Journal of Cybersecurity and Privacy

MDPI

Article

Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy

Mohamad Saalim Wani [1,*], Michael Rademacher [2], Thorsten Horstmann [2] and Mathias Kretschmer [1]

[1] Fraunhofer FIT, 53757 Sankt Augustin, Germany; mathias.kretschmer@fit.fraunhofer.de
[2] Fraunhofer FKIE, 53177 Bonn, Germany; michael.rademacher@fkie.fraunhofer.de (M.R.); thorsten.horstmann@fkie.fraunhofer.de (T.H.)
* Correspondence: mohamad.saalim.wani@fit.fraunhofer.de

Abstract: 5G networks, pivotal for our digital mobile societies, are transitioning from 4G to 5G Stand-Alone (SA) networks. However, during this transition, 5G Non-Stand-Alone (NSA) networks are widely used. This paper examines potential security vulnerabilities in 5G NSA networks. Through an extensive literature review, we identify known 4G attacks that can theoretically be applied to 5G NSA. We organize these attacks into a structured taxonomy. Our findings reveal that 5G NSA networks may offer a false sense of security, as most security and privacy improvements are concentrated in 5G SA networks. To underscore this concern, we implement three attacks with severe consequences and successfully validate them on various commercially available smartphones. Notably, one of these attacks, the IMSI Leak, consistently exposes user information with no apparent security mitigation in 5G NSA networks. This highlights the ease of tracking individuals on current 5G networks.

Keywords: 5G; LTE; security

Citation: Wani, M.S.; Rademacher, M.; Horstmann, T.; Kretschmer, M. Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy. *J. Cybersecur. Priv.* **2024**, *4*, 23–40. https://doi.org/10.3390/jcp4010002

Academic Editor: Francesco Mercaldo

Received: 23 October 2023
Revised: 3 December 2023
Accepted: 11 December 2023
Published: 2 January 2024

1. Introduction

5G is the mobile network generation that is currently being launched across the globe. It is often regarded as a key technology for the future of our digital societies. Compared with previous generations, 5G no longer focuses on the classical use case of mobile telephony. Instead, its main goals are to provide gigabit data rates for end devices (Enhanced Mobile Broadband (eMBB)), to connect the increasing number of smart things (Massive Machine Type Communications (mMTC)), and to provide guaranteed service properties for time-critical applications (ultra-reliable low-latency communication (URLLC)).

Mobile Network Operators (MNOs) are offering customized 5G solutions to end users and the industry alike. It is expected that by the end of 2023, the number of 5G subscriptions will reach more than one billion worldwide. By the end of 2028, it is estimated that the number of 5G subscriptions will surpass five billion, exceeding the count of Long-Term Evolution (LTE) subscriptions. In North America, Northeast Asia, and Europe, 5G networks have quickly become available, in particular in urban areas [1]. For example, in 2022, on 80% of the German territory, 5G was already provided by at least one of the major MNOs [2]. Many end devices for 5G, in particular modern smartphones, are available. In fact, the latest high-end smartphones from all major vendors offer 5G functionalities.

From a security perspective, many of the basic mechanisms of 4G are reused. However, to address the security requirements of the various 5G deployment scenarios, a new authentication framework has been developed. These new security mechanisms are mainly implemented in the new 5G core network, which heavily relies on modern technologies such as Software-Defined Networking (SDN), Network Functions Virtualization (NFV), and cloud computing. An extensive amount of research and development has gone into the security of 5G networks, in particular taking into account the interest of different shareholders, such as network and end-user equipment vendors, MNOs, and governments [3].

The 3rd Generation Partnership Project (3GPP), in its different committees, is responsible for transferring these ideas into applicable standards [4].

Many people are already "enjoying a 5G Symbol" and better data rates on their smartphones. However, it is widely unknown to the public that in most current 5G deployments, many novel 5G features are missing. In particular, this refers to security mechanisms, such as the new authentication framework, to better protect the privacy of users.

Currently, the majority of 5G networks operate in a special transitory mode referred to as 5G Non-Stand-Alone (NSA) [5]. The idea of 5G NSA is to help MNOs to swiftly move from 4G to 5G while reusing the current 4G facilities. The NSA mode of operation allows 5G deployments to utilize LTE core networks and base stations while adding new 5G base stations. 5G NSA enables MNOs to begin offering 5G services, providing higher data speed and capturing additional revenue streams while, in the background, they are implementing their new 5G core infrastructure. It is unclear how long a complete transition from 5G NSA to the fully 5G Stand-Alone (SA) architecture, which includes the new 5G core network, will take. But the latest 5G status update report by the Global Mobile Suppliers Association shows that only 22% of the MNOs worldwide are currently investing in public SA networks [5]. As a result, it is expected that 5G NSA will remain primarily in use in the coming years; thus, its security is critical.

The critical nature of the security of 5G NSA networks has prompted research into 4G attacks that can be transferred to 5G NSA networks, with a few attacks having been verified to date. Nevertheless, existing research lacks a comprehensive and systematic study that explores the state of the art, identifies transferable attacks, and categorizes them into a structured taxonomy to provide a holistic understanding. These insights are necessary to develop effective countermeasures tailored to specific attack techniques, rogue devices, or a common root cause. For instance, the shift toward Open Radio networks [6] may offer an opportunity to leverage third-party apps (xApps) for detecting fake base stations—a primary device used in attacks against mobile networks [7–12]. Moreover, the advent of private 5G networks [13] for Industry 4.0, managed by companies relatively new to the 5G security domain, also adds to the importance of such studies.

To address this gap in the literature, we present, to the best of our knowledge, the first taxonomy of attacks on 5G NSA over the radio interface. Through an extensive exploration of the existing literature, we identify transferable attacks and systematically categorize them based on the active or passive nature of the attacker, attack techniques, underlying vulnerabilities, and type of rogue device used. Our study provides a succinct summary of all the attacks, serving as a comprehensive reference and analytical resource. Additionally, it also reveals that 5G NSA may offer a false sense of security, as most enhancements are implemented in 5G SA networks, such as IMSI encryption [14]. To underscore this concern, we implement three attacks with severe consequences (yet to be verified) and successfully validate them on various commercially available smartphones, thereby extending the list of verified attacks to date. Based on our results, we also offer valuable recommendations for companies considering investments in private 5G networks.

This paper is structured as follows: In Section 2, we briefly summarize the architecture of 5G NSA networks. Section 3 provides a comprehensive overview of known 4G vulnerabilities and discusses them in the context of 5G NSA networks. We discuss our findings from the literature review in Section 4. Section 5 introduces our testbed and the additional infrastructure which we used to conduct our experiments. Afterwards, we present our results (Section 6) of practically applying three different attacks to 5G NSA networks, namely, *IMSI Leak Attack*, *Numb Attack*, and *Downgrade Attack*. The last section, Section 7, provides a summary of the results and discusses possible future work.

2. Background on 5G NSA

The 3GPP has introduced five architecture options for 5G deployment and divided them into two deployment scenarios: Stand-Alone (SA) and Non-Stand-Alone (NSA).

The SA version provides 5G services using solely the New Radio (NR) radio technology, whereas the NSA version provides services using both 4G and 5G radio technologies. The architecture options "2" and "5" belong to the SA version, while "3", "4" and "7" belong to the NSA version [15]. The standardization of option "3" (NSA) and option "2" (SA) is already complete, and current deployments are adopting either of these two architecture options [16].

Similar to other mobile network generations, a 5G NSA network architecture (Option 3) can be divided into three components: User Equipment (UE), the Radio Access Network (RAN), and the core network. A simplified overview is shown in Figure 1.

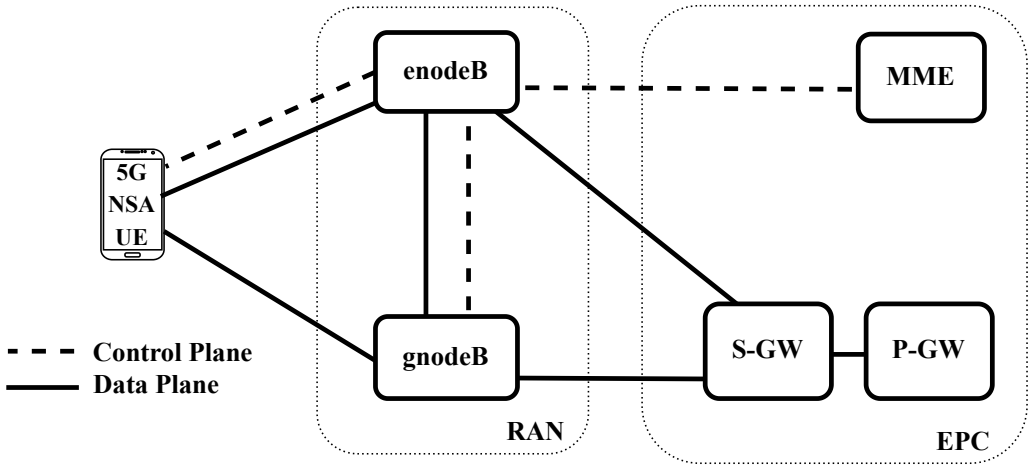

Figure 1. The 5G NSA architecture consists of a 4G core network and two types of base stations (BSs).

The **UE** is a device the end user uses to communicate with the mobile network (e.g., a smartphone). It contains a physical Subscriber Identity Module (SIM) card or an electronic SIM that securely stores the International Mobile Subscriber Identity (IMSI) and the secret long-term symmetric key. The IMSI is a 15-digit number that uniquely identifies a SIM, and its leakage can make a UE prone to tracking or impersonation. The **RAN** consists of two types of BSs: enodeBs and gnodeBs. The **enodeBs** (master nodes) are LTE BSs that are used to exchange control plane and data plane messages with the UE. In a 5G NSA architecture, the enodeB performs functions like paging, over-the-air security, and handovers. The **gnodeBs** (secondary nodes), also referred to as "en-gNB" or "SgNB," serve as 5G base stations dedicated to exchanging data plane messages. They work in conjunction with the enodeBs, primarily to significantly enhance the data rate for the UEs.

The NSA version of 5G uses the LTE core network known as Evolved Packet Core (EPC). In the following, we provide a brief summary of the main components of the core network. The Mobility Management Entity (MME) is the central control node, which is responsible for authenticating and allocating resources to the UEs when they connect to the network. It also takes care of other important functionalities, such as tracking the UE location at a macro level, bearer activation/deactivating, and ciphering/integrity protection for Non-Access Stratum (NAS) signaling protocols (a set of protocols that run between UE and the MME). The Home Subscriber Service (HSS) is a database that stores user-related data such as IMSIs, shared keys, and subscription data. The Serving Gateway (S-GW) is responsible for routing and forwarding user data packets. It also serves as an anchoring point for handovers. The PDN Gateway (P-GW) serves as a point of interconnection between the core network and the external IP networks (i.e., the Internet and other mobile networks).

For MNOs, the 5G architecture option "3", the NSA option, is a compromise between adding new capacity for eMBB and saving Capital Expenditure (CapEx) for deploying the 5G core network [17]. In this architecture, the RAN is composed of enodeBs as the Master Node (MN) and gnodeBs as the Secondary Node (SN). The RAN is connected to the 4G core network. MNOs usually use the term 5G NSA to refer to 5G NSA option 3. Therefore,

in this paper, any reference to "5G NSA" refers to this option. 5G NSA option 3 is further divided into three types, based on the data split method, as shown in the Figure 2.

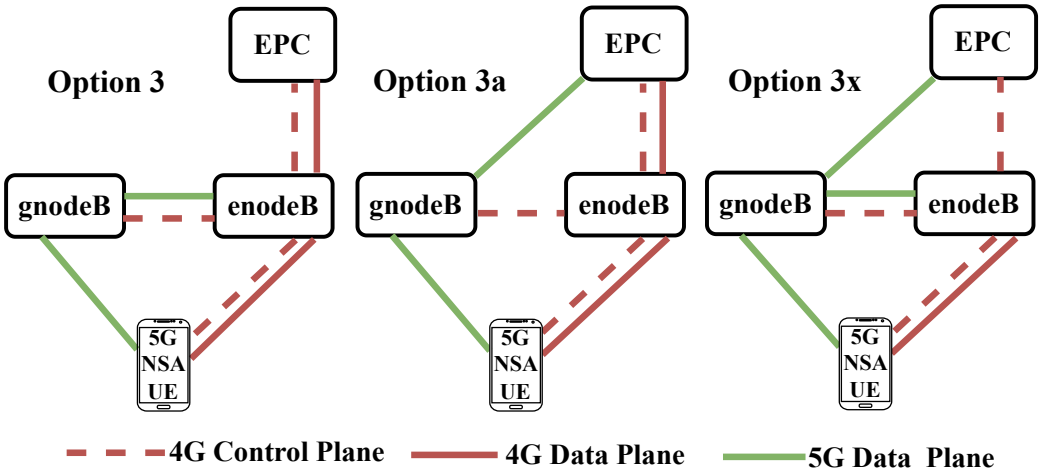

Figure 2. 5G NSA option 3 consists of three variants, namely 3, 3a, and 3x [16].

From a control plane perspective, in all three options, the UE has control plane connectivity only with the enodeB, while the gnodeB works in conjunction with the enodeB via the X2 interface. Regarding the data plane, option 3 involves a traffic split at enodeB. In this option, the EPC forwards the traffic to only enodeB, which can either transmit it directly to the UE or forward (split data) a part of it to gnodeB for transmission over the NR interface. In option 3a, data traffic is split at the EPC, which can then transmit/receive the data traffic to/from both the enodeB and gnodeB. In option 3x, the EPC forwards the data traffic to the gnodeB, which can either transmit it directly over the NR air interface or forward a part of the data to the enodeB for transmission over the LTE air interface.

Variant 3x is the preferred choice in the industry, since it has a minimal impact on the core network and avoids excessive load on the data plane of the existing enodeB [16]. Additionally, this option offers more graceful service continuity in scenarios where 5G radio coverage is lost and minimizes excessive signaling between the RAN and the core network. Since option 3x is the industry's mainstream *standard*, our work focuses on the security aspects of this widely deployed 5G NSA option.

3. Attacks on 5G NSA

In this section, we present a comprehensive literature review of known attacks on mobile networks that can theoretically be launched against 5G NSA network architectures. It is important to note that we conducted our literature exploration for known 4G attacks. For each of the attacks, we assessed if this attack is also (theoretically) possible against 5G NSA networks. Only such attacks are presented in the following.

To guide the reader through this section, we introduce a taxonomy that is motivated by a similar document that already exists for 5G SA network architectures [18]. We structure the taxonomy hierarchically and unfold it throughout this section. Concrete known attacks define the leaves in this tree structure. An overview of the complete taxonomy is provided in Figure 3.

On the highest level of this structure, attacks on 5G NSA can be divided into active attacks and passive attacks. Active attacks require the attacker to transmit signals to perform the attacks. Passive attacks rely on sniffing signals without intercepting them.

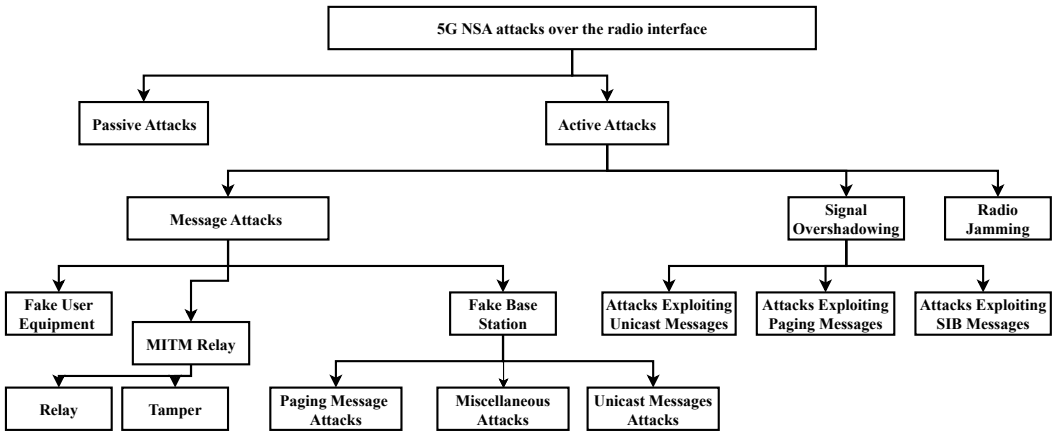

Figure 3. Taxonomy of possible attacks which can be transferred from 4G to 5G NSA networks.

3.1. Active Attacks

Active attacks on mobile networks involve adversaries who actively participate in carrying out the attack. The adversary actively injects signals or messages to influence what the UEs or the network would receive. Active attacks can be classified into three categories: radio jamming, signal shadowing, and message attacks.

3.1.1. Radio Jamming

Radio jamming is a technique of performing an active attack where the adversary disturbs the communication between a legitimate sender and a legitimate receiver by increasing the noise on the wireless channel. Depending upon the frequencies jammed by the adversary, this type of attack can be used to deny all services to a UE or may force it to downgrade to a lower generation of mobile networks [7]. An attack performed using this technique is not persistent because the system self-recovers when the attacker stops performing the attack. Further, it is challenging for an attacker not to be detected.

The attacks based on this technique are usually performed using either constant jamming or smart jamming approaches. In a constant jamming approach, the attacker jams the complete communication bandwidth over time and disturbs the communication of all victims. A smart jamming approach is targeted at specific control information, such as the Physical Broadcast Channel (PBCH) or Physical Random Access Channel (PRACH) [19]. Although smart jamming is more efficient than constant jamming, it requires the attacker to be in sync with the cell to obtain the position of control information.

3.1.2. Signal Overshadowing

Signal overshadowing is a technique where the adversary overshadows a specific message without interfering with the synchronization between the BS and the victim UE [20]. Specifically, this technique leverages the capture effect by injecting a generated subframe at a higher power to precisely overshadow the legitimate subframe. The capture effect forces the decoding of the stronger signal when several simultaneous (wireless) signals collide in the air. The injected subframes are prepared such that the UEs that receive and decode them behave based on the (malicious) information included in the generated subframes.

The victim UE involved in this attack maintains a secure signaling connection with the legitimate enodeB and the MME, as opposed to the attacks involving fake BSs, where the UE is disconnected from the legitimate core network. Although attacks based on this technique are stealthier than those employing fake BSs and man-in-the-middle (MITM) relay (see below), in practice, these attacks are difficult to perform. There are two major technical challenges. First, there is a hard dependency on time and frequency synchronization for precise overshadowing. Second, the subframe needs to be carefully prepared so that it is successfully decoded by the victim UE. In recent years, several attacks have been

reported using this technique that fall into three distinctive categories: attacks exploiting System Information Block (SIB) messages, attacks exploiting paging, and attacks exploiting unicast messages.

Attacks Exploiting SIB Messages

These attacks exploit the vulnerability arising from the lack of integrity protection for SIB messages through the signal overshadowing technique.

By performing a so-called *Signaling Storm*, an adversary storms prepared messages towards the core network by repeatedly triggering the invalid TAU procedure [20]. In order to perform this attack, the adversary first needs to overshadow a paging message with the "system_Info_Modification" field set as true, which forces the UE to read the SIB1 message. Next, it overshadows SIB1 messages using a spoofed Tracking Area Code (TAC), which forces the UE to initiate a Tracking Area Update (TAU) request toward the legitimate enodeB. Repeating the above procedure leads to a signaling storm toward the core network.

Selective DoS through Access Barring exploits the lack of integrity check for SIB messages to modify a feature in SIB2 messages that can control the number of UEs that are able to access a cell [20]. Generally, MNOs manage the amount of traffic and maintain the stability of the network under specific conditions, e.g., a disaster, by using the Barring Factor parameter in SIB2 message. In this attack, the adversary exploits this feature by setting the Barring Factor to 0 and the Barring Time to 512 s (via signal overshadowing) to restrict all data traffic and signaling originating from the UE, leading to a Denial of Service (DoS). The adversary can also use this attack to perform a persistent DoS attack by repeating the attack before the expiry of the Barring Time. Moreover, it is also possible to selectively block only the targeted services (e.g., voice calls, video conferences, and SMS) using this attack.

Attacks Exploiting Paging Messages

These are attacks that exploit the specification flaw (decision) of keeping the paging messages cryptographically unprotected.

The *DoS Attack by Overshadowing Paging with IMSI* exploits the concept of paging with IMSI using the signal overshadowing technique to perform a limited time DoS on the victim UE [20]. When a UE receives a paging message that contains its IMSI, it terminates all sessions and initiates a registration procedure. To perform the attack, the adversary injects a paging message that contains the IMSI of the victim UE at its paging occasion (via signal overshadowing), which detaches the UE from the network.

Network Downgrading Attack via CS Paging downgrades the victim UE to a 3G network by injecting a paging message with a Circuit Switched Notification (using the Serving Temporary Mobile Subscriber Identity (S-TMSI) of the victim UE) [20]. In order to perform the attack, the adversary needs to first acquire the S-TMSI of the victim UE and then inject a paging message that contains the S-TMSI using the signal overshadowing technique.

Coarse-grained tracking of a UE exploits the contention resolution technique to perform coarse-grained location tracking on the victim [20]. In order to perform the attack, the adversary first needs to inject a paging message with S-TMSI using the signal overshadowing technique. It then requires eavesdropping on the Connection Setup message sent from the legitimate BS (as a reply to the Connection Request message from the UE). If the Connection Setup message containing S-TMSI of the victim UE is received by the attacker, it infers that the victim UE is present within the coverage area of the BS.

Attack Exploiting Unicast Messages

In these attacks, the adversary forces the injection of non-integrity protected unicast messages to trigger malicious behavior. The specification allows the acceptance of some unicast messages without integrity protection to handle exceptional cases [21].

The *Service Reject Attack* exploits the specification flaw of accepting a Service Reject message without an integrity check to realize a DoS attack toward the victim UE [21]. The idea behind the attack is to overshadow the Service Accept request sent by the MME and

replace it with a Service Reject message with cause value 8 (i.e., EPS services and non-EPS services not allowed). In order to perform the attack, the adversary needs to implement a downlink decoder (sniffer) that specifically listens and decodes messages from both the enodeB and the MME so that it can correctly schedule the Reject message [22]. Upon reception of the RRC Connection Setup message, the adversary needs to continuously inject Service Reject messages on every subframe for the next 2 sec to overshadow the Service Accept message.

The *Attach Reject Attack* exploits the specification flaw of accepting the Attach Reject message without an integrity check to realize a DoS attack toward the victim UE [21]. To perform the attack, the adversary needs to replace the response to an Attach Request message on the wireless channel with an Attach Reject message [22]. The attack procedure is similar to the Service Reject Attack described above, except for the specific message that needs to be injected (i.e., Attach Reject instead of Service Reject).

The *IMSI Extractor Attack* exploits the specification flaw of accepting an Identity Request for IMSIs before the establishment of the security context to force a UE to leak its IMSI [21]. In order to perform the attack, the adversary needs to sniff traffic and wait for Connection Requests containing the Temporary Mobile Subscriber Identity (TMSI) [23]. Once the adversary receives the Connection Setup message, it needs to overshadow the message sent by the BS (e.g., Authentication Request) to the UE with an Identity Request message. Upon receiving this message, the victim UE replies with an Identity Response message containing its IMSI in plain text. The attacker needs to sniff this Identity Response containing the IMSI of the victim and modify the uplink allocation so that the legitimate BS does not receive this request.

3.1.3. Message Attacks

This is a technique of performing active attacks where the attacker sets up (and operates) fake device(s) to perform the attack. The adversary can spoof, replay, and/or tamper with traffic under its control. Message attacks are typically carried out using fake BS, fake UE, or an MITM relay.

Fake Base Station

A fake BS impersonates a legitimate BS by broadcasting system information with higher signal strength to lure a victim UE to connect to it. The adversary learns the appropriate parameters to configure the fake BS by sniffing public channels for the relevant broadcast messages. The attacks based on fake BS can be categorized into Unicast message attacks and Paging message attacks.

(A) **Unicast Message Attacks.** These are attacks where the attacker originates and sends a unicast message to the victim UE after it has camped on its cell (fake BS). The adversary exploits the fact that certain messages sent from the network are accepted by an UE without integrity protection [21]. Selected attacks in this category are described below.

- The *Downgrade Attack* allows the adversary to downgrade the user to a 2G/3G network [8]. The attack is based on the specification flaw that a UE accepts the TAU Reject message without an integrity check. Specifically, there is no need for the establishment of mutual authentication and security contexts between the UE and the network for accepting the message. In order to perform the attack, the adversary needs to operate a fake BS on a TAC different from the real enodeB to trigger a TAU message from the victim UE. Once the victim UE sends a TAU request, the fake BS replies with a TAU Reject message, including an EMM cause. If the cause included is "EPS services not allowed," the victim UE disconnects from the current network and tries to connect to a nearby 2G/3G BS if available. Later, the UE tries to reconnect to the legitimate BS after the expiry of a timer [24]. Toggling airplane mode or rebooting the phone could nullify the effect of this attack.

- The *Numb Attack* allows an adversary to severely disrupt the service of a victim UE by performing a DoS attack [12]. The attack is based on the specification flaw that a UE accepts the Authentication Reject message without an integrity check. In order to perform the attack, the adversary needs to set up a malicious enodeB (BS). Once the UE connects to the fake enodeB, it needs to reply with the Authentication Reject message, irrespective of the victim UE context. After receiving this message, any cellular services on the UE are disabled as the UE enters the "EU3 Roaming not allowed" state. Later, the UE tries to reconnect to the 4G BS after the expiry of a timer [24]. Toggling airplane mode or rebooting the phone could nullify the effect of this attack. Similar attacks are also possible with Service Reject/Attach Reject messages.
- The *Identity Leak Attack* exploits a specification flaw of accepting an Identity Request for IMSI numbers without an integrity check [21]. In order to perform the attack, the adversary needs to operate a fake BS. Once the UE connects to such a prepared BS, it needs to send an Identity Request back to the UE. Upon receipt of the Identity Request, the victim UE replies with an Identity Response message containing its IMSI in plain text.

(B) **Paging Message Attacks** Paging messages are cryptographically unprotected. A fake BS is required to perform these attacks. Selected attacks in this category are described below.

- *Hijacking Paging Channels* allows an adversary to deny any service to the UE (e.g., incoming call or SMS) [12]. To perform this attack, the adversary first needs to determine the UE's paging cycle. After that, the adversary needs to operate a fake BS and broadcast empty paging messages using higher signaling power at the paging occasions of the UE.
- The *Stealthy Kicking-off Attack* aims to force a victim UE to detach from a network surreptitiously [12]. In order to perform this attack, the adversary first needs to hijack the victim's paging channel. After that, the adversary needs to send prepared paging messages with one of the paging records containing the IMSI of the victim UE. Upon the reception of the generated paging message containing its IMSI, the UE disconnects from the EPC and sends an Attach Request message.
- The *Panic Attack* allows an adversary to inject fake emergency paging messages [12]. It could be used by a malicious organization to create a situation of artificial emergency or chaos among the public. In order to perform the attack, the adversary needs to send paging messages with empty records but with fake emergency warnings on all possible paging occasions to ensure numerous UEs are affected. The paging messages can be generated by setting the bits related to earthquake and tsunami warning system (ETWS). Upon reception of this message, the UE displays warning messages sent by the attacker. Researchers further revealed that with four fake base stations operating at one-watt power, it is possible to send fake presidential warning messages to a stadium of 50,000 seat capacity with an impressive success rate of 90 percent [9].
- The *Energy Depletion Attack* forces the victim UE to perform expensive cryptographic operations repeatedly, thus depleting its battery at a faster rate [12]. In order to perform the attack, the adversary can force the UE to carry out the expensive attach procedure repeatedly by sending a paging message containing the IMSI between two successive attach procedures. Alternatively, in case the adversary knows the Globally Unique Temporary Identifier (GUTI) of the victim, it can page the UE using the GUTI, which forces the UE to respond with a Service Request message.

Fake User Equipment

A fake UE is a device that tries to impersonate a legitimate UE. The adversaries usually use a Software-Defined Radio (SDR) along with software implementation of a UE modem to set up the fake UE. In this category, we list the attacks that mainly require a fake UE to perform the attack. However, some attacks may require a fake BS to gain initial insights, such as the victim's IMSI. Attacks that can be performed using a fake UE are listed below.

A *BTS Resource Depletion Attack* is based on the specification flaw of not verifying the subscriber/UE in the BS, i.e., the initial RRC connection procedure is unprotected. According to the standard [25], the initial authentication procedure takes place between the UE and the MME after the RRC connection procedure, thus allowing enodeB to accept connection requests from any UE. The goal of this attack is to deplete the capacity of active RRC connections at a base station and thus prevent legitimate users from connecting to it.

A *Blind DoS Attack* allows an adversary to establish an RRC connection by spoofing as the victim UE [26]. In order to perform this attack, the adversary first needs to determine the victim UE identity (S-TMSI) using a fake BS and then establish an RRC connection using this identity with the help of a fake UE. The impact of this attack varies based on the RRC connection state. When the victim UE is in the idle state, this attack changes the UE connection state in the MME to RRC connected and thus blocks any incoming traffic to the victim UE (no paging messages sent). If the victim UE is in the RRC connected state, this attack could lead to a limited time DoS attack.

An *Authentication Synchronization Failure Attack* forces the victim UE to suffer from service disruption [27]. The concept involves disrupting the attach procedure by intentionally creating a mismatch in the sequence numbers stored in the UE and the HSS. This is achieved by exploiting the sequence number during the UE sanity check. In order to perform the attack, the adversary sends several Attach Request messages using the victim's IMSI (malicious UE) but with different security capabilities between successive attach messages. Sending such Attach Request messages forces the network to drop the previous Attach Request, consider the new request as valid, and increase the sequence number in the HSS. Consequently, once the victim UE initiates the Attach Request and receives the authentication challenge from the core network, it fails the sanity check for sequence numbers and is discarded by the UE. The UE would then have to re-synchronize its sequence number by sending an authentication failure message to the EPC.

In a *Service Disruption using Authentication Request Attack*, the adversary exploits a specification flaw related to the handling of sequence numbers of the Authentication Request message [27]. In order to perform the attack, the adversary first sends an Attach Request to the MME using malicious UE (using the victim's IMSI) and captures the Authentication Request message. Later, when the adversary plans to perform the attack, it replays the old Authentication Request message toward the UE, which forces the UE to regenerate all session keys, causing the UE to discard packets directed toward it.

By conducting a *Linkability using Authentication Response Attack*, the adversary exploits different responses of the Authentication Request message to track the presence of a user in a particular cell area [27]. In order to perform the attack, the adversary needs to send an Attach Request to the MME using a malicious UE (using the victim's IMSI) and capture the Authentication Request message. Later, the adversary would have to operate a fake BS, connect to all nearby UEs, and then replay the captured Authentication Request message to all the devices. The victim UE would accept this message and reply with an Authentication Response message, while all other UEs in the cell respond with a Message Authentication Code (MAC) failure.

In the *SON poisoning* attack, the adversary exploits an implementation flaw of not verifying measurement reports sent by the UE. This attack allows the adversary to poison the SON feature of the network by injecting fake measurement reports using legitimate mobile devices as a covert channel. The attack could lead to a DoS attack against the network and the UE. It could also be used to waste network resources by generating ample X2 signaling. The adversary can perform this form of attack by either (a) setting

up rogue UE to send maliciously crafted reports or (b) setting up rogue base station(s) to create a false radio environment around uncompromised UEs, causing them to send attacker-wanted reports to the legitimate base station. Notably, networks with robust SON implementations can mitigate such attacks [18], while those with poor SON implementation remain vulnerable. Although this attack can be performed using either a fake base station or rogue UE, we have classified it under Fake UE to simplify the classification.

MITM Relay

An MITM relay consists of a fake enodeB and a fake UE connected locally or remotely (e.g., via another communication technology). The fake enodeB part of the relay is used to lure victim UE to connect to the relay, while the fake UE part acts as a legitimate UE towards the core. The adversary can replay the messages between victim UE and the legitimate enodeB with and without tampering.

(A) **Tampering**. In these attacks, the MITM attacker tampers with some messages before sending them to the recipient. Selected attacks belonging to this category are described below.

- In an *Alter Attack*, the adversary exploits the lack of integrity protection for user plane data to perform a chosen ciphertext attack [28]. Specifically, the adversary performs a Domain Name System (DNS) redirection attack by manipulating the destination IP address of a DNS request, redirecting the request to a malicious server. In order to perform the attack, the adversary operates a malicious relay between the UE and the enodeB and applies a manipulation mask on the DNS packet to change its destination IP address to a malicious IP address. Then, it forwards the packets to the external network (e.g., the Internet). At the core network, the malicious DNS request is decrypted and routed to the malicious DNS server, which replies with a spoofed DNS response.
- An *IMP4GT Attack* is an extension of the Alter attack. In this attack, the adversary exploits the missing integrity protection for user plane data and the reflection mechanism of the IP stack mobile operating system to impersonate a user toward the network and vice versa [29]. In the uplink impersonation variant, the adversary can access the Internet using the victim's IP address. In the downlink variant, the adversary establishes a TCP/IP connection to the phone to bypass the firewall mechanisms.
- The *Null Ciphering Attack* [30] allows the UE to establish an unencrypted radio connection with gnodeB. It occurs due to the implementation flaw within the network of not rejecting UEs with invalid UE Additional Security Capabilities and the implementation flaw in the UE of not verifying replayed UE Additional Security Capabilities and Hash of the Attach message. These additional capabilities specify information about the supported algorithms for protecting the data transferred over gnodeB in 5G NSA. The capabilities are sent in the Attach Request message and are later replayed back to detect manipulation. In order to perform the attack, the adversary needs to set up an MITM relay to lure the UE to connect to it. Once the UE sends the Attach request message to the MITM relay, the attacker modifies the UE Additional Security Capabilities to include support only for null ciphering (NEA0). The network receives this message and replays the UE Additional Security Capabilities back to the UE in an integrity-protected NAS Security mode command without checking the capabilities. In the next phase, the MME would inform the target gnodeB about the additional security capabilities. Since the only ciphering algorithm left in the 5G security capability set is NEA0, enodeB would instruct the UE to establish an unencrypted radio connection to gnodeB via the RRC Connection Reconfiguration message. Note that it is also possible to perform a *battery draining attack on IoT devices* (implementation flaw) or a DoS attack [8] (implementation flaw) using a similar attack procedure.

- In the *Radio Service Hijacking* attack [8], the adversary exploits an implementation flaw where the enodeB requests the UE Radio Capabilities before establishing the RRC security. The enodeB requests the Radio Capability from the UE by sending a UECapabilityEnquiry message, and the UE responds with the UECapabilityInformation message. In order to perform the attack, the adversary operates an MITM relay at a different TAC and lures the UE into initiating a new registration procedure via the relay. After the NAS security setup, the relay forwards the UECapabilityEnquiry message to the UE, receiving a plain text UECapabilityInformation response. The relay then alters this message to downgrade the CAT category and disable several features and supported bands. The altered message is then forwarded to the legitimate network, and the UE is released using an RRC release message. These altered capabilities are stored in the network for future use, leading to lower data rates. Moreover, the UE would be handed over to a 3G/2G base station during voice calls due to missing 4G/5G bands.

(B) **Relaying**. In these attacks, the MITM attacker relays messages (or forwards messages) between the victim UE and the legitimate enodeB without tampering with them. An attack that belongs to this category is described below.

- An *Authentication Relay Attack* allows a malicious UE to connect to the EPC without possessing proper credentials [12]. The implications include the ability to spoof a location to the core network (location poisoning) as well as conduct DoS attacks. This attack is performed using an MITM relay such that the malicious UE and malicious enodeB parts of the relay are connected via a private connection. In order to perform the attack, the adversary first needs to force the UE to disconnect from the EPC and connect to the fake BS part of the relay. Once the victim UE connects to the fake BS and sends an Attach Request, the malicious enodeB forwards it to the remote malicious UE, and the malicious UE forwards it to the legitimate BS. Similarly, the malicious UE forwards the reply sent by the core network to the malicious BS, which forwards it to the victim UE. Following the same principle, other messages involved in the attach procedure are exchanged, thus allowing a malicious UE to connect to the core network without proper credentials.

3.2. Passive Attacks

In passive attacks on mobile networks, the adversary is only passively involved in the attack. Generally, the adversary silently sniffs the signals/messages exchanged between the UE and the BS using a passive sniffer. Depending upon the attack, the adversary may need to sniff the control and/or the data plane traffic.

The *Passive Fingerprinting Attack* allows the adversary to classify the baseband modem of phones by passively analyzing the uplink control traffic [23,31]. Specifically, the attacker needs to sniff core network capabilities sent in plain text in the Attach Request message. The adversary first needs to build a reference model that classifies the baseband modem based on their capabilities. Later, whenever required, the adversary needs to sniff the capabilities of the UE and compare them to the reference model to classify the baseband modem.

In a *Passive Localization Attack*, the adversary uses information from unencrypted Timing Advance command responses and the time of arrival of messages at the sniffer to localize a victim UE [23]. The adversary should have access to a combined custom uplink/downlink LTE sniffer to extract the required information [31]. The attack narrows down the location of a victim to two possible areas at the intersection of an ellipse and a wide ring.

In the *ReVoLTE* attack [32], the adversary exploits an implementation flaw of reusing key streams in successive calls to recover the contents of an encrypted VoLTE call. Generally, when a UE connects to a base station, a new user-plane key is negotiated for the radio connection. However, if two consecutive calls occur within a single radio connection, key

stream reuse may occur, depending on the network operator's implementation. The attack capitalizes on this weakness, taking advantage of the XOR operation used in generating an encrypted ciphertext from the keystream and plain text. In order to perform the attack, the adversary first needs to sniff the first call (target call) directed towards the victim. Subsequently, upon detecting the end of the target call, it needs to immediately place a keystream call (second call) toward the victim. For the second call, the attacker needs to record the unencrypted sound (known plaintext) and sniff encrypted radio traffic. To decrypt the target call, the adversary needs to compute the keystream by XORing the contents of the second call (unencrypted sound and encrypted voice). Once it has access to the keystream, it decrypts the first call by XORing the first call's ciphertext with this keystream. Note that the attacker needs to engage the victim in conversations that last for the same time as the previous call to retrieve all of the previous call's content.

Passive attacks on 5G NSA that require sniffing control plane data can be carried out using 4G sniffing tools because the non-stand-alone version of 5G uses the control plane from 4G. However, attacks that require sniffing the data plane are currently difficult to perform using open-source tools.

Sniffing 5G traffic using open-source tools presents greater complexity compared to earlier technologies, particularly concerning hardware requirements. A 5G sniffer should be capable of processing RF signals exceeding 24 GHz, as 5G operates across two frequency ranges: sub-6GHz and millimeter wave [33]. Notably, even high-end SDRs like the USRP X410 can currently only support frequencies up to 8 GHz.

Additionally, if the operator plans to send data via both enodeB and gnodeB, the attacker would need two sniffers to record the data, which further complicates the process of passively sniffing 5G NSA traffic.

4. Motivation

As described in Section 2, the core network (EPC) and the control plane segment of the RAN in 5G NSA are based on LTE. Therefore, theoretically, the NSA version of 5G is likely to be vulnerable to known 4G attacks.

Some research has already been carried out to practically verify the working of 4G attacks on 5G NSA. The work in [34] validated three vulnerabilities that are based on implementation flaws on 5G: key-stream reuse, null-ciphering, and IMS IP security off. The work in [35] tried to verify two design flaws and several implementation flaws on 5G NSA. The authors verified the RRC Blind DoS and EPC scanning attacks on two commercial networks. Similarly, the work in [36] also analyzed the possibility of performing the Blind DoS Attack on 5G NSA and suggested some countermeasures. Furthermore, one more work [30] recently verified the Null Ciphering attack on 5G NSA.

However, so far, no literature has systematically explored the state of the art and provided a comprehensive taxonomy of possible attacks on 5G NSA over the radio interface. We addressed this gap in the literature and presented the first taxonomy of attacks on 5G NSA in Section 3.

The sheer number of theoretically possible attacks on 5G NSA motivated us to the next step. We selected and implemented three attacks that have severe consequences for the user and have not been practically verified on 5G NSA architectures yet.

The attacks we selected are the *Downgrade Attack*, the *Numb Attack*, and the *IMSI Leak Attack*. These are active message attacks using a fake BS (cf. Section Fake Base Station).

5. Methodology

We implemented an experimental testbed to practically verify the working and persistence of the above-discussed attacks on 5G NSA. Our experimental testbed consisted of a commercial 5G NSA BS, a fake 4G BS based on open-source software and SDRs, and a 2G BS also based on open-source software and an SDR. Figure 4 provides an abstract representation of the testbed, illustrating the interconnected components involved.

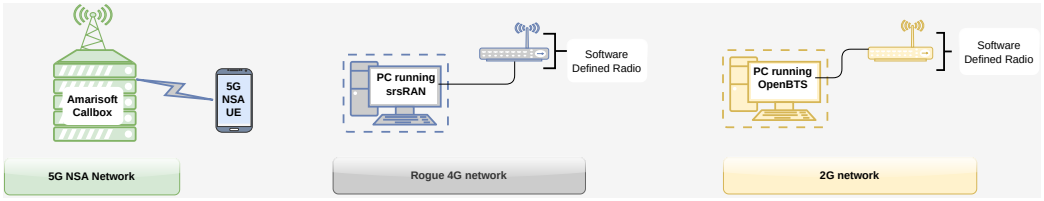

Figure 4. Schematic representation of the implemented experimental testbed, featuring a 5G NSA network, a 5G NSA UE, a fake 4G network, and a 2G network.

5.1. Components

In the following, we provide more details about the components and configurations involved in the testbed. The components involved in the testbed are shown in Figure 5.

Figure 5. Our experimental testbed consisting of an Amarisoft Call Box Classic (**left**), two SDRs, two personal computers (PCs), test SIM cards, and Commercial Off-the-Shelf (COTS) UE (**right**).

- **5G NSA Network** We use the Amarisoft Callbox Classic [37] as a 5G NSA network. The Callbox provides a closed-source 3GPP compliant enodeB, a gnodeB for the RAN, and an EPC and 5GC for the core network. It can be configured to act as a mobile network for different generations and standards (i.e., 5G SA, 5G NSA, LTE M, LTE NB-IoT).
- **Fake 4G Network** Since 5G NSA is based on LTE control traffic, a fake 4G network can act as a fake BS for a UE connected to the 5G NSA network. We have set up the malicious enodeB by adapting the srsRAN [38] software package. srsRAN is an open-source software radio suite for 4G implemented in C/C++. The software runs on a Linux-based PC (Intel Core i5 7th Gen laptop). A USRP B210 [39] acts as the radio front end for our fake 4G network. It is connected to the host-based PC running the modified srsRAN software. The fake BS needs to be configured to broadcast Mobile Number Code (MNC) and Mobile Country Code (MCC) numbers identical to the 5G NSA BS. It must also be operated using higher power than nearby enodeBs to lure the victim UE to connect to it. Our laboratory setup consists of only one 5G NSA BS under our control, operating at a particular frequency. Operating the fake 4G BS at this frequency could be considered analogous to a real-world situation, where the attacker usually operates the fake BS at the highest priority frequency.
- **2G Network** We have set up a 2G network using the OpenBTS [40] framework. It runs on a Linux-based PC (Intel Core i5 7th Gen laptop). OpenBTS is a C++ application that implements the GSM cellular stack. A USRP B210 acts as the radio front end for our 2G network. It is connected to the host-based PC running the OpenBTS software.

- **COTS UEs** We used the following eight 5G NSA COTS UEs for the tests: Samsung A40, Huawei P40, Huawei Mate40 Pro, Oppo Find X3 Neo 5G, Google Pixel 7 Pro, Samsung Galaxy S20FE, Samsung Galaxy S21FE and iPhone 12. The UEs are connected to the Amarisoft Callbox using test sim cards that were shipped with the system.

5.2. Procedure to Verify the Attacks

In order to verify the attacks, we first ensured that the UE was connected to the 5G NSA network. Once the UE was successfully connected, we operated the fake 4G base station using the required parameters discussed in Section 5.1. Additionally, the fake BS was operated using code modifications that force it to send a TAU Reject/Authentication Reject/Identity Request, depending on the attack being examined.

Next, we verified if the UE disconnected from the 5G NSA network and connected to the fake 4G network. The UE's loss of connection to the 5G base station was validated by observing the 5G sign disappear on the UE. The Amarisoft logs also help to verify this fact. The UE's attempt to connect to the fake BS was confirmed by viewing the initial UE message on the srsEPC console.

Subsequently, we closed the srsEPC and srsENB consoles and verified whether the fake BS sent the intended reject message by reviewing the pcap file associated with srsEPC. We then examined the behavior of the UEs.

Furthermore, we verified if the UE has implemented a timer to recover automatically from the *Numb* and *Downgrade Attacks*. In accordance with the guidelines set forth by the 3GPP SA3 group, a back-off timer was recommended as a means to recover from potential attacks stemming from unauthenticated rogue messages [18,41,42]. Our evaluation aimed to ascertain whether the UEs promptly resumed normal operation after the attack or remained in a compromised state.

6. Results

For all the performed tests, the UEs disconnected from the 5G network and connected to the fake BS, which was verified by the procedure described in Section 5.2. Additionally, the respective reject messages were also visible in the pcap file related to srsEPC. The behavior of the tested UEs upon receiving the reject message is described below.

The IMSI Leak attack was verified on four COTS UEs. All of them leaked their IMSIs. The Numb attack was tested on eight COTS UEs. Only four of these examined UEs had implemented a mitigation strategy to immediately reconnect to the 5G network once the fake base station was shut down. This result is particularly interesting since most of the 4G UEs tested before [22,43] did not quickly recover from such attacks.

The Downgrade attack was tested on eight COTS UEs. Among these, four of the tested UEs did not recover from the attack and remained linked to the 2G base station. Conversely, the remaining four UEs promptly re-established their connection with the 5G network once the fake base station was deactivated. The results of all three attacks are summarized in Table 1.

Table 1. Results for the IMSI Leak, Numb, and Downgrade attacks.

UE	IMSI Leaked	Numb Attack (Quick Recovery)	Downgrade Attack (Quick Recovery)
Samsung Galaxy A40	Yes	No	No
Huawei P40	Yes	Yes	Yes
Huawei Mate40 Pro	Yes	Yes	Yes
Oppo Find X3 Neo 5G	Yes	No	No
Google Pixel 7 Pro	Not tested	Yes	Yes
Samsung Galaxy S20FE	Not tested	No	No
Samsung Galaxy S21FE 5G	Not tested	Yes	Yes
iPhone 12	Not tested	No	No

7. Summary and Discussion

5G networks are considered a cornerstone for the information exchange in our digital mobile societies. While the goal is to deploy 5G Stand-Alone networks to replace the LTE technology, 5G Non-Stand-Alone networks are widely in use to provide a smooth transition phase. The timeline for a complete shift from 5G NSA to 5G SA remains uncertain, underscoring the importance of 5G NSA security.

Therefore, in this work, we investigate potential attacks against 5G NSA networks, specifically over the radio interface. Conducting an extensive literature review, we compiled the first taxonomy of possible attacks against 5G NSA networks and categorized them based on the attack vector. At the highest level, our taxonomy classifies attacks based on the attacker's capabilities, distinguishing between active or passive attacks. Within the realm of active attacks, we identified three techniques: radio jamming, signal overshadowing, and message attacks. Signal overshadowing attacks are grouped by the underlying common vulnerability they exploit. Message attacks involve three types of rogue devices—fake base station, fake UE, and MITM relay. Each rogue device is associated with potential attacks, which are further classified based on additional criteria. These rogue devices can be deployed using open-source hardware and software [11,42]. Furthermore, we provide a succinct summary of all the attacks encompassed in our taxonomy, serving as a comprehensive reference and an analytical resource.

Notably, our work reveals that a significant number of attacks from 4G networks can potentially be transferred to 5G NSA networks. To assess previously unexplored threats in 5G NSA networks, we selected and implemented three attacks. These attacks could be conducted with affordable resources and pose severe consequences for the user. We constructed a testbed and examined common 5G COTS smartphones to determine if they are vulnerable to these attacks. Our findings underscore the efficacy of these attacks. Specifically, the IMSI Leak attack performed as anticipated on all tested UEs with no apparent avenue for security patching in 5G NSA networks. This raises significant concerns about the ease of tracking individuals on current 5G networks. Regarding the Downgrade and Numb attacks, our findings indicated that half of the tested UEs did not employ a quick recovery timer to mitigate the effects of these attacks.

For companies planning to invest in private 5G networks [13] (Campus Networks) and having flexibility in choosing between 5G SA and 5G NSA, we highly recommend opting for 5G SA over 5G NSA due to the described attacks in this work. Additionally, we advise thorough testing of the UEs intended for deployment to ensure they possess a fast recovery mechanism against attacks based on unauthenticated Reject [21] messages such as Authentication Reject messages, which could lead to a DoS attack and hamper the working on important tasks.

Overall, we have demonstrated that current 5G networks can provide the user with a false sense of security since the new 5G security mechanisms are only available in 5G Stand-Alone networks.

Multiple future tasks arise from the results of this study. Additional attacks that have been presented in this work should be validated against 5G NSA networks while the variety of investigated UEs should be increased. A valuable contribution might be to integrate the attacks into a security audit framework to automatically conduct such tests with every new generation of UEs to help track the vulnerabilities and mitigation capabilities of different UE implementations over time [26,44].

Author Contributions: Conceptualization, M.S.W., M.R. and M.K.; methodology, M.S.W., M.R. and M.K.; software, M.S.W. and T.H.; validation, M.S.W. and T.H.; investigation, M.S.W. and T.H.; writing—original draft preparation, M.S.W., M.R., M.K. and T.H.; writing—review and editing, M.S.W., M.R. M.K. and T.H.; supervision, M.R. and M.K.; project administration, M.R. and M.K.; funding acquisition, M.R. and M.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been partially funded by the Federal Ministry for Digital and Transport of the Federal Republic of Germany (Förderkennzeichen 165GU054B, IndustrieStadtpark: 5G-Anwendungen im Projektgebiet IndustrieStadtpark Troisdorf) and by the German Federal Office for Information Security of the Federal Republic of Germany (BSI) under project (Förderkennzeichen 01MO23003B, PlusMoSmart) funding reference number. The authors alone are responsible for the content of this paper.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

3GPP	3rd Generation Partnership Project
BS	base station
COTS	Commercial Off-the-Shelf
CapEx	Capital Expenditure
DoS	Denial of Service
DNS	Domain Name System
EPC	Evolved Packet Core
HSS	Home Subscriber Service
eMBB	Enhanced Mobile Broadband
ETWS	earthquake and tsunami warning system
GUTI	Globally Unique Temporary Identifier
IMSI	International Mobile Subscriber Identity
TMSI	Temprary Mobile Subscriber Identity
LTE	Long-Term Evolution
MAC	Message Authentication Code
MNO	Mobile Network Operator
MCC	Mobile Country Code
MNC	Mobile Number Code
NSA	Non-Stand-Alone
NAS	Non-Access Stratum
NFV	Network Functions Virtualization
NR	New Radio
MITM	man-in-the-middle
MN	Master Node
MME	Mobility Management Entity
mMTC	Massive Machine Type Communications
PC	personal computer
P-GW	PDN Gateway
RAN	Radio Access Network
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SN	Secondary Node
SA	Stand-Alone
SIB	System Information Block
SIM	Subscriber Identity Module
SIB	System Information Block
S-TMSI	Serving Temporary Mobile Subscriber Identity
S-GW	Serving Gateway
PRACH	Physical Random Access Channel
PBCH	Physical Broadcast Channel
TAC	Tracking Area Code
TAU	Tracking Area Update
TMSI	Temporary Mobile Subscriber Identity
URLLC	ultra-reliable low-latency communication
UE	User Equipment

References

1. Ericsson. *Ericsson Mobility Report*; Technical Report EAB-22:010742 Uen Rev D; Ericsson: Stockholm, Sweden, 2023.
2. Bundesnetzagentur. Pressemitteilung—Bundesnetzagentur Aktualisiert Darstellung der Netzabdeckung mit 5G. Available online: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/2022/20221123_5G.pdf?__blob=publicationFile&v=2 (accessed on 30 November 2023)
3. Zhang, X.; Kunz, A.; Schröder, S. Overview of 5G security in 3GPP. In Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 18–20 September 2017; pp. 181–186. [CrossRef]
4. Cao, J.; Ma, M.; Li, H.; Ma, R.; Sun, Y.; Yu, P.; Xiong, L. A Survey on Security Aspects for 3GPP 5G Networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 170–195. [CrossRef]
5. GSA. 5G-Standalone November 2023 Summary. 2023. Available online: https://gsacom.com/paper/5g-market-snapshot-february-2023 (accessed on 30 November 2023).
6. Kliks, A.; Dryjanski, M.; Ram, V.; Wong, L.; Harvey, P. Towards Autonomous Open Radio Access Networks. *ITU J. Future Evol. Technol.* **2023**, *4*, 251–268. [CrossRef]
7. Park, S.; Shaik, A.; Borgaonkar, R.; Seifert, J.P. Anatomy of Commercial IMSI Catchers and Detectors. In Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society (WPES'19), London, UK, 11 November 2019; pp. 74–86. [CrossRef]
8. Shaik, A.; Borgaonkar, R.; Park, S.; Seifert, J.P. 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 (WiSec '19), Miami, FL, USA, 15–17 May 2019; pp. 221–231. [CrossRef]
9. Lee, G.; Lee, J.; Lee, J.; Im, Y.; Hollingsworth, M.; Wustrow, E.; Grunwald, D.; Ha, S. This is Your President Speaking: Spoofing Alerts in 4G LTE Networks. In Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '19), Seoul, Republic of Korea, 17–21 June 2019; pp. 404–416. [CrossRef]
10. Mjølsnes, S.F.; Olimid, R.F. Easy 4G/LTE IMSI Catchers for Non-Programmers. In Proceedings of the Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, 8–30 August 22017; Rak, J., Bay, J., Kotenko, I., Popyack, L., Skormin, V., Szczypiorski, K., Eds.; Springer: Cham, Switzerland, 2017; Volume 10446. [CrossRef]
11. Rupprecht, D. Enhancing the Security of 4G and 5G Mobile Networks on Protocol Layer Two. Ph.D. Thesis, Ruhr-Universität Bochum, Universitätsbibliothek, Bochum, Germany, 2021. [CrossRef]
12. Hussain, S.; Chowdhury, O.; Mehnaz, S.; Bertino, E. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In Proceedings of the 25th Annual Network and Distributed System Security Symposium, (NDSS), San Diego, CA, USA, 18–21 February 2018. [CrossRef]
13. Aijaz, A. Private 5G: The Future of Industrial Wireless. *IEEE Ind. Electron. Mag.* **2020**, *14*, 136–145. [CrossRef]
14. 3GPP. Universal Mobile Telecommunications System (UMTS); Numbering, Addressing and Identification: 3GPP TS 23.003 V16.3.0 Release 16 (2020-10). Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729 (accessed on 30 November 2023).
15. El Rhayour, A.; Mazri, T. 5G Architecture: Deployment scenarios and options. In Proceedings of the 2019 International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Rome, Italy, 27–29 November 2019; pp. 1–6. [CrossRef]
16. Ondrusova, S.; Kim, D. *5G Implementation Guidelines: NSA Option 3*; Technical Report; GSM Association: London, UK, 2020.
17. Liu, G.; Huang, Y.; Chen, Z.; Liu, L.; Wang, Q.; Li, N. 5G Deployment: Standalone vs. Non-Standalone from the Operator Perspective. *Comm. Mag.* **2020**, *58*, 83–89. [CrossRef]
18. 3GPP. Study on 5G Security Enhancement against False Base Stations (FBS); Technical Report (TR): 3GPP TR 33.809 V18.1.0 Release 18 (2023-09). Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729 (accessed on 30 November 2023).
19. Aziz, F.M.; Shamma, J.S.; Stüber, G.L. Resilience of LTE networks against smart jamming attacks. In Proceedings of the 2014 IEEE Global Communications Conference, Austin, TX, USA, 8–12 December 2014; pp. 734–739. [CrossRef]
20. Yang, H.; Bae, S.; Son, M.; Kim, H.; Kim, S.M.; Kim, Y. Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE. In Proceedings of the 28th USENIX Conference on Security Symposium, Santa Clara, CA, USA, 14–16 August 2019; pp. 55–72.
21. 3GPP. Universal Mobile Telecommunications System (UMTS); LTE; 5G; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Technical Specification (TS): 3GPP TS 24.301 V15.6.0 Release 15 (2019-04). Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729 (accessed on 30 November 2023).
22. Erni, S.; Kotuliak, M.; Leu, P.; Roeschlin, M.; Capkun, S. AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks. In Proceedings of the 28th Annual International Conference on Mobile Computing And Networking (MobiCom '22), Sydney, Australia, 17–21 October 2022; pp. 743–755. [CrossRef]
23. Kotuliak, M.; Erni, S.; Leu, P.; Röschlin, M.; Capkun, S. LTrack: Stealthy Tracking of Mobile Phones in LTE. In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), Boston, MA, USA, 10–12 August 2022; pp. 1291–1306. [CrossRef]
24. 3GPP. Digital Cellular Telecommunications System (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Mobile Radio Interface Layer 3 Specification; Core Network Protocols; Technical Specification (TS): 3GPP TS 24.008: V13.0.0 Release 13 (2016-10). Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729 (accessed on 30 November 2023).

25. 3GPP. Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification; Technical Specification (TS): 3GPP TS 36.331 V13.0.0 Release 13 (2016-01). Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729 (accessed on 30 November 2023).
26. Kim, H.; Lee, J.; Lee, E.; Kim, Y. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1153–1168. [CrossRef]
27. Karim, I.; Hussain, S.; Bertino, E. ProChecker: An Automated Security and Privacy Analysis Framework for 4G LTE Protocol Implementations. In Proceedings of the 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), Virtual, 7–10 July 2021; pp. 773–785. [CrossRef]
28. Rupprecht, D.; Kohls, K.; Holz, T.; Pöpper, C. Breaking LTE on Layer Two. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1121–1136. [CrossRef]
29. Rupprecht, D.; Kohls, K.; Holz, T.; Pöpper, C. IMP4GT: IMPersonation Attacks in 4G NeTworks. In Proceedings of the 27th Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 23–26 February 2020. [CrossRef]
30. Karakoc, B.; Fürste, N.; Rupprecht, D.; Kohls, K. Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G. In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23), Guildford, UK, 29 May–1 June 2023; pp. 97–108. [CrossRef]
31. Kotuliak, M. LTE Monitoring. Master's Thesis, ETH Zurich, Zurich, Switzerland, 2020. [CrossRef]
32. Rupprecht, D.; Kohls, K.; Holz, T.; Pöpper, C. Call Me Maybe: Eavesdropping Encrypted LTE Calls with ReVoLTE. In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), Boston, MA, USA, 12–14 August 2020; USENIX Association: Berkeley, CA, USA, 2020; pp. 73–88.
33. Hoang, T.D.; Park, C.; Son, M.; Oh, T.; Bae, S.; Ahn, J.; Oh, B.; Kim, Y. LTESniffer: An Open-Source LTE Downlink/Uplink Eavesdropper. In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23), Guildford, UK, 29 May–1 June 2023; pp. 43–48. [CrossRef]
34. Kwon, S.; Park, S.; Cho, H.; Park, Y.; Kim, D.; Yim, K. Towards 5G-Based IoT Security Analysis against Vo5G Eavesdropping. *Computing* **2021**, *103*, 425–447. [CrossRef]
35. Park, S.; Kim, D.; Park, Y.; Cho, H.; Kim, D.; Kwon, S. 5G Security Threat Assessment in Real Networks. *Sensors* **2021**, *21*, 5524. [CrossRef] [PubMed]
36. Park, S.; You, I.; Park, H.; Kim, D. Analyzing RRC Replay Attack and Securing Base Station with Practical Method. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22), Vienna, Austria, 23–26 August 2022. [CrossRef]
37. Amarisoft. AMARI Callbox Classic Datasheet. 2021. Available online: https://www.amarisoft.com/app/uploads/2021/10/AMARI-Callbox-Classic.pdf (accessed on 30 November 2023).
38. SRS. srsRAN—Open Source SDR 4G/5G Software Suite from Software Radio Systems. 2023. Available online: https://github.com/srsran/ (accessed on 30 November 2023).
39. Ettus Research. USRP B210 Datasheet. Available online: https://www.ettus.com/all-products/ub210-kit/ (accessed on 30 November 2023).
40. Networks, R. Getting Started with OpenBTS. Available online: https://github.com/RangeNetworks/openbts (accessed on 30 November 2023).
41. 3GPP SA3. S3-152498; Anaheim, US *LS on Backoff Timer*; Technical Report S3-152498. 2015. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729 (accessed on 30 November 2023).
42. Shaik, A. Towards Secure 4G and 5G Access Network Protocols. Ph.D. Thesis, Technische Universität Berlin, Berlin, Germany, 2020. [CrossRef]
43. Erni, S. Protocol-Aware Reactive LTE Signal Overshadowing and its Applications in DoS Attacks. Master's Thesis, ETH Zurich, Zurich, Switzerland, 2020. [CrossRef]
44. Garbelini, M.E.; Shang, Z.; Chattopadhyay, S.; Sun, S.; Kurniawan, E. Towards Automated Fuzzing of 4G/5G Protocol Implementations Over the Air. In Proceedings of the GLOBECOM 2022—2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 86–92. [CrossRef]