah Mohamed, and Bee Wah Yap (Eds.). Springer Singapore, Singapore, 129–140.

[52] 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, Santa Clara, CA, 55–72. https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon

[53] Wei Zheng, Haijun Zhang, Xiaoli Chu, and Xiangming Wen. 2013. Mobility robustness optimization in self-organizing LTE femtocell networks. *EURASIP Journal on Wireless Communications and Networking* 2013 (02 2013). https://doi.org/10.1186/1687-1499-2013-27

ACRONYMS

3GPP	3rd Generation Partnership Project
5G	5^{th} Generation
AS	Access Stratum
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
ANR	Automatic Neighbor Relation
ARFCN	Absolute Radio Frequency Channel Number
BSS	Base Station Subsystem
CHO	Conditional Handover
CU	Centralized Unit
DoS	Denial-Of-Service
DU	Distributed Unit
eNodeB	Evolved NodeB
EPS	Evolved Packet System
gNodeB	Next Generation NodeB
GSM	Global System for Mobile Communications
GSMA	GSM Association
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
LTE	Long Term Evolution
MCC	Mobile Country Code
MIB	Master Information Block
MitM	Man-In-The-Middle
MME	Mobility and Management Entity
MNC	Mobile Network Code
MR	Measurement Report
MSC	Mobile Switching Center
NAS	Non-Access Stratum
NGAP	NG Application Protocol
OAM	Operations, Administration and Management
PCI	Physical Cell Identifier
PEI	Permanent Equipment Identifier
PLMN	Public Land Mobile Network
PRACH	Physical Random Access Channel
RACH	Random Access Channel
RAN	Radio Access Network
RAT	Radio Access Technology
RLF	Radio Link Failure
RNC	Radio Network Controller
RNTI	Radio Network Temporary Identifier
RRC	Radio Resource Control
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
SDR	Software-Defined Radio
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIB	System Information Block
SINR	Signal-to-Interference-plus-Noise Ratio
SIP	Session Initiation Protocol
SMF	Session Management Function
SMS	Short Message Service
SON	Self-Organizing Networks
SRVCC	Single Radio Voice Call Continuity
TAC	Tracking Area Code
TAI	Tracking Area Identity
TAU	Tracking Area Update
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UPF	User Plane Function

A Trigger Events in LTE and 5G

3GPP specifications [2, 7] specify the following *event* types defined for LTE and 5G NR:

A1: when Serving Cell becomes better than the threshold.
A2: when Serving Cell becomes worse than the threshold.
A3: when neighboring Cell becomes offset better than the Special Cell.
A4: when neighboring Cell becomes better than the threshold.
A5: when the Special Cell becomes worse than $threshold_1$ and the neighboring becomes better than $threshold_2$.
A6: when neighboring Cell becomes offset better than Secondary Cell.
B1: when Inter-RAT neighboring Cell becomes better than the threshold.
B2: when Primary Serving Cell becomes worse than $threshold_1$ and Inter-RAT neighboring Cell becomes better than $threshold_2$.

By closely observing the events above, we can categorize them accordingly. A1-A6 events are Intra-RAT events and B1-B2 events are Inter-RAT Events. The terms Intra-RAT and Inter-RAT are explained in Section 2.1.

B Handover Failures

Incorrect HO parameter settings can negatively affect user experience and waste network resources by causing handover ping-pongs, handover failures and RLFs. One example is the incorrect setting of handover hysteresis, which may results in ping-pongs or excessively delayed handovers to a target cell. Therefore, we need to optimize the handover mechanism to curtail unnecessary or missed handovers [48, 53].

Most problems associated with handover failures or sub-optimal system performance can ultimately be categorized, as either too-early or too-late triggering of the handover, provided that the required fundamental network RF coverage exists. Thus, poor handover-related performance can generally be categorized by the following events [50]:

(1) Intra-RAT late handover triggering
(2) Intra-RAT early handover triggering
(3) Intra-RAT handover to an incorrect cell
(4) Inter-RAT too late handover
(5) Inter-RAT unnecessary handover

The UE is programmed to send RLF reports when it is connected back to the network after a failure. To initiate this connection, it sends the RRC Reestablishment request to the best available base station. In terms of security it is crucial that the network distinguishes failures related to the above events from failures related to attacks.

C False Base Station Signal Power and Detection

In our attacks we tried to use the least signal power possible in order to trigger an event while at the same time being careful about the safety of our equipment. It is of paramount importance for the attacker to achieve enough cell gain to have significant chances in triggering an event. Ideally, attacker's signal should be scaled as excellent achieving at least −70 dBm for RSSI in 2G/3G and −80 dBm for RSRP in 4G. Equivalent signal strength is required for the SS-RSRP in 5G. Additionally, a linear amplifier could make attacker's signal more robust. Nevertheless, unusual signal power that deviates from normal base station transmissions in the cellular environment may be used by the operator to detect an attack. Therefore, maximum signal power can expose the attacker, even though he/she may imitate legitimate base station as accurately as possible. Of course, we take into account that the attacker constantly monitors the network for alterations in frequencies, cell identifiers, supported services and other parameters, and immediately adapt reconfiguring the malicious station. Using outdated or invalid parameters may make him/her even more susceptible to detection, since the operator can easily discover misconfigurations through MRs, RLF reports, network errors, etc.

D Cellular Network Configurations

We configured the network to use the testing PLMN which is 00101. The eNodeB/gNodeB in computer 1 has the $enb/gnb\_id = 0x1A2D0$ and $tac = 0x0001$. Its cell 1 has the $cell\_id = 0x01$, $n\_id\_cell = 1$ (Physical Cell Id), $root\_seq\_index = 204$. Its cell 2 has the $cell\_id = 0x02$, $n\_id\_cell = 2$, $root\_seq\_index = 28$. In 5G, we kept the Physical Cell IDs with their default configurations, meaning that cell 1 and 2 had $n\_id\_cell = 500$ and $n\_id\_cell = 501$ respectively.

For the eNodeB/gNodeB in computer 2 we have the $enb/gnb\_id = 0x1A2D1$ and $tac = 0x0002$. Its cell 3 has a $cell\_id = 0x03$, $n\_id\_cell = 3$ (Physical Cell Id), $root\_seq\_index = 202$. Its cell 4 has the $cell\_id = 0x04$, $n\_id\_cell = 4$, $root\_seq\_index = 29$. Likewise in 5G, cell 3 and 4 had $n\_id\_cell = 502$ and $n\_id\_cell = 503$ respectively.

In addition, for LTE we used band 3 and band 7 based on the Frequency Division Duplex (FDD) which are $ARFCN = 1575$ and 3100 respectively for the downlink. Whereas for 5G, we used Time Division Duplex (TDD) with a downlink $ARFCN = 40620$ which is band 41 (used for 5G NSA), and with a downlink $ARFCN = 627300$ which is band $n78$ (used for 5G SA). Regarding the transmission features in our experiments, we utilized the Single-Input-Single-Output (SISO) and Multiple-Input-Multiple-Output 2x2 (MIMO 2x2) technologies.

Next, we had to also configure two Access Point Names (APNs) in order for the UEs to have full services; the Internet APN and the IMS APN. Table 2 shows more information about the utilized devices.

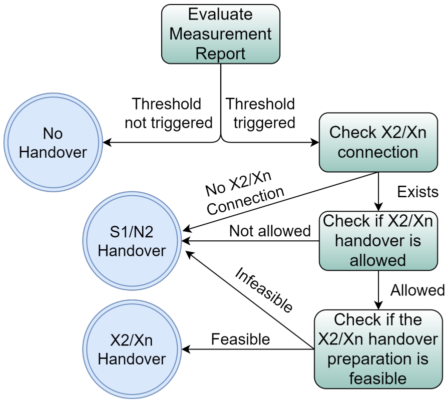


Figure 5: Handover Interface Decision flow, as executed by the source base station.

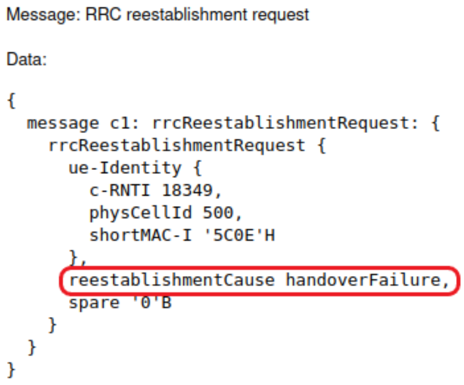
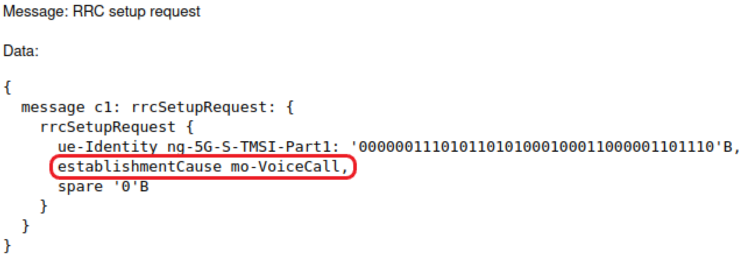

```
Message: RRC reestablishment request

Data:

{
  message c1: rrcReestablishmentRequest: {
    rrcReestablishmentRequest {
      ue-Identity {
        c-RNTI 18349,
        physCellId 500,
        shortMAC-I '5C0E'H
      },
      reestablishmentCause handoverFailure,
      spare '0'B
    }
  }
}
```

Figure 6: 5G RRC Reestablishment Request

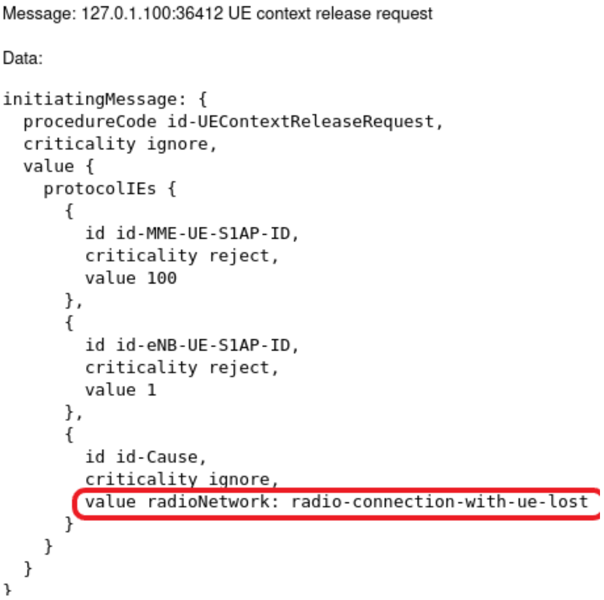
Finally, our basic measurement configurations for LTE and NR cells were mostly defined as follows:

```
meas_config_desc: [
        a1_report_type: "rsrp",
        a1_rsrp: -70,
        a1_hysteresis: 10,
        a1_time_to_trigger: 320,
        a2_report_type: "rsrp",
        a2_rsrp: -80,
        a2_hysteresis: 0,
        a2_time_to_trigger: 640,
        a3_report_type: "rsrp",
        a3_offset: 6,
        a3_hysteresis: 0,
        a3_time_to_trigger: 256,
        rsrp_filter_coeff: 3,
        nr_b1_report_type: "rsrp",
        nr_b1_rsrp: -119,
        nr_b1_hysteresis: 10,
        nr_b1_time_to_trigger: 480,
        nr_rsrp_filter_coeff: 3  ]
```



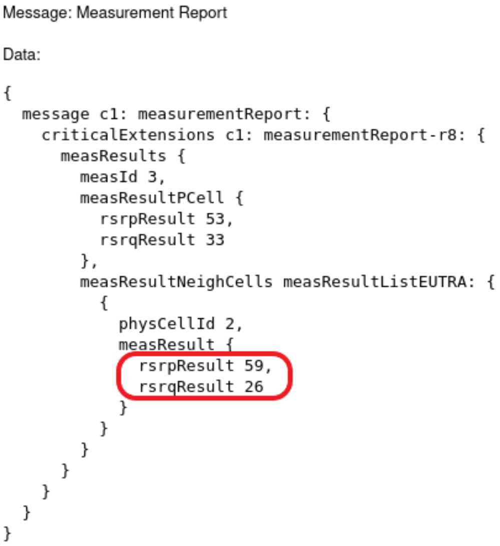
```
Message: RRC setup request

Data:

{
  message c1: rrcSetupRequest: {
    rrcSetupRequest {
      ue-Identity ng-5G-S-TMSI-Part1: '000000111010110101000100011000001101110'B,
      establishmentCause mo-VoiceCall,
      spare '0'B
    }
  }
}
```

Figure 7: 5G RRC Setup Request



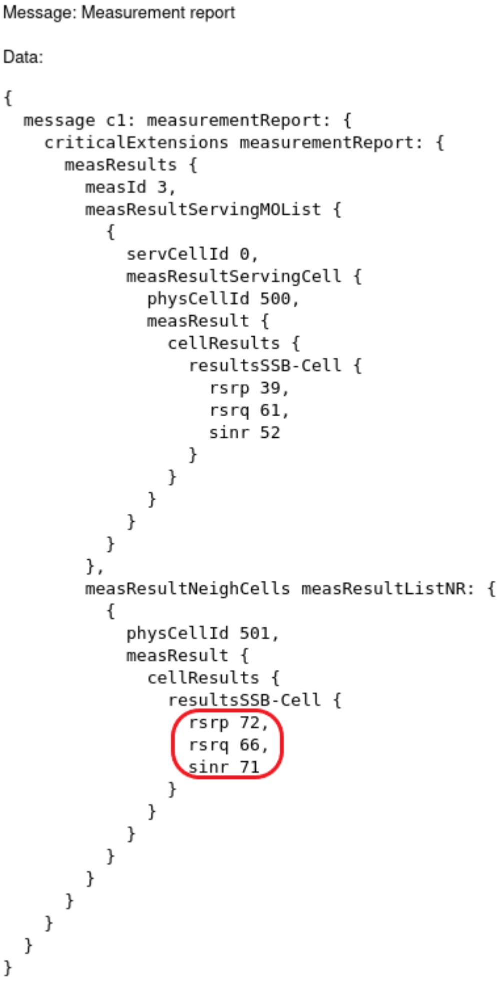
```
Message: 127.0.1.100:36412 UE context release request

Data:

initiatingMessage: {
  procedureCode id-UEContextReleaseRequest,
  criticality ignore,
  value {
    protocolIEs {
      {
        id id-MME-UE-S1AP-ID,
        criticality reject,
        value 100
      },
      {
        id id-eNB-UE-S1AP-ID,
        criticality reject,
        value 1
      },
      {
        id id-Cause,
        criticality ignore,
        value radioNetwork: radio-connection-with-ue-lost
      }
    }
  }
}
```

Figure 8: UE context release due to UE disconnection



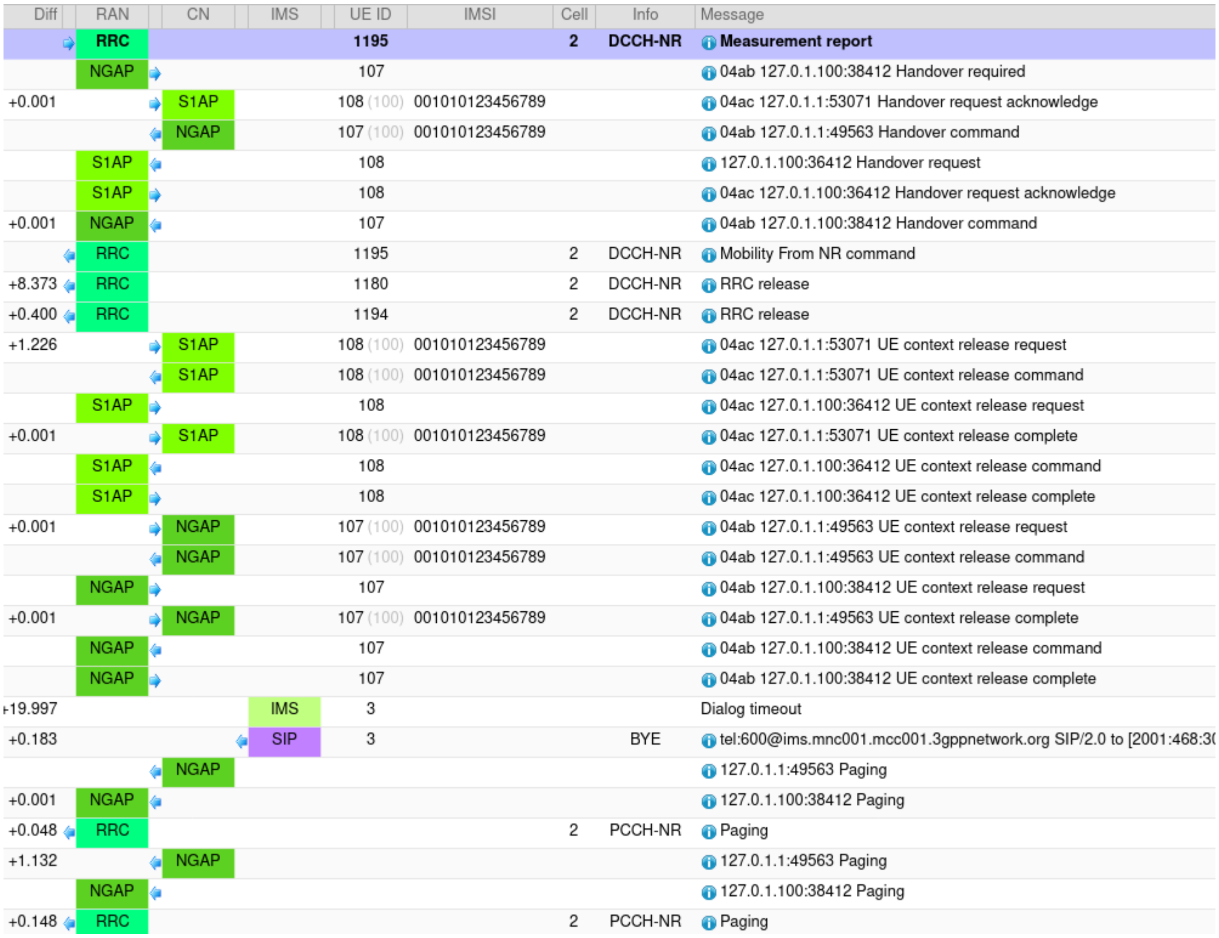
```
Message: Measurement Report

Data:

{
  message c1: measurementReport: {
    criticalExtensions c1: measurementReport-r8: {
      measResults {
        measId 3,
        measResultPCell {
          rsrpResult 53,
          rsrqResult 33
        },
        measResultNeighCells measResultListEUTRA: {
          {
            physCellId 2,
            measResult {
              rsrpResult 59,
              rsrqResult 26
            }
          }
        }
      }
    }
  }
}
```

Figure 9: Malicious LTE Measurement Report



```
Message: Measurement report

Data:

{
  message c1: measurementReport: {
    criticalExtensions measurementReport: {
      measResults {
        measId 3,
        measResultServingMOList {
          {
            servCellId 0,
            measResultServingCell {
              physCellId 500,
              measResult {
                cellResults {
                  resultsSSB-Cell {
                    rsrp 39,
                    rsrq 61,
                    sinr 52
                  }
                }
              }
            }
          }
        },
        measResultNeighCells measResultListNR: {
          {
            physCellId 501,
            measResult {
              cellResults {
                resultsSSB-Cell {
                  rsrp 72,
                  rsrq 66,
                  sinr 71
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Figure 10: Malicious 5G Measurement Report with high signal power



Diff	RAN	CN	IMS	UE ID	IMSI	Cell	Info	Message
→	**RRC**			**1195**		**2**	**DCCH-NR**	**Measurement report**
	NGAP →			107				04ab 127.0.1.100:38412 Handover required
+0.001		→ S1AP		108 (100)	001010123456789			04ac 127.0.1.1:53071 Handover request acknowledge
		← NGAP		107 (100)	001010123456789			04ab 127.0.1.1:49563 Handover command
	S1AP ←			108				127.0.1.100:36412 Handover request
	S1AP →			108				04ac 127.0.1.100:36412 Handover request acknowledge
+0.001	NGAP ←			107				04ab 127.0.1.100:38412 Handover command
←	RRC			1195		2	DCCH-NR	Mobility From NR command
+8.373 ←	RRC			1180		2	DCCH-NR	RRC release
+0.400 ←	RRC			1194		2	DCCH-NR	RRC release
+1.226		→ S1AP		108 (100)	001010123456789			04ac 127.0.1.1:53071 UE context release request
		← S1AP		108 (100)	001010123456789			04ac 127.0.1.1:53071 UE context release command
	S1AP →			108				04ac 127.0.1.100:36412 UE context release request
+0.001		→ S1AP		108 (100)	001010123456789			04ac 127.0.1.1:53071 UE context release complete
	S1AP ←			108				04ac 127.0.1.100:36412 UE context release command
	S1AP →			108				04ac 127.0.1.100:36412 UE context release complete
+0.001		→ NGAP		107 (100)	001010123456789			04ab 127.0.1.1:49563 UE context release request
		← NGAP		107 (100)	001010123456789			04ab 127.0.1.1:49563 UE context release command
	NGAP →			107				04ab 127.0.1.100:38412 UE context release request
+0.001		→ NGAP		107 (100)	001010123456789			04ab 127.0.1.1:49563 UE context release complete
	NGAP ←			107				04ab 127.0.1.100:38412 UE context release command
	NGAP →			107				04ab 127.0.1.100:38412 UE context release complete
+19.997			IMS	3				Dialog timeout
+0.183		←	SIP	3			BYE	tel:600@ims.mnc001.mcc001.3gppnetwork.org SIP/2.0 to [2001:468:3
		← NGAP						127.0.1.1:49563 Paging
+0.001	NGAP ←							127.0.1.100:38412 Paging
+0.048 ←	RRC					2	PCCH-NR	Paging
+1.132		← NGAP						127.0.1.1:49563 Paging
	NGAP ←							127.0.1.100:38412 Paging
+0.148 ←	RRC					2	PCCH-NR	Paging

Figure 11: Abusing EPS fallback (Inter-Base station)