

# SoK: Evaluating 5G-Advanced Protocols Against Legacy and Emerging Privacy and Security Attacks

Stavros Eleftherakis  
stavros.eleftherakis@imdea.org  
Imdea Networks Institute  
Universidad Carlos III de Madrid  
Madrid, Spain

Domenico Giustiniano  
domenico.giustiniano@imdea.org  
Imdea Networks Institute  
Madrid, Spain

Nicolas Kourtellis  
nicolas.kourtellis@keysight.com  
Keysight  
Barcelona, Spain

## Abstract

Ensuring user privacy remains a critical concern within mobile cellular networks, particularly given the proliferation of interconnected devices and services. In fact, a lot of user privacy issues have been raised in 2G, 3G, and 4G networks. Acknowledging these concerns, 3GPP has prioritized addressing these issues in the development of 5G, implementing numerous modifications to enhance user privacy since 5G Release 15. In this systematization of knowledge paper, we first provide a framework for studying privacy and security related attacks in cellular networks, setting as privacy objective the User Identity Confidentiality defined in 3GPP standards. Using this framework, we discuss existing privacy and security attacks in pre-5G networks, analyzing the weaknesses that lead to these attacks. Furthermore, we thoroughly study the security characteristics of 5G up to the latest 5G-Advanced Release 19, and examine mitigation mechanisms of 5G to the identified pre-5G attacks. Afterwards, we analyze how recent 5G attacks try to overcome these mitigation mechanisms. Finally, we identify current limitations and open problems in security of 5G, and propose directions for future work.

## CCS Concepts

• Security and privacy → Mobile and wireless security.

## Keywords

Cellular Networks, Wireless, Security, Privacy

## ACM Reference Format:

Stavros Eleftherakis, Domenico Giustiniano, and Nicolas Kourtellis. 2025. SoK: Evaluating 5G-Advanced Protocols Against Legacy and Emerging Privacy and Security Attacks. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2025)*, June 30–July 3, 2025, Arlington, VA, USA. ACM, New York, NY, USA, 15 pages. <https://doi.org/10.1145/3734477.3734716>

## 1 Introduction

The number of smartphone mobile network subscriptions worldwide reached almost 6.4 billion in 2022, and is forecast to exceed 7.7 billion by 2028 [1]. However, the fact that smartphones and cellular networks have become a fundamental aspect of our lives raises an important question: *How do we protect the privacy of cellular network*

*users?* Vast literature (see [2–5] for some surveys) demonstrated that 4G/LTE networks and their predecessors (2G, 3G) are vulnerable to various security and privacy attacks for the User Equipment (UE). Specifically, attacks were shown to violate different properties of UE Identity Confidentiality (Sec. 5.1 of [6, 7]), such as identity disclosure [8–10], and location privacy [11–13]. Some attacks were demonstrated in 5G early versions and even with cheap commodity equipment and open-source code implementations [14, 15].

Indeed, it is a challenge for the current and future 5G networks to improve or mitigate the pre-5G networks’ vulnerabilities, thus enhancing user privacy [3, 16–22]. Consequently, the 3rd Generation Partnership Project (3GPP) has addressed these issues after 5G Release 15, through Technical Reports (TRs), which present study outcomes, and by introducing changes in the 5G Security Technical Specifications (TSs), which define normative requirements for the standard [23]. That said, recent surveys on the topic [3, 18, 20, 24] include only theoretical ideas about 5G privacy mechanisms, since they were written before or concurrently with the older, 5G Release 15. Other surveys focused on specific use cases, such as the application of Machine Learning algorithms in the 5G Physical layer [25, 26], the security of the Early Data Transmission 5G mechanism [27] or the security of alternative computing paradigms (e.g., catalytic computing) in 5G [28]. Finally, [21, 22] analyzed previous cellular generations’ attacks and studied corresponding mitigation mechanisms (MMs) offered by 5G, but were not informed about new 3GPP Releases, recent 5G measurement studies [29–32] and privacy attacks [10, 33–35].

In fact, an in-depth study of current literature on this topic raised further questions: 1) What vulnerabilities did the attacks in past cellular generations exploit, and what were the privacy implications of each? 2) What MMs have been introduced in the new release of 5G to overcome such weaknesses? 3) What gaps still remain for future exploration in the topic of 5G Security? 4) How do recent 5G specific attacks take advantage of them? In order to answer these questions, we present this systemization of knowledge (SoK) paper. We first propose a framework to study the efficiency of current cellular generation security aspects, considering well-studied adversaries from past cellular generations, under specific user privacy objectives. Second, we examine the resilience of new 5G security features up to Release 19, which corresponds to the second phase of 5G standardization known as 5G-Advanced [36], against attacks inherited from previous generations. Third, we analyze the specification status of these security features in the 3GPP standards, classifying them as optional or mandatory. Fourth, we raise open questions and gaps for future work.

With this SoK, our contributions are as follows:

- We define a framework for analyzing privacy-related attacks, setting the User Identity Confidentiality defined in 3GPP as our privacy objective (Sec. 3).
- We describe 12 existing pre-5G attacks (2G, 3G, 4G/LTE) that violate User Identity Confidentiality, and highlight 13 vulnerabilities or weaknesses that lead to them (Sec. 4).
- We discuss security enhancements of 5G and mention 11 MMs that are proposed against the aforementioned attacks (Sec. 5).
- We describe 8 recent 5G attacks along with their corresponding vulnerabilities, and the degree they are mitigated by the existing 5G MMs (Sec. 6).
- We give a didactic summary of our results from Sec. 4, 5 and 6 in Table 1.
- We discuss key takeaways of our work and outline future research directions (Sec. 7).

## 2 Background

### 2.1 5G Cellular Network Infrastructure

Here, we give an overview of the Cellular Network infrastructure, referring to the main entities and their properties.

**User Equipment (UE):** The UE consists of the Mobile Equipment (ME) and USIM card. It is used by consumers to access mobile services and applications.

**Radio Access Network (RAN):** The Radio Access Network consists of Base Stations (BSs) that are separated into distinct Tracking Areas (TAs). The Radio Resource Control (RRC) protocol manages the establishment, maintenance, and release of radio connections between the User Equipment (UE) and the RAN [37].

**Core Network (CN):** The Core Network consists of different entities called Network Functions (NFs), that are responsible for a variety of network services and functionalities. The Non-Access Stratum (NAS) protocol manages signaling procedures and messages between the UE and the CN [38].

### 2.2 Identifiers in 5G Cellular Networks

Cellular networks use permanent and temporary identifiers to recognize different entities, and especially the UE at hand.

The International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) are the key permanent identifiers. The IMSI, linked to the USIM card, enables CN authentication, and was transmitted in plaintext in 2G, 3G, and 4G. IMSI is composed of three parts: the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Subscriber Identification Number (MSIN). IMEI is the identifier of the Mobile Equipment (ME), manufactured on the device during its production. Both of them are global and privacy-sensitive. 5G replaces IMSI with Subscription Permanent Identifier (SUPI) [39], which must not be transmitted in plaintext, except for emergency cases [23]. The Permanent Equipment Identifier (PEI) is the 5G equivalent of the IMEI [40].

Regarding temporary identifiers, 5G introduces Subscription Concealed Identifier (SUCI) [39], a privacy-preserving version of the SUPI generated by the USIM. Further, the CN assigns a temporary identifier to the UE for their communication (e.g., paging procedures). In the past, many terminologies have been used for this: Temporary Mobile Subscriber Identity (TMSI) in 2G and 3G, Globally Unique Temporary Identity (GUTI) or TMSI in 4G and

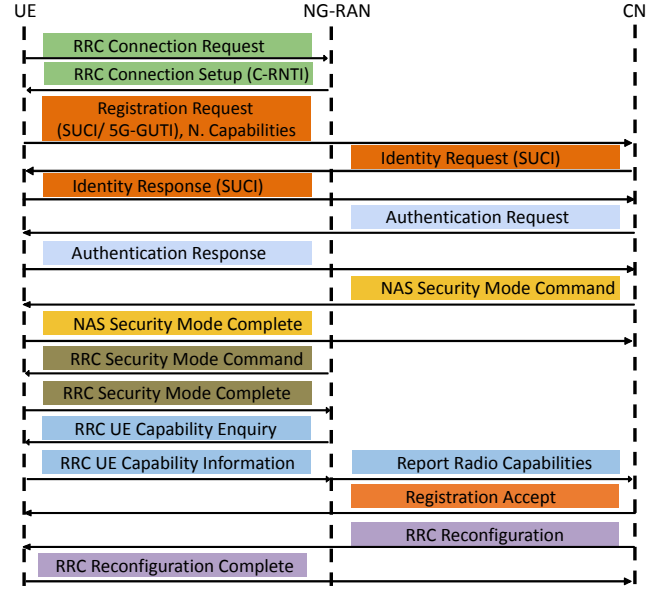


Figure 1: UE Registration & Authentication signal flow in 5G.

5G-GUTI in 5G. For consistency, this paper refers to TMSI for 3G and 4G and 5G-GUTI for 5G. Finally, RAN assigns the Cell Radio Network Temporary Identity (C-RNTI) to the UE.

### 2.3 UE Capabilities

UE capabilities are categorized into CN capabilities [38] and Radio Access capabilities [41]. The CN capabilities indicate general UE characteristics, such as the security algorithms supported by the UE for integrity and ciphering protection, and are transmitted as a NAS message. The Radio Access capabilities contain information regarding the radio capabilities of the UE, such as the supported frequency bands, and are transmitted as an RRC message. [42, 43] provide further information about UE capabilities.

### 2.4 UE Registration & Authentication Procedure

Fig. 1 illustrates the 5G message exchange flow for key procedures outlined in 3GPP specifications [23]. First, the UE establishes an RRC Connection with the NG-RAN and is assigned a C-RNTI. After, the UE initiates registration, sending its subscriber identity (SUCI or 5G-GUTI) and security capabilities. If the CN cannot resolve the 5G-GUTI, it requests the SUCI via an Identity Request/Response exchange. Then the Authentication and Key Agreement Protocol (AKA) is initiated by the CN. We mention that both EPS-AKA (Evolved Packet System Authentication and Key Agreement) and 5G-AKA (5G Authentication and Key Agreement) are supported, but since the differences are beyond the scope of this paper, we use 5G-AKA (Sec. 6.1.3.2 of [23]). After a successful mutual authentication, the NAS Security Command establishes a secure channel for NAS messages, ensuring integrity and ciphering protection.

The same procedure is followed for the RRC messages, exchanged between the UE and the gNB, to activate an RRC secure channel. Afterwards, the UE radio capabilities are transmitted to the 5G network, *once a secure channel is established* (see Figure 1). This is in contrast to prior cellular generations, where radio capabilities

were sent before the establishment of a secure channel between the UE and the RAN. Finally, User Plane (UP) security is activated through the RRC Reconfiguration message.

### 3 Methodology

This section outlines our methodology. First, Section 3.1 defines User Identity Confidentiality and its key properties. Then, Section 3.2 presents the types of adversaries that aim to violate these properties. Finally, Section 3.3 describes the Framework used for this systematization.

#### 3.1 User Identity Confidentiality

With the rise of sensitive data transmission, setting privacy objectives is crucial for ensuring user privacy. Since 3G and 4G, 3GPP (Sec. 5.1.1 [6, 7]) has emphasized protecting IMSI, user location, and service data. These requirements are still relevant in 5G [44], where Sec. 5.2.5 of [23] mandates SUPI and PEI protection, equivalent to IMSI and IMEI in previous generations (Sec. 2.2). Numerous studies [21, 33, 45–47] have addressed UE Identity Confidentiality, which we define as the privacy objective of this work. The following properties are necessary for its protection [6, 7]:

- **UE Identity Privacy:** "the permanent user identity (IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link".
- **UE Location Privacy:** "the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link".
- **UE Untraceability:** "an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link".

#### 3.2 Adversaries

We focus on three types of adversaries reported in literature and classified as passive, semi-passive and active, as also proposed in [42].

**1. Passive adversary:** It eavesdrops radio signals within a specific range, using channel sniffers. It can receive, decode, and store transmissions.

**2. Semi-Passive adversary:** It is a passive adversary that can also ping its target. For instance, it may send (silent) messages, or initiate (silent) calls [48] to its victim.

**3. Active adversary:** It can transmit radio signals, send or modify messages that were sent from or to the victim. It typically operates through a fake BS with strong signal strength and may also utilize sniffers, another UE, or jammer devices [49].

We mention that the equipment needed for such attacks is now easily deployable and affordable [50]. For example, a rogue BS can be built using a Universal Software Radio Peripheral (USRP) [51] with a modified code of open-source projects like OpenLTE [52], srsRAN [53, 54], gr-LTE [55, 56] and OAI [57, 58]. Furthermore, there are available open-source tools for channel sniffers [59–62], that are capable of decoding downlink traffic. Finally, jammers can be implemented using commodity equipment [63, 64].

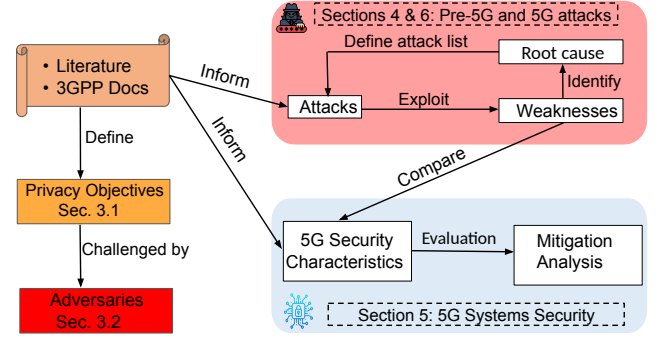


Figure 2: General Framework of our Systematization.

#### 3.3 Framework

**Description:** First, we explain the framework used for the systematization of the knowledge analyzed in this paper, as depicted in Figure 2. The first step is to select the privacy objectives that a network system must meet to protect stakeholders. Based on scientific literature and 3GPP documents, we set UE Identity Confidentiality (Sec. 3.1) as the privacy objective. Then, we assume that the adversaries described in Sec. 3.2 try to challenge the UE Identity Confidentiality, by performing relevant attacks. Thus, Sections 4 and 6 overview pre-5G and recent 5G attacks from existing literature, identifying their corresponding weaknesses and root cause, thus defining our attack list. Furthermore, Sec. 5 focuses on 5G Systems (5GS) comparing their security characteristics with past generations and evaluating whether identified weaknesses are mitigated—fully or partially. Since attacks exploited these weaknesses, their mitigation in 5G directly impacts attack feasibility.

**Example:** To facilitate the reader’s understanding of the perspective of this work, we give a concrete example of our framework with the IMSI Catching. This is a well-known attack (Sec. 4.1.1), performed by an active adversary, that violates all three properties of the UE Identity Confidentiality, thus breaking the system’s privacy objectives. The weakness behind this attack in 2G, 3G, and 4G is the *IMSI plaintext transmission*. As a fix to this problem, a new 5G Security characteristic has been introduced, which is the SUCI mechanism (Sec. 5.1), that encrypts IMSI. By evaluating the SUCI mechanism, we conclude that the previously mentioned weakness, that led to the IMSI Catching attack, is mitigated.

**Paper Collection Methodology:** Our literature search began with domain expertise papers, forming an initial list. Next, we expanded the list by searching papers that cited or were cited by these initial papers. Then, we searched various databases (e.g. Google Scholar, ACM Digital Library) using terms related to S&P attacks across cellular generations, adding relevant papers to our list. Afterwards, we analyzed the papers to determine whether the described attacks occur through the wireless medium and violate UE Identity Confidentiality and whether their underlying weaknesses originate from vulnerabilities in 3GPP specifications, rather than operator or vendor mis-implementations. For example, we excluded attacks that have a different target than the UE Identity Confidentiality, such as Denial of Service (DoS) [65–67] or battery drain [68], as well as attacks relying on implementation flaws (e.g., baseband processor vulnerabilities [69, 70] or network misconfigurations [71]). Furthermore, we excluded attacks that occur outside the wireless medium,

such as those executed by malicious applications running on the UE [72], or those involving inter-network communication, such as roaming-related threats [73]. Our paper focuses on intra-network attacks that violate UE Identity Confidentiality through the wireless medium, where the root cause lies in 3GPP standardization flaws. We refined our list accordingly to include only attacks that meet these criteria. Finally, for each selected attack, we conducted name-based searches for additional papers, finalizing a 150+ paper database. Since some attacks persist across cellular generations, our chronological search spanned from 2000 onward.

## 4 Pre-5G Cellular Generation Attacks

In this section, following the framework defined in Sec. 3.3, we analyze various pre-5G attacks reported in the scientific literature. First, the different attacks are categorized into privacy and security attacks, followed by the weaknesses that led to them, which are outlined (in italic font) and enumerated from W1 to W13. We summarize our findings in Table 1.

### 4.1 User Privacy attacks

**4.1.1 IMSI Catching.** IMSI Catching, which aims to steal the IMSI of the USIM, was one of the first practical attacks in 2G and has also been persistent in 3G and 4G [74–81]. An IMSI Catcher acts as a rogue BS, forcing the UE to connect by offering a stronger signal [82–94]. Alternatively, signal overshadowing can be used, where the adversary synchronizes with the legitimate BS and transmits a signal that is slightly stronger [95] or slightly weaker [96]. Once connected, the adversary sends an Identity Request, prompting the UE to transmit its IMSI in plaintext, leading to identity disclosure, traceability, and location tracking, thereby violating UE Identity Confidentiality. Furthermore, IMSI catchers can work in conjunction with a variety of different attacks, such as SIM card cloning [97], DoS [98, 99], UE localization [10], UE passive tracking (IMSI probing) [100] and stealing of the UE’s phone number [101]. Evidently, the plaintext IMSI transmission was characterized as a key vulnerability in the clause 6.1.3 of 3GPP Specifications [7]. Thus, IMSI catching exploits Weakness #1 (W1):

■ **W1:** *Plaintext IMSI transmission during UE authentication.*

**4.1.2 IMSI Paging.** Paging is initiated when the network searches for a UE to deliver a service. While the TMSI is typically used, the IMSI may be used if the TMSI cannot be resolved [102–104]. This plaintext IMSI transmission exposed the paging process to semi-passive adversaries across 2G [105–107], 3G [108, 109] and 4G [42, 110]. In this attack, an adversary with prior knowledge of the victim (e.g., phone number or social media account), exploits paging to track the victim’s location and extract the IMSI. By sending silent messages or calls, the attacker triggers paging and uses a sniffer to capture unencrypted downlink messages. Silent messages or calls keep the attack stealthy, as the UE remains unaware. This attack violates all User Identity Confidentiality properties, enabling IMSI disclosure, location tracking, and traceability. In conclusion, Weakness #2 (W2) is:

■ **W2:** *Paging procedure with plaintext IMSI transmission.*

**4.1.3 ToRPEDO.** Another problem of previous cellular generations is that the Paging Occasions (POs) of a UE are correlated to the

IMSI [111, 112]. A PO is a specific time interval during which a UE monitors the paging channel for incoming paging messages. More specifically, one of the parameters of the PO is the Paging Frame Index (PFI) of a UE that is estimated using the IMSI ( $PFI = IMSI \bmod 1024$ ) (Sec. 7 of [113]). The ToRPEDO semi-passive adversary [111] observes the unencrypted and fixed PFI of a UE, thereby managing to obtain synchronization between the UE and its corresponding paging delay. Finally, ToRPEDO obtains information about the victim’s IMSI from the fixed PFI managing to learn 7 bits of the victim’s IMSI, leading to partial user identity leakage along with location tracking and traceability. Concluding, the vulnerability that leads to this attack is Weakness #3 (W3):

■ **W3:** *Estimate of fixed POs based on IMSI.*

**4.1.4 IMEI Catching.** In 2G and 3G, cleartext IMEI transmission was allowed in response to an Identity Request Message, enabling active adversaries using fake base stations to steal the IMEI [9, 88]. LTE standard specification addressed this issue by restricting IMEI transmission until a secure channel is established [7, 82]. The analysis made in [114] confirmed this privacy enhancement, and as reported in [81, 115], only older 4G MEs remain vulnerable to the IMEI Catching attack, due to device misimplementations rather than protocol flaws. Consequently, IMEI Catching is considered resolved in LTE. In summary, Weakness #4 (W4) is:

■ **W4:** *Plaintext IMEI transmission.*

**4.1.5 TMSI Anonymity.** The primary purpose of TMSI is to minimize IMSI transmissions, enhancing UE anonymity. In theory, the network should periodically update TMSI to prevent UE tracking [116]. However, experiments in 2G, 3G and LTE revealed that TMSI remained constant for days across multiple countries [12, 42, 105, 108, 116–119]. More in detail, extensive tests made in 11 countries across 28 operators demonstrated that even when TMSI was refreshed, the new value was predictable [12]. A semi-passive adversary, using a sniffer and silent calls/messages, could link a victim’s phone number to its TMSI, enabling location tracking and traceability, thereby violating two properties of UE Confidentiality. Thus, the vulnerability behind this attack is Weakness #5 (W5):

■ **W5:** *Not frequent or misconfigured update policy of TMSI.*

Arapinis et al. [116] introduced as a proof of concept the TMSI reallocation replay attack. However, in their newest work [109], they claim that this attack is theoretical, as the likelihood of catching the reallocation message is low. Since neither [116] nor [109] provided an implementation, this attack is not considered further.

**4.1.6 C-RNTI tracking.** C-RNTI based attacks threaten UE confidentiality [120–125]. C-RNTI is local to the user’s serving BS and is used for the communication between the UE and the RAN. C-RNTIs can be found in both UL and DL control plane messages, and [120] showed that in LTE, the C-RNTI is transmitted unencrypted in every packet header, whether signaling or user traffic. A semi-passive adversary can link the C-RNTI to a victim’s phone number or social media account (e.g., WhatsApp). Available sniffers can decode DL messages containing the C-RNTI, compromising UE location privacy and untraceability [60–62]. Thus, Weakness #6 (W6) is:

■ **W6:** *The lack of ciphering in RRC messages.*

**4.1.7 AKA Protocol Linkability.** As mentioned in Sec. 2.4, AKA protocols provide mutual authentication between the UE and CN from 3G onwards. If authentication fails, the failure reason is either a MAC Failure or Sync Failure. An active adversary [108, 109, 126–129] first observes an AKA session of the target user and records the Authentication Request including the authentication challenge (RAND) and token (AUTN). Then, the adversary replays these values to check if the target UE is present in a specific area. Since failure messages are unencrypted, the attacker can distinguish the target UE based on its Sync Failure response, while all other UEs respond with MAC Failure. Thus, linking two AKA sessions compromises the UE location privacy. Moreover, [45] demonstrated that a linkability attack can also be executed through the sequence number (SQN) parameter, which is used to verify the freshness of authentication tokens. An adversary that knows the victim's IMSI repeatedly replays the same RAND and AUTN values. Observing changes in the SQN, the adversary infers the number of connections the victim has made, exploiting the weak protection provided by the Exclusive-OR (XOR) operation used to conceal the SQN. Concluding, Weaknesses #7 (W7) and #8 (W8) are:

■ **W7:** AKA session failure cause is exposed in plaintext.

■ **W8:** Weak confidentiality protection for SQN.

**4.1.8 Device Fingerprinting.** Device fingerprinting attack was proposed in LTE networks by Shaik et al. [43]. The adversary builds a database of different devices' CN and Radio capabilities. This attack has both passive and active variants. In the passive version, the adversary eavesdrops on the first NAS message, which, up to LTE, contained CN capabilities, such as supported security algorithms and telephony features. By comparing this data to its fingerprinting database, the attacker can identify the device model and infer the user's service. In addition, the active version transmits a UE Capabilities Enquiry message to the victim, exploiting Weakness 13 as described in the Sec. 4.2.3, and thus stealing the Radio Capabilities of the UE. This makes the fingerprinting more accurate, as the attacker now obtains both CN and Radio Capabilities. This attack compromises location and untraceability properties and may also impact identity privacy, as IMSI is transmitted in the first NAS message. The causes behind this attack are W13 and a new one, Weakness #9 (W9):

■ **W9:** Transmission of the whole set of Core Network capabilities in the initial NAS message.

**4.1.9 UE measurement reports tracking.** UE measurement reports, containing signal characteristics of nearby BSs, are sent to the BS as RRC messages to facilitate RAN maintenance [130]. An active attacker using a rogue BS with high signal quality can force a victim UE to connect and request its measurement reports, enabling location tracking [42, 131]. Furthermore, [82] proposes a passive version of this attack by simply decoding the plaintext RRC messages including the user's measurement reports and C-RNTI. LTE standards mandated that the UE measurement reports should be sent only after the activation of an RRC secure channel in Release 13 (LTE-Advanced) of TS. 36.331 [132], thereby mitigating the active version of this attack. However, the passive version of this attack can only be mitigated if RRC ciphering is activated, something that is operator-dependent since ciphering is optional [7]. Thus,

this attack is considered partially applicable in LTE as shown in Table 1. The vulnerabilities behind this issue are W6 and a new one, Weakness #10 (W10):

■ **W10 (up to LTE Release 13):** Transmission of UE measurements reports before the establishment of a secure channel.

## 4.2 User Security Attacks

**4.2.1 Data Manipulation Attacks.** Data manipulation attacks are performed by active adversaries that exploit the lack of integrity in user plane messages, thus managing to redirect the victim UE to a malicious server or impersonate him [121, 133]. Specifically, the ALTER attack [121] uses a rogue BS to establish a connection with the victim and redirect them to a malicious website, thus violating both location privacy and untraceability. The adversary intercepts and modifies the Uplink DNS request message, ensuring it reaches an adversarial DNS server instead of the intended one. The downlink DNS response is also modified to avoid detection by the victim. Furthermore, IMPersonation in 4G networks (IMP4GT) attack [133] extends ALTER, enabling impersonation of both the UE and the network. The cause of Data Manipulation attack is Weakness #11 (W11):

■ **W11:** Lack of integrity in user plane messages.

**4.2.2 TAU Reject Bidding-Down attack.** Bidding-Down attacks [35, 42, 43] aim to downgrade a UE to lower cellular generations with weaker privacy mechanisms (e.g., 2G lacks AKA protocol). The first identified bidding-down attack exploited the Tracking Area Update (TAU) procedure in LTE networks [42]. Specifically, the adversary uses a fake BS to respond to the NAS TAU Request message with a TAU Reject including a clause: "LTE services not allowed". Similar attacks have been demonstrated using different clauses within the TAU Reject message [35]. As a result, the UE begins searching for a network belonging to a lower generation. This problem arises from the fact that the TAU Reject message is not integrity protected. Although applying existing NAS security protections to TAU Reject messages has been discussed by the 3GPP security group [134], no such protection has been included in either LTE or 5G TSs. Concluding, Weakness #12 (W12) is:

■ **W12:** Lack of integrity in TAU Reject message.

**4.2.3 Radio Capabilities Bidding-Down attack.** [43] analyzes an attack based on the UE radio capabilities. An active adversary intercepts the Radio Capabilities Enquiry message, sent in 4G before secure channel establishment, and modifies the radio characteristics (e.g., supported frequencies) to downgrade the victim to a lower cellular generation. Location privacy is directly violated as the adversary establishes a connection with its victim. Further, identity privacy and untraceability properties may also be violated, since a successful bidding-down attack facilitates the entire set of attacks described in Sec. 4. Therefore, Weakness #13 (W13) is:

■ **W13:** Insecure transmission of UE Radio Capabilities.

## 5 5G Systems Security

In this section, we analyze the security protocols and mechanisms proposed for 5G in the relevant 3GPP document [23], aiming to minimize or eliminate the problems and security risks of Sec. 4. These improvements stand as MMs, as mentioned in our Framework

in Sec. 3.3 and are clearly enumerated at the end of each subsection. Further, we evaluate their efficacy in enhancing privacy by mapping them to the weaknesses ( $W1 - W13$ ) identified in Sec. 4. Finally, we assess whether these mechanisms are optional or mandatory in current 5G networks. The last two columns of Table 1 summarize our findings for 5G.

### 5.1 UE Identity Privacy based on SUCI

To avoid the plaintext transmission of SUPI, SUCI is introduced in 5G as an *encrypted* form of SUPI, based on elliptic cryptography. Specifically, the MSIN part of the SUPI is encrypted, while the MCC and MNC remain in plaintext to support network routing. SUCI is primarily used for authentication if the temporary identifier, 5G-GUTI, is not available. We highlight that the implementation of SUCI is of paramount importance for the UE's privacy, since it mitigates the attacks imposed by the IMSI plaintext transmission as described in Sec. 4.1.1. However, its implementation is still optional [23]. In summary, mitigation mechanism #1 (MM1) is:

■ **MM1:** *Concealment of SUPI using SUCI.*

### 5.2 Improvements on 5G-GUTI

**5.2.1 Strict 5G-GUTI update mechanism.** 5G-GUTI is the corresponding identifier to TMSI in previous cellular network generations. As analyzed in Sec. 4.1.5, previous generations faced serious privacy problems due to the infrequent or miss-configured refreshment of this temporary identifier [12]. To address this, 5G enforces stricter update rules (clause 6.12.3 of [23]), requiring a mandatory 5G-GUTI refreshment after paging, initial registration, TA updates, and other events in an *unpredictable* way to enhance user privacy [33]. Thus, Mitigation Mechanism #2 (MM2):

■ **MM2:** *Frequent and unpredictable 5G-GUTI update.*

**5.2.2 5G-S-TMSI-based paging and POs estimate.** Another key improvement in 5G over previous generations is the decoupling of the IMSI/SUPI from the paging procedures. In 5G, paging takes place with a shortened version of 5G-GUTI, called 5G-S-TMSI (5G S-Temporary Mobile Subscription Identifier) as mentioned in Sec. 2.10.1 of [40]. 5G-S-TMSI is derived from 5G-GUTI, so the strict update mechanism discussed in the previous subsection also applies to 5G-S-TMSI. Therefore, 5G-GUTI-based paging mitigates the IMSI paging attack as analyzed in Sec. 4.1.2. In summary, mitigation mechanism #3 (MM3) is:

■ **MM3:** *Decoupling of IMSI from paging.*

Furthermore, the Paging Frame Index (PFI) is now estimated based on 5G-S-TMSI, as mentioned in Sec. 7.1 of [135] instead of the IMSI. Based on this, the ToRPEDO attack (Sec. 4.1.3) is not applicable anymore. We highlight Mitigation Mechanism #4 (MM4):

■ **MM4:** *Decoupling of IMSI from POs' estimate.*

### 5.3 Integrity & Confidentiality Protection

Integrity and confidentiality in 5G networks has many similarities with the status of LTE. First, current 5G Systems are expected to implement the same 128-bit security algorithms with LTE systems: New Radio Encryption Algorithm (NEA) 0, 128-NEA1 and 128-NEA2 for confidentiality (ciphering) and New Radio Integrity Algorithm (NIA) 0, 128-NIA1 and 128-NIA2 for integrity protection,

as outlined in Secs. 5.2.2 and 5.2.3 of [23]. On the other hand, the potential use of 256-bit keys has been introduced as an optional feature in 5G [23, 136] to mitigate potential quantum attacks, such as the Quantum SUCI attack (Sec. 6.1.1). In summary, Mitigation Mechanism #5 (MM5) is:

■ **MM5:** *256-bit security algorithm support.*

Furthermore, in terms of specific messages protection, it is stated that RRC and NAS integrity are *mandatory*, whereas NAS and RRC ciphering are *optional*, something that is similar to LTE [137]. In fact, the attacks described in Secs. 4.1.6 and 4.1.9 can be mitigated by RRC ciphering, whereas the attack discussed in Sec. 6.1.2 can be mitigated by NAS Ciphering. Therefore, Mitigation Mechanisms #6 (MM6) and #7 (MM7) are:

■ **MM6 (similar in LTE):** *Ciphering of RRC messages.*

■ **MM7 (similar in LTE):** *Ciphering of NAS messages.*

Moreover, another 5G enhancement compared to LTE is the optional integrity protection of User Plane (UP) messages, as introduced in Sec. 5.3 of [23] that mitigates the Data Manipulation attacks (Sec. 4.2.1). So, Mitigation Mechanism #8 (MM8) is:

■ **MM8:** *Integrity protection of user plane messages.*

### 5.4 Privacy of the initial NAS message

Another key and *mandatory* 5G security mechanism is the privacy of the initial NAS message, as described in the section 6.4.6 of [23]. In contrast to previous generations, where the whole set of UE CN capabilities was transmitted in plaintext in the initial NAS message, 5G transmits only the security capabilities. The rest of the UE capabilities are transmitted after the activation of a secure NAS channel. This mitigates the Device fingerprinting attack, as described in Sec. 4.1.8. Thus, Mitigation Mechanism #9 (MM9) is:

■ **MM9:** *Enhanced privacy for the initial NAS message.*

### 5.5 Secured Radio Capabilities transmission

As analyzed in Sec. 4.2.3, the UE radio capabilities were transmitted before the establishment of the RRC security channel, enabling bidding-down attacks. This issue was addressed in early 5G releases and subsequently integrated into later LTE releases [138], where the transmission now occurs only after RRC security activation, as noted in Sec. 2.4 and illustrated in Fig. 1. Consequently, the bidding-down attacks based on UE Radio capabilities are eliminated by the *mandatory* Mitigation Mechanism #10 (MM10):

■ **MM10:** *Radio Capabilities transmission in a secure RRC channel.*

### 5.6 Fake Base Station Detection Framework

Fake Base Stations (FBS) were responsible for various attacks in previous cellular generations, as described in Sec. 4. 3GPP specifications, for the first time, included an optional FBS detection framework in Annex E of [23]. This framework aims to mitigate attacks caused by FBS, using measurements such as cell locations, frequencies and cell IDs. Although adversaries are capable of finding the real cell IDs and locations through mobile applications [91], frequency information can contribute to the detection of traditional active attacks, such as IMSI Catching (Sec. 4.1.1). Furthermore, a whole 3GPP document, TR. 33.809 [139] is responsible for enhancing the FBS detection framework in future 3GPP releases. For

instance, recent 3GPP studies (Secs. 6.4, 6.22 and 6.24 of [139]) proposed an enrichment of UE Measurements reports with channel elements, obtained from the Channel State Information Reference Signal (CSI-RS), which are capable of detecting and localizing FBS. In summary, Mitigation Mechanism #11 (MM11) is:

■ **MM11:** *Introduction of FBS detection framework.*

We highlight that current 5G networks operate either in 5G Stand Alone (SA) or 5G Non Stand Alone (NSA). More specifically, 5G NSA relies on the LTE CN, meaning only 5G enhancements related to the RAN can be implemented [140, 141]. For further information about recent measurements studies, we refer to Section 7.

## 6 5G Cellular Generation Attacks

In this section, we discuss various attacks against 5G networks based on recent literature. Similarly to Sec. 4, we first categorize the attacks into privacy and security. We then examine the types of adversaries capable of performing these attacks. Finally, we outline the protocol vulnerabilities that enabled these attacks. The last eight rows of Table 1 indicate our findings.

### 6.1 Privacy Attacks

**6.1.1 Quantum SUCI attack.** As discussed in Sec. 5.1, SUCI relies on elliptic cryptography, which has been shown to be vulnerable to quantum attacks, potentially exposing the SUPI [142]. This concern has been raised by several studies [143–146], suggesting that future mobile generations should account for quantum threats. 3GPP has already made some steps, since an optional support of 256-bit key generation algorithms [23] has been considered as a countermeasure to quantum attacks as analyzed in MM6 (Sec. 5.3). As shown in [146] a 256-bit encryption algorithm does not mitigate completely potential quantum attacks, but makes their implementation more difficult. Therefore, Weakness #14 (W14) is:

■ **W14:** *Vulnerability of SUCI elliptic cryptography to quantum attacks.*

Other SUCI-related attacks are considered low risk. SUCI probing or replay attack [147] attempts to verify a victim’s presence at a specific location by capturing their SUCI. 3GPP characterized this attack as low risk and no normative measures are needed (Key Issue #2.2 of [148]), since the actual identity of the user cannot be revealed by the SUCI. Furthermore, SUPI guessing attacks [149, 150], in which SUCIs are generated from guessed SUPIs and sent to potential victims, were also deemed impractical (Key Issue #3.2 in [148]). Finally, a passive adversary can observe the MCC and MNC during SUCI transmission [151], since these fields remain in plaintext. However, as many users can share the same MCC and MNC, this information cannot be reliably linked to a specific individual. Based on the above, only the SUCI Quantum attack is included in Table 1.

**6.1.2 GUTI Reallocation Command Attack.** [33] introduced the NAS GUTI Reallocation Command attack in real 5G SA networks. As the name suggests, the CN transmits this Command when a new GUTI value is assigned after the procedures introduced in Sec. 5.2. As explained in [33], this command was transmitted without ciphering, and can potentially lead to location tracking and traceability by a semi-passive adversary. The cause behind this attack is the lack of NAS ciphering, which remains optional in 5G cellular networks

as indicated in the related 3GPP document [23] and explained in MM7 (Sec. 5.3). Thus, Weakness #15 (W15) is:

■ **W15:** *Lack of ciphering in the NAS GUTI Reallocation Command.*

**6.1.3 CSI reports tracking attack.** Channel State Information (CSI) reports poses another potential danger to user privacy in 5G as shown in [152]. First, the BS transmits the CSI-RS in the downlink. Then, the UE sends the CSI reports in the Uplink to the BS as described in the Sec. 5.2 of [153]. The CSI reports include plaintext information, such as the power of the strongest beam of the CSI-RS, which is crucial for the UE positioning. The adversary [152] first builds a fingerprint database including the power of the strongest beam for the physical area of a BS. After, they learn the victim’s C-RNTI with the procedures described before (e.g., silent messages) and passively decode the CSI reports including the victim’s C-RNTI and strongest beam. Finally, the adversary compares the decoded beam value with the ones existing in the database, thereby estimating the position of the victim and violating the location privacy. In summary, Weakness # 16 (W16) is:

■ **W16:** *Lack of encryption of CSI reports.*

As stated in [152] CSI reports are an RRC message and can use the existing RRC security context after its activation. However, the 3GPP document [153] that defines the structure of the CSI reports message does not include encryption. Investigating further, we found a draft of the 3GPP meeting 3GPPSA3#101-e [154] that mentions the possible encryption of CSI reports, but no official 3GPP TS specifies this. Therefore, no formal 5G mitigation mechanism exists, and 3GPP should address this in future releases.

**6.1.4 ISAC-based tracking attack.** Integrated Sensing and Communication (ISAC) is a new 3GPP Rel. 19 study item [155]. ISAC support facilitates emerging 5G and beyond applications, such as health monitoring, smart-homes or environment mapping [156–160]. ISAC applications focus on the analysis of wireless signals’ reflections (e.g., channel variation in amplitude and phase, signal attenuation, Doppler shift, angle of arrival (AoA)) to infer sensing results. However, a lot of privacy concerns have been raised about ISAC systems in recent literature [161–167]. An active adversary can spoof the legitimate signals to control the sensing applications [168], whereas a passive adversary only needs to eavesdrop the wireless channel and sniff the sensing information. As a result, a stealthy passive attacker can estimate the victim’s location through existing localization algorithms [159, 169–171] and potentially learn about the services delivered to the victim (e.g., respiration rate application [172]). As stated in Sec. 7.1.4 of [155], 3GPP community has discussed this problem and confidentiality of sensing data is proposed. However, the 5G Security TS [23] does not refer to the security of sensing data. As standardization efforts for ISAC technologies are at an early stage and the adversarial attacks are mainly theoretical, the related security issues are considered as *Potential Weaknesses (PW)* in 5G-Advanced, if not addressed by future 3GPP security specifications. Thus, Potential Weakness #1 (PW1) is:

■ **PW1:** *Lack of sensing data confidentiality.*

**6.1.5 Satellite and NTN tracking attacks.** Satellites and Non Terrestrial Networks (NTNs) are an emerging technology currently under standardization in the 3GPP ecosystem for 5G and beyond cellular networks [173–180]. Initially, 3GPP performed relevant analysis as

a study item for Rel. 15 and 16 [181–183] and later introduced the relevant work item starting from Rel. 17 [184, 185]. Satellite constellations are typically classified based on their orbital type: Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geostationary Earth Orbit (GEO). These constellations enable communication both with terrestrial network components and with satellite-enabled UEs.

However, this promising integration comes with a variety of security and privacy concerns, such as eavesdropping and spoofing [186–195]. In fact, satellite communications are usually not security protected, neither in terms of encryption nor in terms of integrity [196–199], since the implementation of satellite cryptographic algorithms is quite complex and can reduce rapidly the networks' overall performance [200, 201]. This problem is leveraged by the RECORD attack, which uses a passive sniffer to correlate the unencrypted signals and messages transmitted by LEO satellites, with the target's TMSI [202], thereby enabling location tracking. In addition, SatOver is a signal overshadowing attack, performed by an active adversary that obtains a connection with a LEO or GEO satellite UE, thereby violating the complete set of UE Identity Confidentiality properties [203].

Furthermore, *Non Terrestrial Networks expand the attack surface*. More in detail, in current 3GPP standards, NTN integration requires the existence of GNSS for network synchronization and proper operations [180]. This means that the operation of the network is sensitive to standard attacks to GNSS signals, such as spoofing [204–207]. The effort of GNSS-free specification is currently in its very early stage in Rel. 19 [208]. Similar to Sec. 6.1.4, the aforementioned security issues are considered as Potential Weaknesses (PW). Thus, Potential Weaknesses #2 (PW2) and #3 (PW3) are:

■ **PW2:** *Lack of security algorithms for NTNs.*

■ **PW3:** *Mandatory activation of the vulnerable GNSS support.*

There is a variety of research proposals to improve the security and privacy offered by satellite and NTN networks. A first set of solutions proposes the application of AI algorithms that aim to detect the existence of an adversary [209–214]. Other solutions propose improvements of PHY layer security [215, 216], such as adding artificial noise to the channel [217, 218], and improved cryptographic schemes, such as the adoption of quantum algorithms [219, 220].

## 6.2 Security Attacks

**6.2.1 PRS spoofing attack.** PRS (Positioning Reference Signal) spoofing attacks violate the UE location privacy and hijack the victim's positioning data [34, 221, 222]. An active adversary transmits a high-power PRS, interfering with the legitimate PRS signal. As a result, the victim UE considers the hijacked PRS as the legitimate signal, since there is no integrity mechanism in the PHY layer to show the PRS modification. Then, this hijacked PRS is used for UE localization. So, the adversary not only violates the UE location privacy, but also controls the victim's position. Thus, the weakness #17 (W17) is:

■ **W17:** *Lack of integrity protection for PRS.*

Even after the activation of the security context, physical signals cannot be easily protected due to high computational overhead and extensive protocol changes. A viable solution is a robust FBS detection framework. [34] proposes an Artificial Intelligence (AI)-based FBS detection framework to detect this attack.

**6.2.2 Ambient-IoT device related attacks.** Technically moving beyond typical UEs, the latest Release 19 [223, 224] of 5G-Advanced has introduced the implementation of ambient-IoT devices (AIoT). AIoT devices are battery-free devices that essentially operate using environmental energy through backscatter method [225–227].

The consumption of AIoT devices starts from a power budget of about  $1 \mu\text{W}$  for the category of Device 1 [228]. Due to their ultra-low available energy, implementing security algorithms in AIoT devices is challenging, thereby raising security concerns, such as spoofing [229, 230]. Furthermore, recent 3GPP documents recognize multiple security vulnerabilities in AIoT, particularly regarding users' identifiers privacy, communication information protection and authentication [231]. Moreover, the section 5.2.6 of [223], which analyzes security and privacy aspects of AIoT devices, is in a preliminary stage, and it is unclear how 3GPP intends to proceed. We mention that the research community has shown that hardware characteristics, such as radio frequency offsets [232], is inaccurate due to channel instability. Security mechanisms based on Radio-Frequency fingerprinting have been proposed leveraging this instability [233]. In summary, *AIoT devices expand the attack surface due to their limited security capabilities, thus, being vulnerable to multiple pre-5G attacks, as described in Sec. 4*. As standardization efforts are in progress, Potential Weakness (PW) #4 (PW4) is:

■ **PW4:** *Lack of security mechanisms for AIoT devices.*

**6.2.3 5G Bidding Down attack.** A 5G bidding down attack was introduced, as a proof of concept in [15]. An active adversary using a FBS eavesdrops the RRC Security Mode Command sent by the legitimate gNB to the UE and then answers on behalf of the victim UE with a RRC Security Mode Failure. As stated in the Sec. 5.3.4.3 of [37], after an RRC Security Mode Failure message reception, the security algorithms used prior to the reception of the RRC Security Mode Command message continue to be used. As a result, no security protection is applied and the UE works in limited mode with "NULL" ciphering and integrity algorithms (NEA0 and NIA0). Finally after deactivating the victim's UE security protection, the adversary may send an identity request message to the victim and steal its SUPI-IMSI, thus breaking the identity privacy as well. Concluding, the Weakness #18 (W18) is:

■ **W18:** *Lack of integrity protection in RRC security mode failure message.*

Considering that this attack occurs before the activation of an RRC secure channel, integrity protection cannot be applied to the affected message. Furthermore, [23] does not provide a clear specification for the use of the Anti-Bidding Down Between Architectures (ABBA) parameter in Release up to 19, leading to variations in how it is implemented across real-world deployments [35, 234]. In addition, ABBA is transmitted within the NAS SMC message and is not designed to protect RRC messages, which are exploited by the attack discussed here. This attack, along with the one described in Section 6.2.1, underscores the need for a robust and mandatory FBS detection framework. For example, a recent study [235] proposes a RAN-based FBS detection system that mitigates bidding-down attacks using deep learning techniques. Currently, there is no concrete defense mechanism for these attacks in the 3GPP standards.

| Attack Name                                      | Privacy Implications |                   |              | Adversary Type |              |         | Pre 5G Generation |    |    |                                      | 5G Security Characteristics        |                       |   |
|--------------------------------------------------|----------------------|-------------------|--------------|----------------|--------------|---------|-------------------|----|----|--------------------------------------|------------------------------------|-----------------------|---|
|                                                  | Identity Disclosure  | Location Tracking | Traceability | Active         | Semi-Passive | Passive | 2G                | 3G | 4G | Weakness Exploited                   | Mitigation Mechanisms              | Optional or Mandatory |   |
| IMSI Catching [74–94]                            | ●                    | ●                 | ●            | ●              | ○            | ○       | ●                 | ●  | ●  | W1 (Sec. 4.1.1)                      | MM1 (Sec. 5.1)<br>MM11 (Sec. 5.6)  | O                     | O |
| IMSI Paging [105–110]                            | ●                    | ●                 | ●            | ○              | ●            | ○       | ●                 | ●  | ●  | W2 (Sec. 4.1.2)                      | MM3 (Sec. 5.2.2)                   | M                     |   |
| ToRPEDO [111]                                    | ●                    | ●                 | ●            | ○              | ●            | ○       | ●                 | ●  | ●  | W3 (Sec. 4.1.3)                      | MM4 (Sec. 5.2.2)                   | M                     |   |
| IMEI Catching [9, 82, 98, 115]                   | ●                    | ●                 | ●            | ●              | ○            | ○       | ●                 | ●  | ○  | W4 (Sec. 4.1.4)                      | Solved since LTE                   | M                     |   |
| TMSI Anonymity [12, 105, 116–119]                | ○                    | ●                 | ●            | ○              | ●            | ○       | ●                 | ●  | ●  | W5 (Sec. 4.1.5)                      | MM2 (Sec. 5.2.1)                   | M                     |   |
| C-RNTI tracking [120–125]                        | ○                    | ●                 | ●            | ○              | ●            | ○       | ●                 | ●  | ●  | W6 (Sec. 4.1.6)                      | MM6 (Sec. 5.3)                     | O                     |   |
| AKA Protocol Linkability [108, 109, 126–129]     | ○                    | ●                 | ●            | ○              | ○            | ○       | ○                 | ●  | ●  | W7 (Sec. 4.1.7)<br>W8 (Sec. 4.1.7)   | No MM                              | -                     |   |
| Device Fingerprinting [43]                       | ●                    | ●                 | ●            | ●              | ○            | ●       | ●                 | ●  | ●  | W13 (Sec. 4.2.3)<br>W9 (Sec. 4.1.8)  | MM10 (Sec. 5.5)<br>MM9 (Sec. 5.4)  | M                     | M |
| UE Measurements reports [42, 82, 130, 131]       | ○                    | ●                 | ○            | ●              | ●            | ○       | ●                 | ●  | ●  | W6 (Sec. 4.1.6)<br>W10 (Sec. 4.1.9)  | MM6 (Sec. 5.3)<br>Solved since LTE | O                     | M |
| Data Manipulation [121, 133]                     | ○                    | ●                 | ●            | ●              | ○            | ○       | ●                 | ●  | ●  | W11 (Sec. 4.2.1)                     | MM8 (Sec. 5.3)                     | O                     |   |
| TAU Reject bidding down [35, 42]                 | ●                    | ●                 | ●            | ●              | ○            | ○       | ○                 | ●  | ●  | W12 (Sec. 4.2.2)                     | No MM                              | -                     |   |
| R. Capabilities bidding down attack [35, 42, 43] | ●                    | ●                 | ●            | ●              | ○            | ○       | ○                 | ●  | ●  | W13 (Sec. 4.2.3)                     | MM10 (Sec. 5.5)                    | M                     |   |
| Quantum SUCI [142]                               | ●                    | ●                 | ●            | ●              | ○            | ○       |                   |    |    | W14 (Sec. 6.1.1)                     | MM5 (Sec. 5.3)                     | O                     |   |
| GUTI Reallocation Command [33]                   | ○                    | ●                 | ○            | ○              | ●            | ○       |                   |    |    | W15 (Sec. 6.1.2)                     | MM7 (Sec. 5.3)                     | O                     |   |
| CSI Reports tracking [152]                       | ○                    | ●                 | ○            | ○              | ●            | ○       |                   |    |    | W16 (Sec. 6.1.3)                     | No MM                              | -                     |   |
| ISAC based tracking [161–165, 167, 168]          | ○                    | ●                 | ●            | ●              | ○            | ●       |                   |    |    | PW1 (Sec. 6.1.4)                     | -                                  | -                     |   |
| Satellite and NTN tracking [196–199, 202, 203]   | ○                    | ●                 | ●            | ●              | ○            | ●       |                   |    |    | PW2 (Sec. 6.1.5)<br>PW3 (Sec. 6.1.5) | -                                  | -                     |   |
| PRS spoofing attack [34, 221, 222]               | ○                    | ●                 | ○            | ●              | ○            | ○       |                   |    |    | W17 (Sec. 6.2.1)                     | MM11 (Sec. 5.6)                    | O                     |   |
| AIoT related attacks [229, 230, 233]             | ○                    | ●                 | ●            | ●              | ○            | ○       |                   |    |    | PW4 (Sec. 6.2.2)                     | -                                  | -                     |   |
| 5G bidding down attack [15]                      | ●                    | ●                 | ●            | ●              | ○            | ○       |                   |    |    | W18 (Sec. 6.2.3)                     | MM11 (Sec. 5.6)                    | O                     |   |

●: Applicable, ●: Partially Applicable, ○: Not Applicable.

**Table 1: Top part: Overview of pre-5G (2G-4G) attacks against UE Confidentiality, corresponding weakness (W#) exploited, and any mitigation method (MM#) proposed. Bottom part: Overview of new 5G attacks, corresponding weakness exploited and any mitigation method proposed.**

## 7 Discussion

In this paragraph, we comment on the results presented in Sections 4, 5 and 6, evaluating the progress of 5G security compared to its predecessors and highlighting key takeaways.

5G standard paid particular attention to 5G-GUTI mechanism and paging procedures. Consequently, IMSI has been replaced by 5G-GUTI for paging and POs’ estimate as explained in Sec. 5.2.2. These *mandatory* modifications along with the *mandatory* 5G-GUTI reallocation mechanism, mitigated several pre-5G attacks (Secs. 4.1.2, 4.1.3, 4.1.5).

**Takeaway 1:** 5G ensures a secure paging procedure through the mandatory 5G-GUTI mechanism.

5G enhances the privacy of UE CN and Radio Capabilities by securing the first NAS message (Sec. 5.4) and transmitting Radio Capabilities only after the establishment of a secure channel (Sec. 5.5). These measures mitigate the related attacks described in Secs. 4.1.8 and 4.2.3.

**Takeaway 2:** 5G strengthens the privacy of UE CN and Radio Capabilities.

Three attacks affect 5G SA networks due to the absence of MMs: two inherited attacks (AKA linkability and TAU Reject bidding-down) and one recent 5G attack (CSI reports localization), all posing threats to user privacy. 3GPP has acknowledged these issues, including AKA linkability in Sec. 6.2 of [236], the integrity of TAU reject messages [134], and the encryption of CSI reports [154]. However, none of these proposals have been incorporated into the 3GPP Security TS [23].

**Takeaway 3:** 5G is vulnerable to AKA linkability, TAU Reject bidding-down and CSI reports localization attacks. 3GPP should prioritize mitigating these threats in future releases.

An important observation is that 5G security often depends on operators' implementations. Specifically, pre-5G attacks, such as IMSI Catching, C-RNTI tracking, UE Measurement Reports, and Data Manipulation are mitigated by optional MMs. Similarly, recent 5G attacks such as Quantum SUCI, GUTI Reallocation Command, PRS spoofing, and 5G bidding-down are also mitigated solely by optional MMs. Except for the SUCI Quantum attack, which is mainly theoretical, all these attacks have been proven effective in both pre-5G and 5G networks.

**Takeaway 4:** Many 5G MMs are optional, leaving the mitigation of several attacks up to operators' discretion.

Most of these optional mechanisms are related to the ciphering of RRC and NAS messages and the integrity of UP messages. As shown in [237], UP integrity increases the network's computational overhead and latency, with parallel programming and CN architecture improvements suggested as solutions. Regarding RRC ciphering, aside from mandating it, an alternative solution has been proposed: more frequent reallocation of C-RNTI, using a pool of multiple C-RNTIs, which can be 3GPP-compliant with minimal modifications [11, 238, 239].

**Takeaway 5:** 3GPP should prioritize addressing issues related to the ciphering and integrity of messages. A detailed analysis of the overhead from their mandatory activation is needed, and if prohibitive, alternative solutions should be explored.

SUCI was introduced in 5G to mitigate the IMSI catching attack. However, its optional status poses risks to UE identity privacy.

**Takeaway 6:** 3GPP should prioritize mandating SUCI to protect identity privacy.

The FBS detection framework is the only 5G MM capable of mitigating stealthy attacks, such as those presented in Secs. 6.2.1 and 6.2.3. In addition, many research proposals focus on enhancing the FBS detection framework. Some solutions [240–242] propose the authentication of legitimate BSs by defining new authentication protocols, network entities or digital signature schemes, thus mitigating the impact of FBS but increasing both the computational overhead of the network and soliciting protocol modifications. Furthermore, numerous works focus on the application of AI for FBS detection [34, 235, 243–247] with promising results. In particular, the AI-based FBS frameworks proposed by [34, 235], can detect even new and sophisticated attacks, as analyzed in Secs. 6.2.1 and 6.2.3. The Open RAN (O-RAN) evolution can facilitate the implementation of these AI solutions in current 5G networks [248, 249].

**Takeaway 7:** 3GPP should define a strict and mandatory FBS detection framework in 6G, utilizing AI advancements.

Recent 3GPP Releases introduced ISAC, NTN and Ambient-IoT. As discussed in Secs. 6.1.4, 6.1.5 and 6.2.2 and illustrated in Table 1, these technologies face potential privacy and security risks *thereby, substantially expanding the attack surface*.

**Takeaway 8:** 3GPP should propose security and privacy frameworks for emerging technologies in future 6G releases.

Finally, we comment on the results of recent measurement studies on 5G SA and 5G NSA networks. Recent real-world 5G NSA measurement studies [29, 35, 250–254] indicate significant privacy risks for UEs, due to the reliance of 5G NSA on the LTE CN. In contrast, recent 5G SA measurement studies [30, 33] showed substantial improvements, since mandatory 5G MMs are in place. Furthermore, SUCI was shown to be activated among three different operator networks [33]. However, incompatibility issues between the 5G CN and USIM cards [31] along with USIM cards miss-functionalities [32] can potentially limit the SUCI implementation [30]. In addition, [30, 33] reveal that some operators do not activate RRC and NAS ciphering in 5G SA networks, thus being vulnerable to the corresponding attacks illustrated in Table 1.

**Takeaway 9:** Operators should transition from 5G NSA to 5G SA and ensure proper network implementations.

## 8 Conclusion

In this systematization of knowledge paper, we developed a methodology to analyze security and privacy attacks in cellular networks. Our study examined 12 pre-5G attacks and 11 5G MMs, finding that 1 attack was resolved in LTE, 5 were fully mitigated by mandatory 5G MMs, while 4 depend on optional MMs, leaving their implementation up to operators. The AKA Linkability and TAU Reject bidding-down attacks remain unresolved in 5G. We also analyzed 8 recent 5G attacks, of which CSI reports localization remains unaddressed by current 5G protocols, while 4 rely on optional MMs. Notably, 3 potential S&P issues stem from 5G emerging technologies, including ISAC, Satellite NTN and AIoT integration, highlighting the need for further 3GPP security studies. Finally, we outlined 9 key takeaways, summarizing lessons learned and proposing future work for operators and 3GPP.

## ACKNOWLEDGEMENTS

Stavros Eleftherakis' work is funded by MCIN/AEI/10.13039/501100011033/ and by the ESF+ under the predoctoral training grant PREP2022-000340. This work was funded at Imdea Networks by MICIU/AEI/10.13039/501100011033/ and by the ERDF, EU under project PID2022-136769NB-I00 (6th-SENSE\_ELSA). The work was also supported by The Ministry of Economic Affairs and Digital Transformation of Spain and the European Union-Next Generation EU programme for the Recovery, Transformation and Resilience Plan and the Recovery and Resilience Mechanism under agreements TSI-063000-2021-63 (MAP-6G), TSI-063000-2021-142 and TSI-063000-2021-147 (6G-RIEMANN); The European Union Horizon 2020 program under grant agreements 101021808 (SPATIAL), 101096435 (CONFIDENTIAL6G) and 101139067 (ELASTIC).

## References

- [1] P. Taylor, "Number of smartphone mobile network subscriptions worldwide from 2016 to 2022, with forecasts from 2023 to 2028." <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>, 2023. Accessed: 2025-05.
- [2] G. Cattaneo, G. De Maio, P. Faruolo, and U. F. Petrillo, "A review of security attacks on the GSM standard," in *Information and Communication Technology: International Conference, ICT-EurAsia 2013, Yogyakarta, Indonesia, March 25-29, 2013. Proceedings 1*, pp. 507–512, Springer, 2013.
- [3] D. Rupperecht, A. Dabrowski, T. Holz, E. Weippl, and C. Pöpper, "On security research towards future mobile network generations," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2518–2542, 2018.
- [4] K. Vachhani, "Security threats against LTE networks: A survey," in *Security in Computing and Communications: 6th International Symposium, SSCC 2018, Bangalore, India, September 19–22, 2018, Revised Selected Papers 6*, pp. 242–256, Springer, 2019.
- [5] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 283–302, 2013.
- [6] "3GPP TS 33.102, "3G Security; Security Architecture," version 17.0.0 Rel. 17." <https://www.3gpp.org/>. Accessed: 2025-05.
- [7] "3GPP TS 33.401, "3GPP System Architecture Evolution (SAE): Security architecture," version 17.4.0 Rel. 17." <https://www.3gpp.org/>. Accessed: 2025-05.
- [8] C. Paget, "Practical cellphone spying," *Def Con*, vol. 18, 2010.
- [9] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers," in *Proceedings of the 30th annual computer security applications Conference*, pp. 246–255, 2014.
- [10] M. Kotuliak, S. Erni, P. Leu, M. Röschlin, and S. Çapkun, "{LTrack}: Stealthy tracking of mobile phones in {LTE}," in *31st USENIX Security Symposium (USENIX Security 22)*, pp. 1291–1306, 2022.
- [11] N. Ludant, P. Robyns, and G. Noubir, "From 5G Sniffing to Harvesting Leakages of Privacy-Preserving Messengers," in *2023 IEEE Symposium on Security and Privacy (SP)*, pp. 3146–3161, IEEE, 2023.
- [12] B. Hong, S. Bae, and Y. Kim, "GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier," in *NDSS*, 2018.
- [13] E. Bitsikas, T. Schnitzler, C. Pöpper, and A. Ranganathan, "Freaky Leaky {SMS}: Extracting User Locations by Analyzing {SMS} Timings," in *32nd USENIX Security Symposium (USENIX Security 23)*, pp. 2151–2168, 2023.
- [14] I. Palamà, F. Gringoli, G. Bianchi, and N. Blefari-Melazzi, "IMSI Catchers in the wild: A real world 4G/5G assessment," *Computer Networks*, vol. 194, p. 108137, 2021.
- [15] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "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*, pp. 669–684, 2019.
- [16] F. Liu, J. Peng, and M. Zuo, "Toward a secure access to 5G network," in *2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)*, pp. 1121–1128, IEEE, 2018.
- [17] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, "User privacy, identity and trust in 5G," *A Comprehensive Guide to 5G Security*, pp. 267–279, 2018.
- [18] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.
- [19] R. P. Jover, "The current state of affairs in 5G security and the main remaining security challenges," *arXiv preprint arXiv:1904.08394*, 2019.
- [20] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.
- [21] H. Khan and K. M. Martin, "A survey of subscription privacy on the 5G radio interface-the past, present and future," *Journal of Information Security and Applications*, vol. 53, p. 102537, 2020.
- [22] C. Yu, S. Chen, F. Wang, and Z. Wei, "Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers," *Computer Networks*, vol. 201, p. 108532, 2021.
- [23] "3GPP TS 33.501, "Security architecture and procedures for 5G system," version 18.2.0 Rel. 18." <https://www.3gpp.org/>. Accessed: 2025-05.
- [24] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018.
- [25] J. Tanveer, A. Haider, R. Ali, and A. Kim, "Machine learning for physical layer in 5G and beyond wireless networks: A survey," *Electronics*, vol. 11, no. 1, p. 121, 2021.
- [26] M. Harvanek, J. Bolcek, J. Kufa, L. Polak, M. Simka, and R. Marsalek, "Survey on 5G Physical Layer Security Threats and Countermeasures," *Sensors*, vol. 24, no. 17, p. 5523, 2024.
- [27] D. Segura, J. Munilla, E. J. Khatib, and R. Barco, "5G early data transmission (Rel-16): Security review and open issues," *IEEE Access*, vol. 10, pp. 93289–93308, 2022.
- [28] G. Choudhary and V. Sharma, "A Survey on the Security and the Evolution of Osmotic and Catalytic Computing for 5G Networks," *5G enabled secure wireless networks*, pp. 69–102, 2019.
- [29] O. Lasierra, G. Garcia-Aviles, E. Municio, A. Skarmeta, and X. Costa-Pérez, "European 5G Security in the Wild: Reality versus Expectations," *arXiv preprint arXiv:2305.08635*, 2023.
- [30] S. Nie, Y. Zhang, T. Wan, H. Duan, and S. Li, "Measuring the deployment of 5g security enhancement," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 169–174, 2022.
- [31] C. Yu, S. Chen, Z. Wei, and F. Wang, "SecChecker: Inspecting the Security Implementation of 5G Commercial Off-The-Shelf (COTS) Mobile Devices," *Computers & Security*, p. 103361, 2023.
- [32] E. Bitsikas, S. Khandker, A. Salous, A. Ranganathan, R. Piqueras Jover, and C. Pöpper, "UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 121–132, 2023.
- [33] S. Eleftherakis, T. Otim, G. Santaromita, A. D. Zayas, D. Giustiniano, and N. Kourtellis, "Demystifying privacy in 5g stand alone networks," in *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, pp. 1330–1345, 2024.
- [34] K. Gao, H. Wang, H. Lv, and P. Gao, "Your Locations May Be Lies: Selective-PRS-Spoofing Attacks and Defence on 5G NR Positioning Systems," in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*, pp. 1–10, IEEE, 2023.
- [35] B. Karakoc, N. Fürste, D. Rupperecht, and K. Kohls, "Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G," 2023.
- [36] W. Chen, X. Lin, J. Lee, A. Toskala, S. Sun, C. F. Chiasserini, and L. Liu, "5G-advanced toward 6G: Past, present, and future," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 6, pp. 1592–1619, 2023.
- [37] "3GPP TS 38.331, "NR; Radio Resource Control (RRC) protocol specification," version 17.6.0 Rel. 17." <https://www.3gpp.org/>. Accessed: 2025-05.
- [38] "3GPP TS 24.501, "Non-Access-Stratum (NAS) protocol for 5G System (5GS)," version 18.4.0 Rel. 18." <https://www.3gpp.org/>. Accessed: 2025-05.
- [39] "3GPP TS 23.501, "System architecture for the 5G System (5GS)," version 18.3.0 Rel. 18." <https://www.3gpp.org/>. Accessed: 2025-05.
- [40] "3GPP TS 23.003, "Numbering, addressing and identification," version 18.2.0 Rel. 18." <https://www.3gpp.org/>. Accessed: 2025-05.
- [41] "3GPP TS 38.306, "NR; User Equipment (UE) radio access capabilities," version 18.0.0 Rel. 18." <https://www.3gpp.org/>. Accessed: 2025-05.
- [42] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," *arXiv preprint arXiv:1510.07563*, 2015.
- [43] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert, "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*, pp. 221–231, 2019.
- [44] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pp. 1383–1396, 2018.
- [45] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New privacy threat on 3G, 4G, and upcoming 5G AKA protocols," *Cryptology ePrint Archive*, 2018.
- [46] S. Shen, H. Wang, and Y. Zhao, "Identity-based authenticated encryption with identity confidentiality," *Theoretical Computer Science*, vol. 901, pp. 1–18, 2022.
- [47] H. Khan and K. M. Martin, "On the Efficacy of New Privacy Attacks against 5G AKA," in *ICETE (2)*, pp. 431–438, 2019.
- [48] G.-H. Tu, C.-Y. Li, C. Peng, and S. Lu, "How voice call technology poses security threats in 4G LTE networks," in *2015 IEEE conference on communications and network security (CNS)*, pp. 442–450, IEEE, 2015.
- [49] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, "5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation," in *2018 IEEE international conference on communications workshops (ICC Workshops)*, pp. 1–6, IEEE, 2018.
- [50] E. Bitsikas and C. Pöpper, "You have been warned: Abusing 5G's Warning and Emergency Systems," in *Proceedings of the 38th Annual Computer Security Applications Conference*, pp. 561–575, 2022.
- [51] "Ettus. USRP." <https://www.ettus.com/products/>. Accessed 2025-05.
- [52] "OpenLTE: An open source 3GPP LTE implementation." <https://sourceforge.net/projects/openlte/>. Accessed 2025-06.
- [53] "srsRAN: an open source 4G software radio suite developed by SRS." [https://github.com/srsran/srsRAN\\_4G/](https://github.com/srsran/srsRAN_4G/). Accessed 2025-05.
- [54] I. Gomez-Migueluez, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, "srsLTE: An open-source platform for LTE evolution and experimentation," in *Proceedings of the Tenth ACM International Workshop on Wireless Network*

- Testbeds, Experimental Evaluation, and Characterization*, pp. 25–32, 2016.
- [55] “gr-LTE: GNU Radio LTE receiver.” <https://github.com/kit-cel/gr-lte/>. Accessed 2025-05.
  - [56] J. Demel, S. Koslowski, and F. K. Jondral, “A LTE receiver framework using GNU Radio,” *Journal of Signal Processing Systems*, vol. 78, pp. 313–320, 2015.
  - [57] “OpenAirInterface Source Code for Next Generation Cellular Standard.” <https://gitlab.eurecom.fr/oai/>. Accessed 2025-05.
  - [58] N. Nikaein, M. K. Marina, S. Manickam, A. Dawson, R. Knopp, and C. Bonnet, “OpenAirInterface: A flexible platform for 5G research,” *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 33–38, 2014.
  - [59] T. D. Hoang, C. Park, M. Son, T. Oh, S. Bae, J. Ahn, B. Oh, and Y. Kim, “LTESniffer: An Open-source LTE Downlink/Uplink Eavesdropper,” 2023.
  - [60] S. Kumar, E. Hamed, D. Katabi, and L. Erran Li, “LTE radio analytics made easy and accessible,” *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 4, pp. 211–222, 2014.
  - [61] N. Bui and J. Widmer, “OWL: A reliable online watcher for LTE control channel measurements,” in *Proceedings of the 5th Workshop on All Things Cellular: Operations, Applications and Challenges*, pp. 25–30, 2016.
  - [62] R. Falkenberg and C. Wietfeld, “FALCON: An accurate real-time monitor for client-based mobile network data analytics,” in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, IEEE, 2019.
  - [63] Y. Brown, C. Teng, and A. Wyglinski, “Lte frequency hopping jammer,” *Worcester Polytechnic Institute, Worcester, Massachusetts*, 2019.
  - [64] H. Pirayesh and H. Zeng, “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,” *IEEE communications surveys & tutorials*, vol. 24, no. 2, pp. 767–809, 2022.
  - [65] H. Kim, J. Lee, E. Lee, and Y. Kim, “Touching the untouchables: Dynamic security analysis of the LTE control plane,” in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 1153–1168, IEEE, 2019.
  - [66] R. Ghannam, F. Sharevski, and A. Chung, “User-targeted denial-of-service attacks in lte mobile networks,” in *2018 14th International conference on wireless and mobile computing, networking and communications (WiMob)*, pp. 1–8, IEEE, 2018.
  - [67] D. Klischies, M. Schloegel, T. Scharnowski, M. Bogodukhov, D. Rupprecht, and V. Moonsamy, “Instructions unclear: undefined behaviour in cellular network specifications,” in *32nd USENIX Security Symposium (USENIX Security 23)*, pp. 3475–3492, 2023.
  - [68] S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, “LTEInspector: A systematic approach for adversarial testing of 4G LTE,” in *Network and Distributed Systems Security (NDSS) Symposium 2018*, 2018.
  - [69] E. Kim, D. Kim, C. Park, I. Yun, and Y. Kim, “BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols,” in *NDSS*, 2021.
  - [70] D. Maier, L. Seidel, and S. Park, “Basesafe: Baseband sanitized fuzzing through emulation,” in *Proceedings of the 13th ACM conference on security and privacy in wireless and mobile networks*, pp. 122–132, 2020.
  - [71] M. Chlosta, D. Rupprecht, and T. Holz, “On the challenges of automata reconstruction in lte networks,” in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 164–174, 2021.
  - [72] A. Continella, Y. Fratantonio, M. Lindorfer, A. Puccetti, A. Zand, C. Kruegel, G. Vigna, et al., “Obfuscation-Resilient Privacy Leak Detection for Mobile Apps Through Differential Analysis,” in *NDSS*, vol. 17, pp. 10–14722, 2017.
  - [73] S. Holtmanns, S. P. Rao, and I. Oliver, “User location tracking attacks for LTE networks using the interworking functionality,” in *2016 IFIP Networking conference (IFIP Networking) and workshops*, pp. 315–322, IEEE, 2016.
  - [74] U. Meyer and S. Wetzel, “A man-in-the-middle attack on UMTS,” in *Proceedings of the 3rd ACM workshop on Wireless security*, pp. 90–97, 2004.
  - [75] A. Lilly, “IMSI catchers: hacking mobile communications,” *Network Security*, vol. 2017, no. 2, pp. 5–7, 2017.
  - [76] S. Park, A. Shaik, R. Borgaonkar, and J.-P. Seifert, “Anatomy of commercial IMSI catchers and detectors,” in *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*, pp. 74–86, 2019.
  - [77] S. F. Mjolsnes and R. F. Olimid, “Private identification of subscribers in mobile networks: status and challenges,” *IEEE Communications Magazine*, vol. 57, no. 9, pp. 138–144, 2019.
  - [78] K. Norrman, M. Näsland, and E. Dubrova, “Protecting IMSI and user privacy in 5G networks,” in *Proceedings of the 9th EAI international conference on mobile multimedia communications*, pp. 159–166, 2016.
  - [79] M. Khan, P. Ginzboorg, K. Järvinen, and V. Niemi, “Defeating the downgrade attack on identity privacy in 5G,” in *Security Standardisation Research: 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings 4*, pp. 95–119, Springer, 2018.
  - [80] H. Choudhury, B. Roychoudhury, and D. K. Saikia, “Enhancing user identity privacy in LTE,” in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 949–957, IEEE, 2012.
  - [81] B. Michau and C. Devine, “How to not break LTE crypto,” in *ANSSI Symposium sur la sécurité des technologies de l’information et des communications (SSTIC)*, 2016.
  - [82] R. F. Olimid and S. F. Mjolsnes, “On LowCost Privacy Exposure Attacks in LTE Mobile Communication,” *Proceedings of the Romanian Academy Series AMathematics Physics Technical Sciences Information Science*, vol. 18, pp. 361–370, 2017.
  - [83] U. Meyer and S. Wetzel, “On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks,” in *2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE Cat. No. 04TH8754)*, vol. 4, pp. 2876–2883, IEEE, 2004.
  - [84] Z. Li, W. Wang, C. Wilson, J. Chen, C. Qian, T. Jung, L. Zhang, K. Liu, X. Li, and Y. Liu, “FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild,” in *NDSS*, 2017.
  - [85] S. Park, A. Shaik, R. Borgaonkar, A. Martin, and J.-P. Seifert, “[White-Stingray]: Evaluating {IMSI} catchers detection applications,” in *11th USENIX workshop on Offensive Technologies (WOOT 17)*, 2017.
  - [86] F. Van Den Broek, R. Verdult, and J. De Ruiter, “Defeating IMSI catchers,” in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 340–351, 2015.
  - [87] M. S. A. Khan and C. J. Mitchell, “Trashing IMSI catchers in mobile networks,” in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 207–218, 2017.
  - [88] A. Dabrowski, G. Petzl, and E. R. Weippl, “The messenger shoots back: Network operator based IMSI catcher detection,” in *Research in Attacks, Intrusions, and Defenses: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings 19*, pp. 279–302, Springer, 2016.
  - [89] S. Steig, A. Aarnes, T. Van Do, and H. T. Nguyen, “A network based imsi catcher detection,” in *2016 6th International Conference on IT Convergence and Security (ICITS)*, pp. 1–6, IEEE, 2016.
  - [90] L. Karacay, Z. Bilgin, A. B. Gündüz, P. Çomak, E. Tomur, E. U. Soykan, U. Gülen, and F. Karakoç, “A network-based positioning method to locate false base stations,” *IEEE Access*, vol. 9, pp. 111368–111382, 2021.
  - [91] H. Alrashdeh and R. A. Shaikh, “IMSI catcher detection method for cellular networks,” in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1–6, IEEE, 2019.
  - [92] T. Van Do, H. T. Nguyen, N. Momchil, and V. T. Do, “Detecting IMSI-catcher using soft computing,” in *Soft Computing in Data Science: First International Conference, SCDS 2015, Putrajaya, Malaysia, September 2-3, 2015, Proceedings 1*, pp. 129–140, Springer, 2015.
  - [93] V. T. Do, P. Engelstad, B. Feng, and T. van Do, “Strengthening mobile network security using machine learning,” in *Mobile Web and Intelligent Information Systems: 13th International Conference, MobiWIS 2016, Vienna, Austria, August 22-24, 2016, Proceedings 13*, pp. 173–183, Springer, 2016.
  - [94] P. Ney, I. Smith, G. Cadamuro, and T. Kohno, “SeaGlass: Enabling City-Wide IMSI-Catcher Detection,” *Proc. Priv. Enhancing Technol.*, vol. 2017, no. 3, p. 39, 2017.
  - [95] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, “Hiding in plain signal: Physical signal overshadowing attack on {LTE},” in *28th USENIX Security Symposium (USENIX Security 19)*, pp. 55–72, 2019.
  - [96] N. Ludant and G. Noubir, “SigUnder: a stealthy 5G low power attack and defenses,” in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 250–260, 2021.
  - [97] J. Liu, Y. Yu, F.-X. Standaert, Z. Guo, D. Gu, W. Sun, Y. Ge, and X. Xie, “Small tweaks do not help: Differential power analysis of milenage implementations in 3G/4G USIM cards,” in *Computer Security—ESORICS 2015: 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I 20*, pp. 468–480, Springer, 2015.
  - [98] S. F. Mjolsnes and R. F. Olimid, “Easy 4G/LTE IMSI catchers for non-programmers,” in *Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings 7*, pp. 235–246, Springer, 2017.
  - [99] S. Erni, M. Kotuliak, P. Leu, M. Roeschlin, and S. Capkun, “AdaptOver: adaptive overshadowing attacks in cellular networks,” in *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, pp. 743–755, 2022.
  - [100] D. Fraunholz, D. Brunke, S. Beidenhauser, S. Berger, H. Koenig, and D. Reti, “IMSI Probing: Possibilities and Limitations,” in *Nordic Conference on Secure IT Systems*, pp. 80–97, Springer, 2022.
  - [101] C. Yu, S. Chen, and Z. Cai, “Lte phone number catcher: A practical attack against mobile privacy,” *Security and Communication Networks*, vol. 2019, pp. 1–10, 2019.
  - [102] M. T. Raza, F. M. Anwar, and S. Lu, “Exposing LTE security weaknesses at protocol inter-layer, and inter-radio interactions,” in *Security and Privacy in Communication Networks: 13th International Conference, SecureComm 2017, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13*, pp. 312–338, Springer, 2018.
  - [103] P.-A. Fouque, C. Onete, and B. Richard, “Achieving better privacy for the 3GPP AKA protocol,” *Cryptology ePrint Archive*, 2016.
  - [104] E. C. Jiménez, P. K. Nakarmi, M. Näsland, and K. Norrman, “Subscription identifier privacy in 5G systems,” in *2017 international conference on selected topics in mobile and wireless networking (MoWNeT)*, pp. 1–8, IEEE, 2017.

- [105] D. F. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, "Location leaks on the GSM air interface," *ISOC NDSS (Feb 2012)*, 2012.
- [106] N. Golde, K. Redon, and J.-P. Seifert, "Let me answer that for you: Exploiting broadcast information in cellular networks," in *22nd USENIX Security Symposium (USENIX Security 13)*, pp. 33–48, 2013.
- [107] S. Kukliński, M. Czerwiński, J. Bieniasz, K. H. Kaminska, D. Paczesny, and K. Szczypiorski, "Evaluation of Privacy and Security of GSM Using Low-Cost Methods," in *2020 World Conference on Computing and Communication Technologies (WCCCT)*, pp. 96–105, IEEE, 2020.
- [108] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Bargaonkar, "New privacy issues in mobile telephony: fix and verification," in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 205–216, 2012.
- [109] M. Arapinis, L. I. Mancini, E. Ritter, and M. D. Ryan, "Analysis of privacy in mobile telephony systems," *International Journal of Information Security*, vol. 16, pp. 491–523, 2017.
- [110] I. Bojic, Y. Yoshimura, and C. Ratti, "Opportunities and challenges of trip generation data collection techniques using cellular networks," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 204–209, 2017.
- [111] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information," *Network and distributed systems security (NDSS) symposium 2019*, 2019.
- [112] A. Singla, S. R. Hussain, O. Chowdhury, E. Bertino, and N. Li, "Protecting the 4G and 5G cellular paging protocols against security and privacy attacks," *Proceedings on Privacy Enhancing Technologies*, 2020.
- [113] "3GPP TS 36.304, "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode," version 17.7.0 Rel. 14," <https://www.3gpp.org/>. Accessed: 2025-05.
- [114] S. F. Mjølsetnes and R. F. Olimid, "Experimental Assessment of Private Information Disclosure in LTE Mobile Networks," in *SECURITY*, pp. 507–512, 2017.
- [115] C. Park, S. Bae, B. Oh, J. Lee, E. Lee, I. Yun, and Y. Kim, "{DoLTest}: In-depth downlink negative testing framework for {LTE} devices," in *31st USENIX Security Symposium (USENIX Security 22)*, pp. 1325–1342, 2022.
- [116] M. Arapinis, L. I. Mancini, E. Ritter, and M. Ryan, "Privacy through Pseudonymity in Mobile Telephony Systems," in *NDSS*, 2014.
- [117] S. Saharan and J. Kumar, "Exploiting GSM Vulnerabilities: An Experimental Setup And Procedure To Map TMSI And Mobile Number," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.
- [118] C. Sorseth, S. X. Zhou, S. F. Mjølsetnes, and R. F. Olimid, "Experimental analysis of subscribers' privacy exposure by lte paging," *Wireless Personal Communications*, vol. 109, pp. 675–693, 2019.
- [119] N. Lakshmanan, N. Budhdev, M. S. Kang, M. C. Chan, and J. Han, "A stealthy location identification attack exploiting carrier aggregation in cellular networks," in *30th usenix security symposium (usenix security 21)*, pp. 3899–3916, 2021.
- [120] R. P. Jover, "LTE security, protocol exploits and location tracking experimentation with low-cost software radio," *arXiv preprint arXiv:1607.05171*, 2016.
- [121] D. Rupperecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking LTE on layer two," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 1121–1136, IEEE, 2019.
- [122] K. Kohls, D. Rupperecht, T. Holz, and C. Pöpper, "Lost traffic encryption: fingerprinting LTE/4G traffic on layer two," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 249–260, 2019.
- [123] T. Oh, S. Bae, J. Ahn, Y. Lee, D.-T. Hoang, M. S. Kang, N. O. Tippenhauer, and Y. Kim, "Enabling Physical Localization of Uncooperative Cellular Devices," *arXiv preprint arXiv:2403.14963*, 2024.
- [124] A. J. Ross and B. Reaves, "Towards Simultaneous Attacks on Multiple Cellular Networks," in *2023 IEEE Security and Privacy Workshops (SPW)*, pp. 394–405, IEEE, 2023.
- [125] D. Rupperecht, K. Kohls, T. Holz, and C. Pöpper, "Call me maybe: Eavesdropping encrypted {LTE} calls with {ReVoLTE}," in *29th USENIX security symposium (USENIX security 20)*, pp. 73–88, 2020.
- [126] M. S. A. Khan and C. J. Mitchell, "Another look at privacy threats in 3G mobile telephony," in *Australasian Conference on Information Security and Privacy*, pp. 386–396, Springer, 2014.
- [127] T. Fei and W. Wang, "The vulnerability and enhancement of AKA protocol for mobile authentication in LTE/5G networks," *Computer Networks*, vol. 228, p. 109685, 2023.
- [128] C. Hahn, H. Kwon, D. Kim, K. Kang, and J. Hur, "A privacy threat in 4th generation mobile telephony and its countermeasure," in *Wireless Algorithms, Systems, and Applications: 9th International Conference, WASA 2014, Harbin, China, June 23-25, 2014. Proceedings 9*, pp. 624–635, Springer, 2014.
- [129] I. Karim, S. R. Hussain, and E. Bertino, "Prochecker: An automated security and privacy analysis framework for 4g lte protocol implementations," in *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*, pp. 773–785, IEEE, 2021.
- [130] E. Bitsikas and C. Pöpper, "Don't hand it over: Vulnerabilities in the handover procedure of cellular telecommunications," in *Annual Computer Security Applications Conference*, pp. 900–915, 2021.
- [131] D. Forsberg, H. Leping, K. Tsuyoshi, and S. Alanara, "Enhancing security and privacy in 3GPP E-UTRAN radio interface," in *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–5, IEEE, 2007.
- [132] "3GPP TS 36.331, "Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification," version 18.1.0 Rel. 18," <https://www.3gpp.org/>. Accessed: 2025-05.
- [133] D. Rupperecht, K. Kohls, T. Holz, and C. Pöpper, "IMP4GT: IMPersonation Attacks in 4G NeTworks," in *NDSS*, 2020.
- [134] "3GPP TSG-SA3 Meeting 103-e, "UE procedures at TAU reject in idle mode mobility from 5GS to EPS over N26,"," <https://www.3gpp.org/dynareport?code=Meetings-S3.htm>, 2021. Accessed: 2025-05.
- [135] "3GPP TS 38.304, "NR; User Equipment (UE) procedures in Idle mode and RRC Inactive state," version 17.7.0 Rel. 17," <https://www.3gpp.org/>. Accessed: 2025-05.
- [136] "3GPP TR 33.841, "Study on the support of 256-bit algorithms for 5G," version 16.1.0 Rel. 16," <https://www.3gpp.org/>. Accessed: 2025-05.
- [137] M. Chlosta, D. Rupperecht, T. Holz, and C. Pöpper, "LTE security disabled: misconfiguration in commercial networks," in *Proceedings of the 12th conference on security and privacy in wireless and mobile networks*, pp. 261–266, 2019.
- [138] "3GPP TSG-SA WG3 Meeting 95Bis, "LS reply on Handling of UE radio network capabilities in 4G and 5G,"," <https://www.3gpp.org/dynareport?code=Meetings-S3.htm>, 2019. Accessed: 2025-05.
- [139] "3GPP TS 38.809, "Study on 5G security enhancements against False Base Stations (FBS)," version 18.1.0 Rel. 18," <https://www.3gpp.org/>. Accessed: 2025-05.
- [140] G. Holtrup, W. Lacube, D. P. David, A. Mermoud, G. Bovet, and V. Lenders, "5g system security analysis," *arXiv preprint arXiv:2108.08700*, 2021.
- [141] G. Holtrup, W. Blonay, M. Strohmeier, A. Mermoud, J.-P. Chavanne, and V. Lenders, "Modeling 5G Threat Scenarios for Critical Infrastructure Protection," in *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, pp. 161–180, IEEE, 2023.
- [142] V. Q. Ulitzsch, S. Park, S. Marzougui, and J.-P. Seifert, "A post-quantum secure subscription concealed identifier for 6g," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 157–168, 2022.
- [143] C. J. Mitchell, "The impact of quantum computing on real-world security: A 5G case study," *Computers & Security*, vol. 93, p. 101825, 2020.
- [144] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.
- [145] J. Yang and T. Johansson, "An overview of cryptographic primitives for possible use in 5G and beyond," *Science China Information Sciences*, vol. 63, no. 12, p. 220301, 2020.
- [146] T. C. Clancy, R. W. McGwier, and L. Chen, "Post-quantum cryptography and 5g security: tutorial," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 285–285, 2019.
- [147] M. Chlosta, D. Rupperecht, C. Pöpper, and T. Holz, "5G SUCI-Catchers: Still catching them all?," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 359–364, 2021.
- [148] "3GPP TS 33.846, "Study on authentication enhancements in the 5G System (5GS)," version 17.0.0 Rel. 17," <https://www.3gpp.org/>. Accessed: 2025-05.
- [149] H. Khan, B. Dowling, and K. M. Martin, "Identity confidentiality in 5G mobile telephony systems," in *International Conference on Research in Security Standardisation*, pp. 120–142, Springer, 2018.
- [150] F. Liu, L. Su, B. Yang, H. Du, M. Qi, and S. He, "Security Enhancements to Subscriber Privacy Protection Scheme in 5G Systems," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 451–456, IEEE, 2021.
- [151] R. Bargaonkar and A. Shaik, "5G IMSI Catchers Mirage." Blackhat, online presentation, <https://www.blackhat.com/us-21/briefings/schedule/#5g-imsi-catchers-mirage-23538>, 2021.
- [152] N. Ludant, M. Vomvas, and G. Noubir, "Unprotected 4G/5G Control Procedures at Low Layers Considered Dangerous," *arXiv preprint arXiv:2403.06717*, 2024.
- [153] "3GPP TS 38.214, "NR; Physical layer procedures for data," version 18.2.0 Rel. 18," <https://www.3gpp.org/>. Accessed: 2025-05.
- [154] "pCR to 33.809 – New solution for KI #7 and KI #5, based on modified CSI reports,"," <https://www.3gpp.org/dynareport?code=Meetings-S3.htm>. Accessed: 2025-05.
- [155] "3GPP TR 28.837, "Feasibility Study on Integrated Sensing and Communication " version 19.3.0 Rel. 19," <https://www.3gpp.org/>. Accessed: 2025-05.
- [156] F. Adib and D. Katabi, "See through walls with WiFi!," in *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, pp. 75–86, 2013.
- [157] U. Ha, S. Madani, and F. Adib, "WiStress: Contactless stress monitoring using wireless signals," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 5, no. 3, pp. 1–37, 2021.
- [158] Y. Gu, Y. Zhang, J. Li, Y. Ji, X. An, and F. Ren, "Sleepy: Wireless channel data driven sleep monitoring via commodity WiFi devices," *IEEE Transactions on Big Data*, vol. 6, no. 2, pp. 258–268, 2018.

- [159] D. Vasisht, A. Jain, C.-Y. Hsu, Z. Kabelac, and D. Katabi, "Duet: Estimating user position and identity in smart homes using intermittent and incomplete RF-data," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 2, pp. 1–21, 2018.
- [160] S. Eleftherakis, G. Santaromita, M. Rea, T. Otim, and D. Giustiniano, "Covid-19 contact tracing through multipath profile similarity," in *Proceedings of the 3rd International CoNEXT Student Workshop*, pp. 1–3, 2022.
- [161] Z. Wei, F. Liu, C. Masouros, N. Su, and A. P. Petropulu, "Toward multi-functional 6G wireless networks: Integrating sensing, communication, and security," *IEEE Communications Magazine*, vol. 60, no. 4, pp. 65–71, 2022.
- [162] S. Lu, F. Liu, Y. Li, K. Zhang, H. Huang, J. Zou, X. Li, Y. Dong, F. Dong, J. Zhu, et al., "Integrated sensing and communications: Recent advances and ten open challenges," *IEEE Internet of Things Journal*, 2024.
- [163] J. Wang, N. Varshney, C. Gentile, S. Blandino, J. Chuang, and N. Golmie, "Integrated sensing and communication: Enabling techniques, applications, tools and data sets, standardization, and future directions," *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 23416–23440, 2022.
- [164] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and Beyond," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 6, pp. 1728–1767, 2022.
- [165] W. Sun, T. Chen, and N. Gong, "SoK: Secure Human-centered Wireless Sensing," *Proceedings on Privacy Enhancing Technologies*, 2024.
- [166] H. M. Furqan, M. S. J. Solaija, H. Türkmen, and H. Arslan, "Wireless communication, sensing, and REM: A security perspective," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 287–321, 2021.
- [167] N. Su, F. Liu, C. Masouros, and A. Al Hilli, "Security and privacy in ISAC systems," in *Integrated Sensing and Communications*, pp. 477–506, Springer, 2023.
- [168] Z. Liu, C. Xu, Y. Xie, E. Sie, F. Yang, K. Karwaski, G. Singh, Z. L. Li, Y. Zhou, D. Vasisht, et al., "Exploring practical vulnerabilities of machine learning-based wireless systems," in *20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 23)*, pp. 1801–1817, 2023.
- [169] A. Blanco, N. Ludant, P. J. Mateo, Z. Shi, Y. Wang, and J. Widmer, "Performance evaluation of single base station ToA-AoA localization in an LTE testbed," in *2019 IEEE 30th annual international symposium on personal, indoor and mobile Radio Communications (PIMRC)*, pp. 1–6, IEEE, 2019.
- [170] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "Spotfi: Decimeter level localization using wifi," in *Proceedings of the 2015 ACM conference on special interest group on data communication*, pp. 269–282, 2015.
- [171] S. Eleftherakis, G. Santaromita, M. Rea, X. Costa-Pérez, and D. Giustiniano, "SPRING+: Smartphone Positioning from a Single WiFi Access Point," *IEEE Transactions on Mobile Computing*, 2024.
- [172] F. Adib, H. Mao, Z. Kabelac, D. Katabi, and R. C. Miller, "Smart homes that monitor breathing and heart rate," in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pp. 837–846, 2015.
- [173] X. Fang, W. Feng, T. Wei, Y. Chen, N. Ge, and C.-X. Wang, "5G embraces satellites for 6G ubiquitous IoT: Basic models for integrated satellite terrestrial networks," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14399–14417, 2021.
- [174] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6G era: Challenges and opportunities," *IEEE network*, vol. 35, no. 2, pp. 244–251, 2020.
- [175] F. Rinaldi, H.-L. Maattanen, J. Torsner, S. Pizzi, S. Andreev, A. Iera, Y. Koucheryavy, and G. Araniti, "Non-terrestrial networks in 5G & beyond: A survey," *IEEE access*, vol. 8, pp. 165178–165200, 2020.
- [176] M. M. Azari, S. Solanki, S. Chatzinotas, O. Kodheli, H. Sallouha, A. Colpaert, J. F. M. Montoya, S. Pollin, A. Haqiqatnejad, A. Mostafaei, et al., "Evolution of non-terrestrial networks from 5G to 6G: A survey," *IEEE communications surveys & tutorials*, vol. 24, no. 4, pp. 2633–2672, 2022.
- [177] S. Kota and G. Giambene, "6G integrated non-terrestrial networks: Emerging technologies and challenges," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, IEEE, 2021.
- [178] A. Vanelli-Coralli, A. Guidotti, T. Foggia, G. Colavolpe, and G. Montorsi, "5G and Beyond 5G Non-Terrestrial Networks: trends and research challenges," in *2020 IEEE 3rd 5G World Forum (5GWF)*, pp. 163–169, IEEE, 2020.
- [179] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, et al., "Satellite communications in the new space era: A survey and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 70–109, 2020.
- [180] A. Guidotti, A. Vanelli-Coralli, M. El Jaafari, N. Chuberre, J. Puttonen, V. Schena, G. Rinelli, and S. Cioni, "Role and Evolution of Non-Terrestrial Networks towards 6G systems," *IEEE Access*, 2024.
- [181] "3GPP TR 38.821, "Solutions for NR to support non-terrestrial networks (NTN)," version 16.2.0 Rel. 16," <https://www.3gpp.org/>.
- [182] "3GPP TR 22.865, "Study on satellite access Phase 3," version 19.2.0, Release 19," <https://www.3gpp.org/>. Accessed: 2025-05.
- [183] "3GPP TR 23.700-29, "Study on integration of satellite components in the 5G architecture; Phase 3," version 19.0.0, Release 19," <https://www.3gpp.org/>. Accessed: 2025-05.
- [184] "3GPP TS 38.300, "NR; NR and NG-RAN Overall Description; Stage 2," version 18.2.0 Rel. 18," <https://www.3gpp.org/>.
- [185] "3GPP TS 38.101-5, "User Equipment (UE) radio transmission and reception; Part 5: Satellite access Radio Frequency (RF) and performance requirements," version 18.7.0, Release 18."
- [186] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Computer Networks*, vol. 216, p. 109246, 2022.
- [187] R. Singh, I. Ahmad, and J. Huusko, "The role of physical layer security in satellite-based networks," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pp. 36–41, IEEE, 2023.
- [188] M. Vaezi, A. Azari, S. R. Khosravirad, M. Shirvanimoghaddam, M. M. Azari, D. Chasaki, and P. Popovski, "Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1117–1174, 2022.
- [189] I. Ahmad, J. Suomalainen, P. Poram, A. Gurtov, J. Huusko, and M. Höyhty, "Security of satellite-terrestrial communications: Challenges and potential solutions," *IEEE Access*, vol. 10, pp. 96038–96052, 2022.
- [190] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE signal processing magazine*, vol. 34, no. 5, pp. 27–37, 2017.
- [191] F. Chiti, R. Picchi, and L. Pierucci, "A survey on non-terrestrial quantum networking: Challenges and trends," *Computer Networks*, p. 110668, 2024.
- [192] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in new space: analysis of threats, key enabling technologies and challenges," *International Journal of Information Security*, vol. 20, pp. 287–311, 2021.
- [193] O. B. Yahia, Z. Garroussi, O. Bélanger, B. Sansò, J.-F. Frigon, S. Martel, A. Lesage-Landry, and G. K. Kurt, "Evolution of High-Throughput Satellite Systems: A Vision of Programmable Regenerative Payload," *IEEE Communications Surveys & Tutorials*, 2024.
- [194] M. Kang, S. Park, and Y. Lee, "A Survey on Satellite Communication System Security," *Sensors*, vol. 24, no. 9, p. 2897, 2024.
- [195] D. Koissler, R. Mitev, N. Yadav, F. Vollmer, and A.-R. Sadeghi, "Orbital Trust and Privacy: {SoK} on {PKI} and Location Privacy Challenges in Space Networks," in *33rd USENIX Security Symposium (USENIX Security 24)*, pp. 6093–6111, 2024.
- [196] J. Pavur, M. Strohmeier, V. Lenders, and I. Martinovic, "Qpep: An actionable approach to secure and performant broadband from geostationary orbit," Internet Society, 2021.
- [197] R. Bisping, J. Willbold, M. Strohmeier, and V. Lenders, "Wireless Signal Injection Attacks on {VSAT} Satellite Modems," in *33rd USENIX Security Symposium (USENIX Security 24)*, pp. 6075–6091, 2024.
- [198] J. Classen, A. Heinrich, F. Portner, F. Rohrbach, and M. Hollick, "Starshields for iOS: Navigating the Security Cosmos in Satellite Communication,"
- [199] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "A tale of sea and sky on the security of maritime VSAT communications," in *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 1384–1400, IEEE, 2020.
- [200] J. Pavur and I. Martinovic, "Sok: Building a launchpad for impactful satellite cyber-security research," *arXiv preprint arXiv:2010.10872*, 2020.
- [201] J. Huwyler, J. Pavur, G. Tresoldi, and M. Strohmeier, "QPEP in the Real World: A Testbed for Secure Satellite Communication Performance," in *SpaceSec*, 2023.
- [202] E. Jedermann, M. Strohmeier, V. Lenders, and J. Schmitt, "RECORD: A RECEPTION-Only region determination attack on LEO satellite users," in *33rd USENIX Security Symposium (USENIX Security 24)*, (Philadelphia, PA), pp. 6113–6130, USENIX Association, Aug. 2024.
- [203] W. Liu, Y. Li, H. Li, Y. Chen, Y. Wang, J. Lan, J. Wu, Q. Wu, J. Liu, and Z. Lai, "The dark side of scale: Insecurity of direct-to-cell satellite mega-constellations," in *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 445–464, IEEE, 2024.
- [204] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 48, no. 4, pp. 1–31, 2016.
- [205] L. Meng, L. Yang, W. Yang, and L. Zhang, "A survey of GNSS spoofing and anti-spoofing technology," *Remote sensing*, vol. 14, no. 19, p. 4826, 2022.
- [206] G. Oliveri, S. Sciancalepore, and R. Di Pietro, "GNSS spoofing detection via opportunistic IRIDIUM signals," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 42–52, 2020.
- [207] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins, "GNSS vulnerabilities and existing solutions: A review of the literature," *IEEE Access*, vol. 9, pp. 153960–153976, 2020.
- [208] "3GPP TSG RAN Meeting 102, New WID: Non-Terrestrial Networks (NTN) for NR Phase 3," [https://www.3gpp.org/ftp/tsg\\_ran/TSG\\_RAN/TSGR\\_102/Docs](https://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_102/Docs). Accessed: 2025-05.
- [209] A. Iqbal, M.-L. Tham, Y. J. Wong, G. Wainer, Y. X. Zhu, T. Dagiuklas, et al., "Empowering non-terrestrial networks with artificial intelligence: A survey," *IEEE Access*, 2023.
- [210] P. Kumar, R. Kumar, A. N. Islam, S. Garg, G. Kaddoum, and Z. Han, "Distributed AI and Blockchain for 6G-assisted terrestrial and non-terrestrial networks: Challenges and future directions," *IEEE Network*, vol. 37, no. 2, pp. 70–77, 2023.

- [211] G. Fontanesi, F. Ortiz, E. Lagunas, V. M. Baeza, M. Vázquez, J. Vázquez-Peralvo, M. Minardi, H. Vu, P. Honniah, C. Lacoste, *et al.*, "Artificial intelligence for satellite communication and non-terrestrial networks: A survey," *arXiv preprint arXiv:2304.13008*, 2023.
- [212] S. Mahboob and L. Liu, "Revolutionizing future connectivity: A contemporary survey on AI-empowered satellite-based non-terrestrial networks in 6G," *IEEE Communications Surveys & Tutorials*, 2024.
- [213] M. Rath and S. Mishra, "Security approaches in machine learning for satellite communication," *Machine learning and data mining in aerospace technology*, pp. 189–204, 2020.
- [214] L. Junzhi, L. Wanqing, F. Qixiang, and L. Beidian, "Research progress of GNSS spoofing and spoofing detection technology," in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, pp. 1360–1369, IEEE, 2019.
- [215] S. Han, J. Li, W. Meng, M. Guizani, and S. Sun, "Challenges of physical layer security in a satellite-terrestrial network," *IEEE Network*, vol. 36, no. 3, pp. 98–104, 2022.
- [216] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet of things journal*, vol. 7, no. 1, pp. 33–52, 2019.
- [217] F. Formaggio and S. Tomasin, "Authentication of satellite navigation signals by wiretap coding and artificial noise," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, pp. 1–17, 2019.
- [218] J. Liu, J. Wang, W. Liu, Q. Wang, and M. Wang, "A novel cooperative physical layer security scheme for satellite downlinks," *Chinese Journal of Electronics*, vol. 27, no. 4, pp. 860–865, 2018.
- [219] N. Hosseini-dehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 881–919, 2018.
- [220] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Information*, vol. 3, no. 1, p. 30, 2017.
- [221] K. Gao, H. Wang, and H. Lv, "Surgical Strike on 5G Positioning: Selective-PRS-Spoofing Attacks and Its Defence," *IEEE Journal on Selected Areas in Communications*, 2024.
- [222] G. Focarelli, S. Zanini, G. Bianchi, and S. Bartoletti, "Physical Layer Threats to 5G Positioning: Impact on TOA-Based Methods," in *2024 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 926–931, IEEE, 2024.
- [223] "3GPP TS 22.369, "Service requirements for ambient power-enabled IoT; Stage 1" version 19.1.0 Rel. 19," <https://www.3gpp.org/>. Accessed: 2025-05.
- [224] "3GPP TR 38.769, "Study on solutions for ambient IoT (Internet of Things) in NR," version 19.0.1 Rel. 19," <https://www.3gpp.org/>. Accessed: 2025-05.
- [225] A. Varshney, O. Harms, C. Pérez-Penichet, C. Rohner, F. Hermans, and T. Voigt, "LoRea: A backscatter architecture that achieves a long communication range," in *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*, pp. 1–14, 2017.
- [226] V. Talla, M. Hesar, B. Kellogg, A. Najafi, J. R. Smith, and S. Gollakota, "Lora backscatter: Enabling the vision of ubiquitous connectivity," *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies*, vol. 1, no. 3, pp. 1–24, 2017.
- [227] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," *ACM SIGCOMM computer communication review*, vol. 43, no. 4, pp. 39–50, 2013.
- [228] "3GPP TR 38.769, "Study on solutions for ambient IoT (Internet of Things)", Rel. 19," <https://www.3gpp.org/>. Accessed: 2025-05.
- [229] N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Communications surveys & tutorials*, vol. 20, no. 4, pp. 2889–2922, 2018.
- [230] T. Jiang, Y. Zhang, W. Ma, M. Peng, Y. Peng, M. Feng, and G. Liu, "Backscatter communication meets practical battery-free Internet of Things: A survey and outlook," *IEEE Communications Surveys & Tutorials*, 2023.
- [231] "3GPP TR 33.713, "Study on Security Aspect of Ambient IoT Services in 5G," version 19.3.0, Release 19," <https://www.3gpp.org/>. Accessed: 2025-05.
- [232] D. Zanetti, B. Danev, and S. Capkun, "Physical-layer identification of UHF RFID tags," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, pp. 353–364, 2010.
- [233] R. Narayanan, A. Varshney, and P. Papadimitratos, "Harvestprint: Securing battery-free backscatter tags through fingerprinting," in *Proceedings of the 20th ACM Workshop on Hot Topics in Networks*, pp. 178–184, 2021.
- [234] S. Khandker, M. Guerra, E. Bitsikas, R. P. Jover, A. Ranganathan, and C. Pöpper, "Astra-5g: automated over-the-air security testing and research architecture for 5g sa devices," in *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 89–100, 2024.
- [235] A. Scalingi, S. D'Oro, F. Restuccia, T. Melodia, D. Giustiniano, *et al.*, "Det-RAN: Data-Driven Cross-Layer Real-Time Attack Detection in 5G Open RANs," in *IEEE International Conference on Computer Communications*, pp. 1–10, 2024.
- [236] "3GPP TS 33.846, "Study on authentication enhancements in the 5G System (5GS)," version 17.0.0 Rel. 17," <https://www.3gpp.org/>. Accessed: 2025-05.
- [237] T. Heiligenberg, G. Knips, C. Böhm, D. Rupprecht, and K. Kohls, "BigMac: Performance Overhead of User Plane Integrity Protection in 5G networks," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 145–150, 2023.
- [238] M. M. Saeed, R. A. Saeed, R. A. Mokhtar, H. Alhumyani, and E. S. Ali, "A novel variable pseudonym scheme for preserving privacy user location in 5G networks," *Security and Communication Networks*, vol. 2022, 2022.
- [239] M. M. Saeed, R. A. Saeed, and E. Saeid, "Identity division multiplexing based location preserve in 5G," in *2021 International Conference of Technology, Science and Administration (ICTSA)*, pp. 1–6, IEEE, 2021.
- [240] A. Lotto, V. Singh, B. Ramasubramanian, A. Brighente, M. Conti, and R. Pooven-dran, "BARON: Base-Station Authentication Through Core Network for Mobility Management in 5G Networks," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 133–144, 2023.
- [241] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, "Insecure connection bootstrapping in cellular networks: the root of all evil," in *Proceedings of the 12th conference on security and privacy in wireless and mobile networks*, pp. 1–11, 2019.
- [242] A. Singla, R. Behnia, S. R. Hussain, A. Yavuz, and E. Bertino, "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*, pp. 501–515, 2021.
- [243] Y. Li, S. Liu, Z. Yan, and R. H. Deng, "Secure 5G positioning with truth discovery, attack detection, and tracing," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22220–22229, 2021.
- [244] P. K. Nakarmi, M. A. Ersoy, E. U. Soykan, and K. Norrman, "Murat: Multi-rat false base station detector," *arXiv preprint arXiv:2102.08780*, 2021.
- [245] K. S. Mubasshir, I. Karim, and E. Bertino, "FBSDetector: Fake Base Station and Multi Step Attack Detection in Cellular Networks using Machine Learning," *arXiv preprint arXiv:2401.04958*, 2024.
- [246] P. K. Nakarmi, J. Sternby, and I. Ullah, "Applying machine learning on rsrp-based features for false base station detection," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–7, 2022.
- [247] M. Saedi, A. Moore, P. Perry, and C. Luo, "RBS-MLP: A Deep Learning based Rogue Base Station Detection Approach for 5G Mobile Networks," *IEEE Transactions on Vehicular Technology*, 2024.
- [248] H. Wen, P. Porras, V. Yegneswaran, A. Gehani, and Z. Lin, "5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service," in *Proceedings of the 31st Annual Network and Distributed System Security Symposium (NDSS'24)*, San Diego, California, USA. The Internet Society. Google Scholar Google Scholar Cross Ref Cross Ref, 2024.
- [249] M. Polese, L. Bonati, S. D'oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1376–1411, 2023.
- [250] S. Park, D. Kim, Y. Park, H. Cho, D. Kim, and S. Kwon, "5G security threat assessment in real networks," *Sensors*, vol. 21, no. 16, p. 5524, 2021.
- [251] S. Park, I. You, H. Park, and D. Kim, "Analyzing RRC Replay Attack and Securing Base Station with Practical Method," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–8, 2022.
- [252] Z. Cheng, M. Ordean, F. D. Garcia, B. Cui, and D. Rys, "Watching your call: Breaking VoLTE privacy in LTE/5G networks," *arXiv preprint arXiv:2301.02487*, 2023.
- [253] S. Kwon, S. Park, H. Cho, Y. Park, D. Kim, and K. Yim, "Towards 5G-based IoT security analysis against Vo5G eavesdropping," *Computing*, vol. 103, pp. 425–447, 2021.
- [254] M. S. Wani, M. Rademacher, T. Horstmann, and M. Kretschmer, "Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy," *Journal of Cybersecurity and Privacy*, vol. 4, no. 1, pp. 23–40, 2024.