

Review

From 2G to 5G: Literature Review of Identification and Location Attacks in Cellular Networks

Daniel Asimionesei  and Nirvana Alina Popescu * 

Faculty of Automatic Control and Computer Science, National University of Science and Technology POLITEHNICA Bucharest, Splaiul Independentei No. 313, District 6, 060042 Bucharest, Romania; daniel.asimionesei@stud.acs.upb.ro

* Correspondence: nirvana.popescu@upb.ro

Abstract

Cellular networks from 2G to 5G have evolved to improve performance, reliability, and security. However, the protection of user identity and location remains a persistent challenge across generations. Although newer architectures introduce stronger authentication, temporary identifiers, and privacy-preserving mechanisms, attacks such as IMSI catching, paging-based tracking, downgrade attacks, and identifier correlation continue to affect cellular systems. This study analyzes identification and location attacks in 2G, 3G, 4G, 5G Non-Standalone (5G NSA), and 5G Standalone (5G SA) networks. The analysis focuses on studies published between 2018 and 2026 and follows a structured methodology based on research questions, inclusion and exclusion criteria, quality assessment, and comparative synthesis of studies identified in scientific databases. Following the selection process, 86 studies were included in the final analysis. The review compares attack vectors, affected identifiers, exploited procedures, adversary capabilities, reported performance metrics, and proposed mitigations for each network generation. The results show that vulnerabilities inherited from previous generations, especially GSM/2G, remain relevant in modern architectures through downgrade attacks, fallback mechanisms, and LTE anchoring in 5G NSA deployments. The main contribution of this study is a cross-generational comparative synthesis of identity and location attacks in cellular networks. The findings highlight the need for rigorous standards implementation, effective detection mechanisms, reduced reliance on legacy technologies, and practical evaluation of mitigation solutions in real cellular environments.

Keywords: cellular networks; identity privacy; location privacy; IMSI catcher; fake base station; paging attack; GUTI; SUCI; 5G NSA; 5G SA; cellular privacy; downgrade attacks



Academic Editor: Hossain Shahriar

Received: 16 May 2026

Revised: 10 July 2026

Accepted: 11 July 2026

Published: 14 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Cellular network infrastructure is one of the core components of global digital infrastructure and supports a large share of modern communications. The evolution of mobile networks has been driven by the need for more efficient and secure networks. From one generation to the next, both the architecture and the security mechanisms have become increasingly complex and have included mutual authentication mechanisms, anonymization of unique identifiers and advanced encryption. The International Mobile Subscriber Identity (IMSI) used in 2G–4G networks to identify a user and the Subscription Permanent Identifier (SUPI) in 5G are direct targets for identification and location attacks. Even the use of temporary pseudonyms such as Temporary Mobile Subscriber Identity (TMSI) or

Globally Unique Temporary UE Identity (GUTI) can be tracked and correlated with the user's identity in the context of network mechanisms such as attach, paging, registration, Location Area Update, Tracking Area Update, Routing Area Update, which can expose sensitive information. The 2G generation used a one-way authentication mechanism in which only the Base Transceiver Station (BTS) authenticates the mobile terminal, and the IMSI is transmitted in the clear to the operator, which allowed fake BTS attacks. In the architecture of 3G and 4G technologies, a mutual authentication mechanism and improved encryption were used, and the user's identity was no longer directly exposed. However, attacks have not disappeared in 4G either, where identification and location take place by exploiting signaling procedures, paging mechanisms, correlation of temporary identifiers or interoperability scenarios. The 5G generation introduced the Subscription Concealed Identifier (SUCI), a privacy-preserving concealed form of the Subscription Permanent Identifier (SUPI), to reduce the exposure of permanent subscriber identity during initial network access [1], but the integration of the Long-Term Evolution (LTE) infrastructure into the 5G Non-Standalone (NSA) architecture, maintaining compatibility through fall-back/downgrade with previous generations and the non-uniformity of the networks of mobile network operators that adopt different configurations and implementations, create indirect opportunities for identity and location disclosure by exploiting the vulnerabilities of older technologies. In addition, the attack surface is expanded due to the complexity of the 4G and 5G architectures that implement different control protocols used for connection, authentication and mobility management.

Mobile networks have evolved from simple 2G architectures designed mainly for voice services to complex, scalable, low-latency 5G architectures. In parallel, security mechanisms have increasingly focused on stronger authentication, user identity protection, and secure communication between terminals and the network [2]. Protecting the identity and location of a mobile terminal has been a sensitive point in the architecture of all generations of cellular networks. In Global System for Mobile Communications (GSM) networks, the IMSI identifier is transmitted in the clear, and authentication is unidirectional, as only the BTS authenticates the mobile terminal, which has favored fake BTS attacks. In LTE networks, a bidirectional authentication mechanism was introduced, and the IMSI was replaced with a series of temporary identifiers such as TMSI or GUTI, which initially reduced the identity attack surface, but the way these pseudonyms are managed and reused has created new security gaps. Among the procedures that underlie the functioning of networks, we identified several procedures within the control plane that can expose sensitive information that can facilitate the location or identification of a user. The design of 5G networks has been improved by introducing the SUCI mechanism, which protects the user's identity by encrypting it, but the integration of LTE networks into the 5G NSA infrastructure offers the possibility of indirect attack scenarios on identity or location [1]. This shows that, in each generation, new security mechanisms have been introduced, but identification and location vulnerabilities have not been eliminated; instead, they have adapted to new architectures.

The popularity of mobile devices has grown rapidly, making the protection of user identity and location crucial for national security and critical infrastructure protection. Mobile terminals support a wide range of domains, from banking applications, government communications, healthcare systems and industrial control to IoT applications, so unauthorized identification and location of mobile terminals can lead to abusive directional attacks [3,4]. Numerous fragmented studies have examined generation-specific vulnerabilities, such as IMSI catching in GSM, paging attacks in LTE, and interoperability issues in 5G. The need for a centralizing synthesis that presents the identification and location attacks in 2G–5G cellular networks in comparison is the motivation for this study.

The research problem is identity exposure in cellular networks and the impact on location attacks. Identification (IMSI catcher) or location attacks (paging-based location, multi-cell correlations) can have devastating implications for privacy [5], the safety of vulnerable individuals, and legal compliance. The widespread availability of Software-Defined Radios (SDRs), together with open-source cellular network stacks, has facilitated the emergence of low-cost attacks that require relatively limited resources. Although each generation has brought security improvements such as two-way authentication, new encryption algorithms (A5/3, EPS-AKA, 5G-AKA/SUCI) [6], encryption of identifiers or the use of temporary identifiers, vulnerabilities have persisted in a form adapted to the new architectures. The fact that in the network mechanisms (registration, attach, paging, handover) there are sensitive data exchanges that can allow the identification and location of mobile terminals, even when the IMSI is not transmitted in the clear, represents the main problem in mobile telephony networks [7]. The complexity of 4G and 5G networks, added to which is the interoperability between generations (downgrade LTE to 2G, inter-RAT) and maintaining compatibility, creates new attack scenarios. Attackers manage to bypass theoretical protections and exploit the heterogeneous configurations of different operators. Thus, in 5G networks, identity protection is no longer limited to preventing the explicit transmission of permanent identifiers; attackers may also rely on behavioral correlations and traffic-pattern analysis based on inferred metadata [8].

This paper provides a comparative analysis of identification and location attacks in 2G–5G networks documented in the literature. The goal is to understand how these attacks have evolved, which mechanisms they exploit, the extent to which new protection techniques reduce risk, which vulnerabilities persist due to interoperability and legacy dependencies, and which gaps remain in the current literature. This literature review covers identification and location attacks in 2G, 3G, 4G, 5G Non-Standalone (5G NSA), and 5G Standalone (5G SA) networks, including IMSI catcher, fake base station, and downgrade scenarios, paging-based inference, location attacks based on multi-cell correlations, and the exploitation of information from signaling channels.

The specific objectives of this study are to identify and classify documented attacks according to their type and operational level, including radio, core network, and protocol levels; to analyze the procedures exploited in each cellular generation; to examine how these attacks have evolved over time, with a focus on common patterns and changes in the attack surface; to evaluate mitigation solutions involving cryptographic mechanisms, detection methods, and identification policies; and to determine the vulnerabilities and practical impact of differences between theoretical specifications and real-world implementations, as well as future research directions.

The literature still lacks a centralized perspective examining the evolution of identification and location attacks from 2G to 5G, highlighting the changing attack surface. The lack of such a perspective makes it difficult to identify recurring patterns, exploited mechanisms, the impact of technological progress, and the coherent assessment of countermeasures.

First, the transition to 5G is still shaped by gradual deployment and adaptation to existing infrastructure. Many commercial 5G deployments rely on Non-Standalone (NSA) operation, in which 5G networks remain dependent on 4G infrastructure. Under these conditions, modern 5G mechanisms inherit procedures from LTE networks so that the analysis of a vulnerability can no longer be limited to a single generation, but must also take into account interactions with previous generations [9].

Secondly, modern networks rely on a more complex service-based architecture and virtualized network functions, which increase the attack surface. As a result, the attack no longer focuses on intercepting the unique identifier itself, but rather on exploiting fundamental network mechanisms and procedures to infer sensitive metadata.

Thirdly, it is a crucial moment when a critical evaluation of previous technologies with a focus on identified vulnerabilities can represent a starting point in discussions about 6G technology, so that these problems are no longer propagated in future architectures.

Finally, the identified studies reveal a fragmented literature. Many studies focus on a specific attack type, a single cellular generation, or isolated experimental scenarios. The lack of an overall picture makes it difficult to truly assess the progress brought by new security mechanisms.

This literature review aims to provide a clearer understanding of cellular network security by offering a comparative analysis of identification and location attacks across 2G–5G networks. It integrates isolated studies, examines vulnerabilities across generations, and analyzes how the attack surface has evolved from hardware-based attacks to signaling exploitation and cross-generation interoperability attacks. The paper proposes a methodology for classifying attacks based on typology, level of operation, exploited mechanisms, impact and analyzes the progress of identity protection mechanisms. Last but not least, the study aims to identify areas with gaps that require increased attention and formulate future directions of study in identity and location protection [10].

The main contributions of this study are fivefold. First, it provides a systematic synthesis of mobile network generations by centralizing the evolution of vulnerabilities across cellular technologies. Second, it proposes a classification of attacks according to network generation, from 2G to 5G, including both 5G NSA and 5G SA, attack typology, namely passive, semi-passive, and active attacks, and attack-surface layer, including the Physical Layer (PHY), Medium Access Control (MAC), Radio Resource Control (RRC), Non-Access Stratum (NAS), and Core Network. Third, it analyzes the evolution of the attack surface, highlighting the transition from hardware-based attacks in 2G to protocol- and signaling-based attacks in more recent generations, particularly 4G and 5G. Fourth, it systematically evaluates attack performance according to key metrics such as accuracy, execution time, cost, and the conditions under which the attacks are performed. Finally, it assesses protection mechanisms in terms of their implementation level, including standardization, operator-side deployment, User Equipment (UE) support, and detection mechanisms, as well as their effectiveness, costs, and limitations.

This study is intended for the academic community in mobile communications security, telecommunications security specialists, mobile network operators, standardization bodies, and mobile terminal manufacturers. The literature review provides a list of measures against identification and location attacks that can be a starting point for mobile terminal manufacturers.

This review presents a comparative analysis of the literature, focusing on the theoretical foundations underlying attacks on mobile network security and offers a progressive vision as follows:

- Section 1. Introduction to the context, motivation of the study, issues, objectives, contributions
- Section 2. Systematic review methodology, protocol, research questions
- Section 3. Theoretical foundations of identification and location mechanisms and conceptual framework
- Section 4. Review results, distribution and taxonomy of attacks, experimental techniques
- Section 5. Analysis of results, answers to Research Questions (RQs), vulnerabilities, limitation, mitigation measures and future directions
- Section 6. Study conclusions

2. Review Methodology

The aim of this chapter is to ensure a transparent and reproducible approach, so that the data extracted from the selected studies and the results obtained can be replicated by other researchers. Taking into account the multidisciplinary framework of the chosen topic, the methodology aims to clearly document the selection decisions and objectively compare the results identified in the literature. The defined research protocol follows Kitchenham's recommendations for planning a literature review, to which are added the principles of an adapted PRISMA-like literature review (PRISMA = Preferred Reporting Items for Systematic Reviews and Meta-Analyses. In this review, the term "PRISMA-like" indicates that the selection flow was adapted to the scope of the study and used to report the identification, screening, eligibility assessment, and inclusion of studies.). The delimitation of the research domain is done with the help of research questions regarding identification and location in 2G–5G. The chosen search strategy, search strings and data sources are also presented here. The final set of papers analyzed is obtained by applying inclusion and exclusion criteria and a stepwise selection process. Data are extracted using a standardized scheme, and studies are assessed using a quality and risk of bias assessment mechanism. Finally, conclusions are aggregated to highlight the evolution of attacks.

2.1. Protocol and Guideline Used

The benchmarks underlying the methodology followed are Kitchenham's guide, which is oriented towards rigorous planning and systematic review, and the framework of an adapted PRISMA-like literature review that ensures transparency of the selection process. Considering that the chosen theme includes both theoretical contributions and empirical results, the chosen combination is justified by the empirical nature of the studied field.

Before starting the searches, the literature review protocol was defined by establishing the objective of systematizing identification and location attacks in 2G–5G networks; formulating research questions to guide the identification of attack typologies, adversary capabilities, and countermeasures; defining the search strategy, including target databases, the temporal range, and search strings; specifying explicit inclusion and exclusion criteria to be consistently applied during screening; outlining the step-by-step selection process, including duplicate removal, title and abstract screening, and full-text evaluation; preparing a standardized data extraction template to ensure consistency across attack type, network generation, vector or procedure, adversary capabilities, metrics, resources, limitations, and countermeasures; defining a quality assessment and risk-of-bias procedure based on a quality assessment (QA) score ranging from 0 to 12; and selecting a synthesis method based on structured narrative synthesis and comparisons of attacks by generation and procedure.

As shown in Figure 1, the study selection methodology follows an adapted PRISMA-like flow. The role of the adapted PRISMA-like approach in this review is to ensure transparency of the selection made in the literature. The study selection diagram, based on an adapted PRISMA-like process, presents the audit mechanism used, where the path of each research paper can be seen, from identification to final inclusion. The initial search identified 1055 records: 188 from IEEE Xplore, 113 from ScienceDirect, and 754 from SpringerLink. After removing 91 duplicate records, 964 records were retained for the screening stage based on title and abstract. At this stage, 831 records were excluded, and 133 full-text articles were evaluated for eligibility. During the full-text evaluation, 47 articles were excluded for the following reasons: incorrect topic ($n = 10$), falling outside the 2G–5G domain ($n = 6$), lack of a relevant analysis of identification/location attacks ($n = 19$), and lack of a technical contribution ($n = 12$).

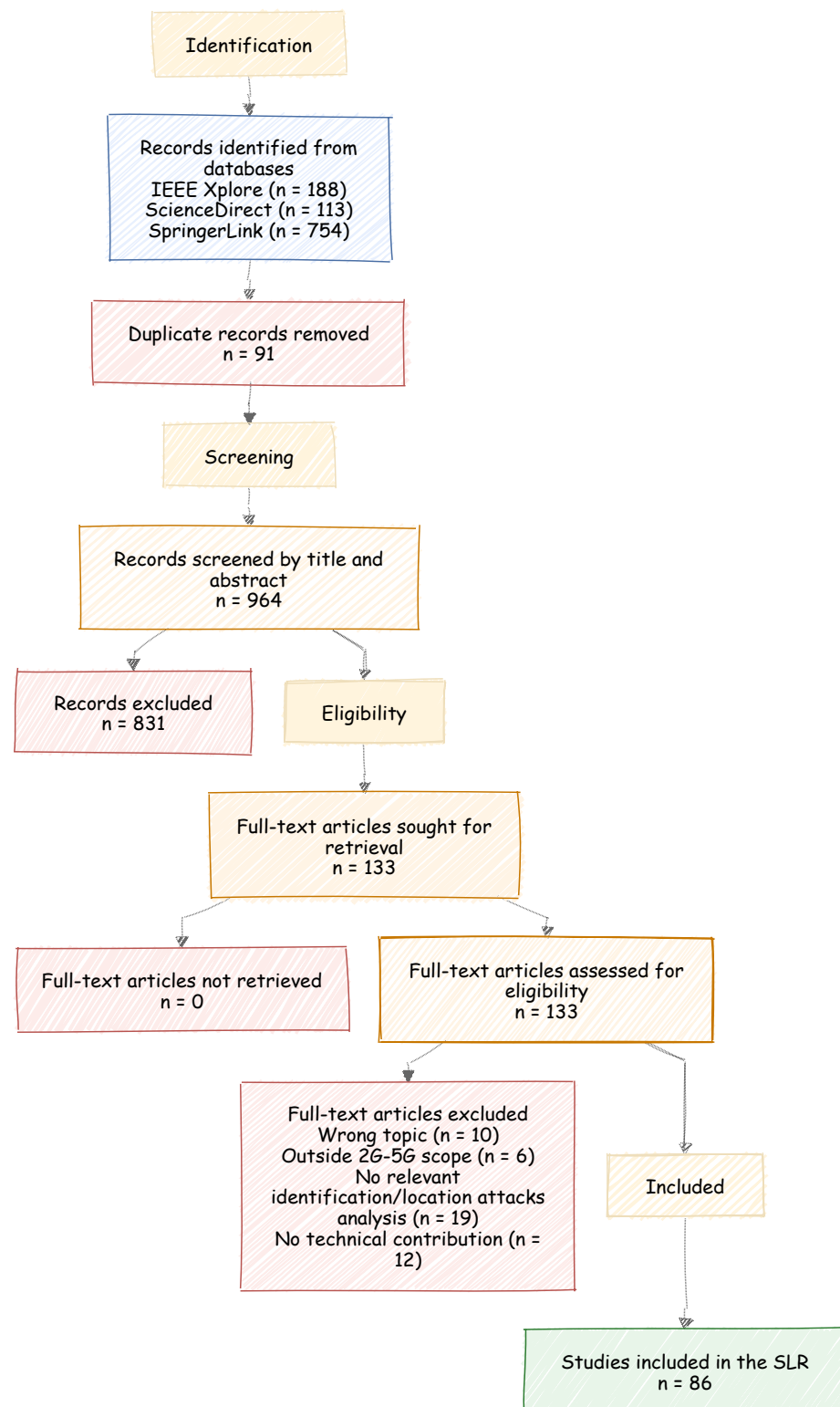


Figure 1. Study selection methodology. The PRISMA diagram illustrates the process of identifying, eliminating duplicates, screening, assessing eligibility, and final inclusion of studies in the systematic literature review.

For transparency and reproducibility, the complete list of studies excluded after full-text assessment, together with the applied exclusion criterion and the specific reason for exclusion, is provided in Appendix B. The date on which the systematic searches were

conducted in the IEEE Xplore, ScienceDirect, and SpringerLink databases to identify eligible studies published during the analyzed period 2018–2026 was 19 March 2026.

Finally, 86 studies were included in the systematic literature review and used for data extraction, quality assessment, and synthesis. The complete list of the studies included after the selection process, together with the main extracted data for each study, is provided in Appendix A.

The main phases of the Kitchenham guideline used in this literature review for clearly defining the protocol are:

- Plan Review: formulating the study objectives, formulating research questions, choosing the protocol, choosing data sources and designing the search strategy, formulating inclusion/exclusion criteria and drafting the data extraction scheme.
- Conduct Review: execution of searches, results management, step-by-step screening (title, abstract, full-text), application of selection criteria and assessment of study quality.
- Document Review: organizing results, synthesizing findings, discussing limitations and formulating implications (operators, UE, standardization).

As shown in Figure 2, the review process follows the Kitchenham methodology phases.

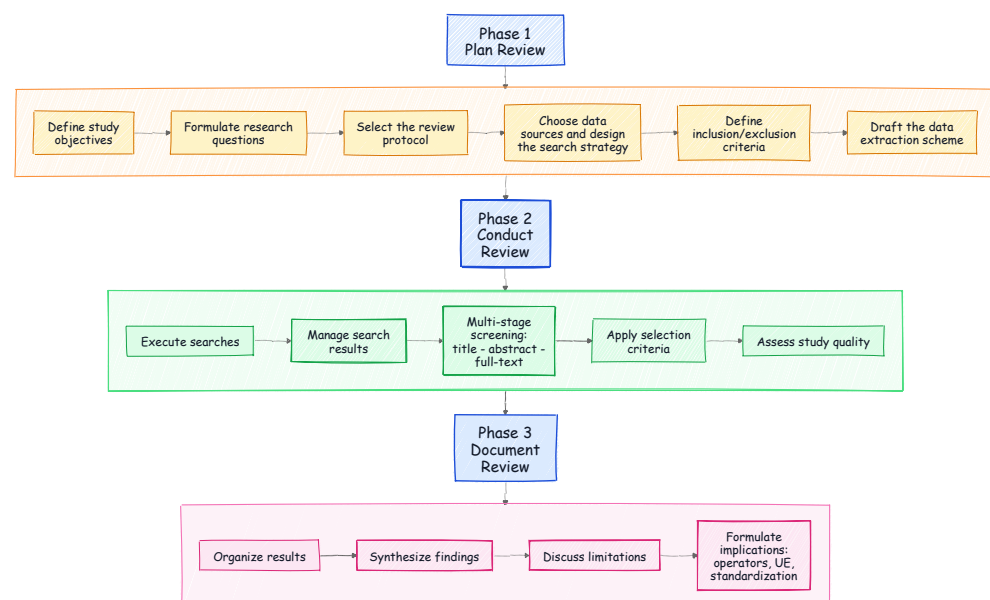


Figure 2. The systematic review process adapted from the Kitchenham methodology. The figure illustrates the three phases of the study: planning the review, conducting the review, and documenting the results, along with the main activities associated with each phase.

2.2. Research Questions (RQ)

A central element of this literature review is the research questions that establish the direction of the analysis, the search strategy, the selection and data extraction criteria. The research questions of this study aim to identify the main types of vulnerabilities, the technical mechanisms exploited by attackers and the effectiveness of countermeasures. In this literature review, the research questions were formulated taking into account the particularities of the field studied, so as to facilitate the comparison of the evolution of vulnerabilities and protection mechanisms between different generations of cellular networks:

1. RQ1: What types of identification and location attacks are documented in cellular networks and how can they be classified?

This question aims to identify and classify the main types of attacks according to 2G–5G generation, capability (passive, semi-passive, active), vectors and procedures exploited (PHY/MAC/RRC/NAS/Core; paging, attach/registration, measurement,

inter-RAT/downgrade, SS7/Diameter), nature of the attack (identification, location) and affected component (RAN/Core) [11] (PHY = Physical Layer; MAC = Medium Access Control; RRC = Radio Resource Control; NAS = Non-Access Stratum; Core = Core Network; inter-RAT = inter-Radio Access Technology; SS7 = Signaling System No. 7; Diameter = authentication, authorization, and accounting protocol used in mobile core networks; RAN = Radio Access Network.).

2. RQ2: What are the capabilities and resources required to carry out these attacks?
This question investigates the attack model described in the literature (cost, range, and technical complexity).
3. RQ3: What performance do the studies report?
This question targets the metrics identified in the literature, targeting both qualitative and quantitative aspects (identification success rate, location accuracy, time, detectability).
4. RQ4: What countermeasures are described (standard, operator, mobile terminal), what is their effectiveness and what are the associated limitations?
This question aims to classify countermeasures as follows: standard, operator-implemented, mobile terminal-level measurements, detection solutions (rule-based, crowd-sourcing).
5. RQ5: How does the attack surface evolve from 2G to 5G and what vulnerabilities persist?
This question analyzes what vulnerabilities persist due to cross-generation compatibility and inter-RAT scenarios (fallback/downgrade, NSA anchoring).

These questions allow for the classification and comparison of documented identification and location attacks and the evaluation of the evolution of security mechanisms depending on the 2G–5G generation.

2.3. Used Data Sources and Databases

The databases used in this literature review to select scientific publications in the field of identification and location attacks are:

- Elsevier: the platform that includes scientific journals in the field of communications, computer security, etc.
- IEEE Xplore Digital Library: database that includes articles published in IEEE journals and conferences relevant to cellular network security.
- Springer: database that includes papers published in journals and conference proceedings in the field of network security.
- Google Scholar: it was not used as the primary database in the systematic search, but rather as a complementary tool for snowballing, verifying citations, identifying related works, and accessing the full text of articles initially found in IEEE Xplore, ScienceDirect, or SpringerLink.

The use of these databases provided a sufficiently large set of studies to form the basis of this literature review. Table 1 presents the initial number of results obtained from each database search.

Table 1. Scientific databases used for the systematic search and the number of records initially identified from each source.

Database	Number of Results
IEEE Xplore	188
Elsevier/ScienceDirect	113
Springer	754
Total	1055

The publication types considered in this literature review include journal articles, conference papers, academic book chapters, and experimental studies.

The time interval chosen for the selection of studies is 2018–2026. This interval was chosen because this period covers the evolution of 2G–5G networks, security mechanisms, but also because during this period, numerous studies on vulnerabilities associated with identification and location mechanisms appeared, which provide interdisciplinary coverage and provide a balance between the 2G past and the 4G/5G present. Numerous studies from this period analyze the vulnerabilities indirectly inherited by modern networks from previous 2G technologies. The temporal evolution of the number of publications by database is illustrated in Figure 3. The year 2026 was excluded from this timeline only because it was still an incomplete publication year at the time of the systematic search conducted on 19 March 2026. Eligible publications from 2026 that were indexed before that date were included in the final corpus, provided they met the inclusion criteria. Choosing this range does not imply ignoring previous contributions. Studies published before 2018 were used as a theoretical and historical foundation for explaining the evolution of identity and location attacks and were not subject to inclusion/exclusion criteria. An important part of the work focuses on vulnerabilities inherited from GSM/2G networks, and how they can continue to affect the security of 4G/5G networks through mechanisms such as fallback, downgrade attacks, and interoperability of old and new infrastructures. The period 2018–2026 was also chosen because during this period, the literature highlights an intensification of research on identity and location privacy in cellular networks, amid the transition to 5G and the security implications generated by the dependence of 5G NSA implementations on the existing LTE infrastructure. The non-inclusion of studies published before 2018 in the systematic review may be a limitation of this review, but these works were used for technical and historical contextualization, to understand the origin of certain vulnerabilities.

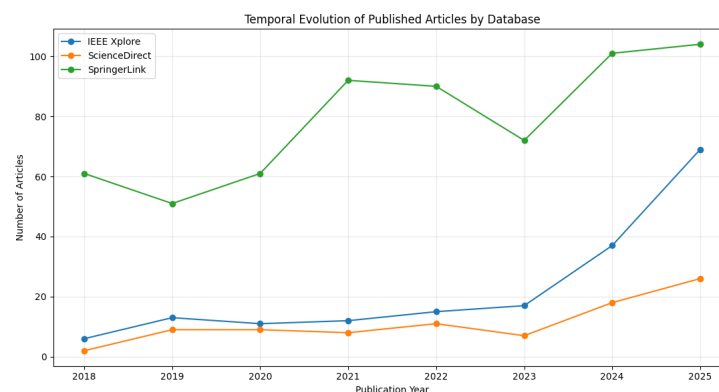


Figure 3. Distribution by year of articles identified in the search stage, before the final selection of studies.

2.4. Search Strategy

The strategy used to identify studies related to identification and location attacks consists of a structural search built around the research questions. Considering the terminological diversity in the literature and the differences between cellular generations, after identifying the main concepts associated with the study topic, three complementary types of searches were formulated. The general search was used to identify studies that directly address identification and location attacks in cellular networks, the mapping search was designed to identify studies analyzing vulnerable mechanisms and procedures in mobile networks, and snowballing was applied by examining the bibliographies of the included studies and identifying works that cite already included publications.

The approach described above allows for the coverage of studies focused on security and attacks, as well as studies that analyze mechanisms that may have implications for user security. The dimensions exploited in the search strategy are cellular network technologies, user identification attacks and user location attacks.

Based on the study objectives and research questions, three main categories of terms were defined for constructing the search strings: terms related to cellular generations, including GSM, 2G, Universal Mobile Telecommunications System (UMTS), 3G, LTE, 4G, 5G, New Radio (NR), cellular networks, and mobile networks; terms related to identification and location, including IMSI catcher, rogue base station, fake base station, identity exposure, subscriber identification, location tracking, user tracking, and privacy leakage; and terms related to exploitable network procedures and parameters, including paging, attach procedure, registration procedure, temporary identifiers, TMSI, GUTI, SUPI, SUCI, timing advance, measurement reports, cell-ID, and handover.

To avoid irrelevant results, searches were limited to titles, abstracts, and keywords, and specialized terms were used where necessary. The search process was performed using the Advanced Search function available in the IEEE Xplore, Elsevier and Springer platforms.

2.4.1. IEEE Xplore

Search terms were queried in the title, abstract and keywords fields in various combinations of search strings, as summarized in Table 2. The main terms related to attacks were searched in the title of the publication or in the abstract, as these fields directly reflect the main topic of the article. Validation of the strategy was carried out in a step where it was checked whether the search strings returned works relevant to identification and location attacks. The results of each database were exported and centralized in a reference management system, where duplicates were eliminated, and the resulting references were subjected to a selection process based on an adapted PRISMA-like approach. Filters used:

- Content type: Journals + Conferences
- Publication years: Years: 2018–2026
- Language: English
- Sort by: relevance

Table 2. General and mapping search strings used in the IEEE Xplore database.

Search Type	Search String
General search	((Publication Title: “IMSI catcher” OR “fake base station” OR “rogue base station” OR “location tracking” OR “subscriber identity exposure”) OR (Abstract: “IMSI catcher” OR “fake base station” OR “rogue base station” OR “location tracking” OR “subscriber identity exposure” OR “identity leakage” OR “re-identification” OR “user tracking”)) AND (Abstract: “cellular network” OR “mobile network” OR GSM OR UMTS OR LTE OR “4G” OR “5G” OR NR)
Mapping search	(Abstract: “paging” OR “paging message” OR “temporary identifier” OR TMSI OR GUTI OR SUPI OR SUCI OR “timing advance” OR “measurement report” OR “cell ID” OR TAC OR ECGI OR “control plane” OR NAS OR RRC OR S1AP) AND (Abstract: “paging” OR “paging message” OR “temporary identifier” OR TMSI OR GUTI OR SUPI OR SUCI OR “timing advance” OR “measurement report” OR “cell ID” OR TAC OR ECGI OR “control plane” OR NAS OR RRC OR S1AP) AND (Abstract: “cellular network” OR “mobile network” OR GSM OR UMTS OR LTE OR “4G” OR “5G”)

2.4.2. Elsevier/ScienceDirect

In the ScienceDirect database, terms were searched in the title and abstract fields, using a query that combines terms (IMSI = International Mobile Subscriber Identity; GSM = Global System for Mobile Communications; UMTS = Universal Mobile Telecommunications System; LTE = Long-Term Evolution; NR = New Radio; TMSI = Temporary Mobile

Subscriber Identity; GUTI = Globally Unique Temporary UE Identity; SUPI = Subscription Permanent Identifier; SUCI = Subscription Concealed Identifier; TAC = Tracking Area Code; ECGI = E-UTRAN Cell Global Identifier; NAS = Non-Access Stratum; RRC = Radio Resource Control; S1AP = S1 Application Protocol.) related to identification and location attacks with cellular network generations and security-related concepts, as summarized in Table 3.

Table 3. General and mapping search strings by cellular network generation used in the ScienceDirect database.

Search Type	Generation	Search String
General search	2G—GSM	(identity OR privacy OR tracking) AND (location OR localization) AND (GSM OR “2G”)
General search	3G—UMTS	(identity OR privacy OR tracking) AND (location OR localization) AND (UMTS OR “3G”)
General search	4G—LTE	(identity OR privacy OR tracking) AND (location OR localization) AND (LTE OR “4G”)
General search	5G	(identity OR privacy OR tracking) AND (location OR localization) AND (“5G”)
Mapping search	2G/3G	(identifier OR paging OR “temporary identifier”) AND (privacy OR tracking) AND (GSM OR UMTS)
Mapping search	4G—LTE	(identifier OR paging OR “timing advance”) AND (tracking OR localization) AND (LTE)
Mapping search	5G	(identifier OR “control plane”) AND (privacy OR tracking) AND (“5G”)

2.4.3. Springer

In the Springer database, the search was performed using filters on title, abstract and keywords of the publications, as summarized in Table 4.

Table 4. General and mapping search strings used in the Springer database.

Search Type	Search String
General search	(“IMSI catcher” OR “fake base station” OR “rogue base station” OR “location tracking” OR “subscriber identity exposure” OR “identity leakage” OR “re-identification” OR “user tracking” OR “location privacy”) AND (“cellular network” OR “mobile network” OR GSM OR UMTS OR LTE OR “4G” OR “5G”)
Mapping search	(“paging” OR “paging message” OR “temporary identifier” OR TMSI OR GUTI OR SUPI OR SUCI OR “timing advance” OR “measurement report” OR “cell ID” OR TAC OR ECGI OR “control plane” OR NAS OR RRC OR S1AP) AND (“privacy” OR “tracking” OR “location inference” OR “re-identification” OR “identity exposure” OR “information leakage”) AND (“cellular network” OR “mobile network” OR GSM OR UMTS OR LTE OR “4G” OR “5G”)

2.5. Inclusion and Exclusion Criteria

The transparency and reproducibility of this work are ensured by the use of inclusion and exclusion criteria defined within an adapted PRISMA-like methodology. These criteria were applied progressively during the selection process, according to the amount of information available at each screening stage. During the title, abstract, and keyword screening stage, only the criteria that could be reliably assessed from the bibliographic information were applied, namely IC1–IC3 and EC1–EC3. The remaining criteria, IC4–IC6 and EC4–EC6, required examination of the full paper and were, therefore, applied during the full-text eligibility assessment.

Inclusion criteria:

- IC1: Studies investigating user identification and location in 2G–5G cellular networks.
- IC2: Attacks that exploit network vectors (IMSI/TMSI/SUPI/SUCI, paging, TAC/LAI/-TAI, Cell-ID/ECGI, timing advance, handover, RRC/NAS/S1AP, broadcast/system information).
- IC3: Studies published in journals, conference proceedings, or academic volumes, with full-text access available.
- IC4: Clarity of the attack mechanism or network vulnerabilities.
- IC5: Studies that include experimental results, analytical evaluation, simulation results, measurement-based evidence, or technically grounded discussion relevant to the research questions.
- IC6: Studies presenting countermeasures (operator/UE/detection/standard).

The inclusion criteria were used to determine the relevance of each study to the scope of the review. Because the reviewed literature is heterogeneous, it was not necessary for each study to meet all inclusion criteria simultaneously. For example, some studies focused primarily on attack mechanisms and empirical evidence, whereas others focused on mitigation solutions or analytical evaluation. However, each included study had to be relevant to the research questions and to the scope of identification or location attacks in 2G–5G cellular networks.

Exclusion criteria:

- EC1: Studies dealing with identification and location without connection to cellular networks.
- EC2: Studies without sufficient technical data.
- EC3: Studies without access to the full content.
- EC4: Studies outside the 2018–2026 timeframe.
- EC5: Studies on non-cellular technologies.
- EC6: Studies published in non-scientific formats.

EC1–EC3 were applied during the title, abstract, and keyword screening stage when they could be assessed from the available bibliographic information. EC4–EC6 were verified during the full-text eligibility assessment, when additional details were required to confirm the temporal scope, the cellular-network focus, and the scientific format of each publication.

Exclusion criteria were used to eliminate records that fell outside the scope of the review or that did not provide sufficient technical relevance. The risk of bias was reduced by defining inclusion and exclusion criteria before the final selection and applying them consistently across all databases.

2.6. Study Selection Process—Adapted PRISMA-like Flow

The study selection process was carried out using an adapted PRISMA-like approach, inspired by the PRISMA guideline, which involves several successive stages commonly referred to as stepwise screening. Thus, we started from a large set of studies and by applying the inclusion criteria, we reached a final set of papers included in this study.

The stages of the selection process, reflected in the adapted PRISMA-like flow diagram and detailed in the methodology, are:

- E1: Identification of studies: records from several academic databases, including IEEE Xplore, ScienceDirect, and SpringerLink, were collected and aggregated into a working database representing the initial set of candidate studies for analysis.
- E2: Identifying and removing duplicates: duplicate records were removed based on predefined criteria (title, authors, year) and the most complete versions were kept, the result being a unique set of records.
- E3: Title, abstract, and keyword screening: only the criteria that could be reliably assessed from the available bibliographic information were applied, namely IC1–IC3 and

EC1–EC3. This step retained records that addressed identification or location attacks in 2G–5G cellular networks, relied on relevant cellular-network vectors, and were published in scientific venues with full-text access available.

- E4: Full-text eligibility assessment: the remaining studies were analyzed by examining their full content and applying the complete set of inclusion and exclusion criteria, namely IC1–IC6 and EC1–EC6. This step verified whether each study provided a clear attack mechanism or vulnerability description, reported experimental results, analytical evaluation, simulation results, measurement-based evidence, or technically grounded discussion, and, where applicable, presented relevant countermeasures. Studies outside the temporal scope, focused on non-cellular technologies, published in non-scientific formats, or providing only general descriptions without sufficient technical detail were excluded.
- E5: Final set of included studies: the studies that satisfied the full-text eligibility assessment formed the final corpus of the review and were subsequently used for data extraction and quality assessment (QA).

The screening process consists of a stepwise filtering procedure and is not a one-step decision. During the screening stage based on the title and abstract, the records were evaluated against the initial inclusion and exclusion criteria, with the aim of eliminating studies that were clearly outside the scope of the review. At this stage, studies were excluded if they did not address cellular networks, if they did not focus on identification and localization, or if they were not relevant to the context of security and privacy in 2G–5G networks. The full-text assessment focused on verifying the extent to which each study presented a relevant identification or localization attack, whether the attack exploited mechanisms or identifiers specific to cellular networks, whether the study provided sufficient technical details, and whether it was relevant to the research questions. The final set of 86 studies was then used for data extraction, quality assessment, and synthesis.

The results of steps E1–E5 are summarized in the selection diagram based on an adapted PRISMA-like process and illustrate the number of records identified, the records excluded during screening, and the final set of included studies, as shown in Table 5:

Table 5. Study selection process results, including the number of records identified, screened, excluded, assessed for eligibility, and included in the final review.

Stage	Number of Articles
Identified records	1055
Duplicates removed	91
Title/abstract screening	964
Excluded articles	831
Full-text articles assessed	133
Studies included in the literature review	86

Appendix A includes Table A1, which lists the 86 studies included in the review and provides the extracted data used to support the transparency, traceability, and reproducibility of the analysis. For each study, the following information was extracted: year of publication, database, attack analyzed, network analyzed, exploited mechanism, adversary model, metrics, countermeasures, and the calculated evaluation score. The metrics and measures were filled in when this information was found in the studies analyzed. If this information was missing, the fields were marked as “Not reported”. The data extracted in the appendix show that the literature focuses on 5G networks; studies targeting 5G networks predominate; and the identified attacks are based on fake base stations, attacks on identity and authentication confidentiality, location tracking attacks, and mobility inference attacks.

Some of the studies examine legacy 2G/3G/4G environments or 4G/5G combinations, which shows that some vulnerabilities are carried over to the new generations and arise at the interoperability level. With regard to the adversary's model, active attacks aimed at manipulating authentication procedures are predominant. In the case of unauthorized tracking of mobile devices, the most commonly used attacks are passive ones that exploit metadata from paging, tracking area updates, and temporary identifiers. The metrics identified in the included studies fall into two categories. Location-oriented metrics such as signaling overhead, paging cost, tracking area update cost, power consumption of user equipment, paging efficiency, and metrics related to detection accuracy, classification, radio fingerprinting indicators, location, or the performance of identification mechanisms. Not all studies report explicit quantitative metrics, and in these cases, the table marks the information as unreported. The countermeasures identified in the 86 studies are divided into measures to protect identity through mechanisms such as pseudonyms, SUCI/SUPI, updating temporary identifiers, and improving authentication procedures. Another direction of countermeasures is the detection methods of fake base stations, based on radio fingerprinting, statistical analysis and classification. Some authors have proposed ideas for optimizing paging, tracking area update and mobility management, with the aim of reducing exposure to tracking and limiting signaling overhead.

The aim of the screening process is to identify a set of high-quality and relevant papers that reflect the current state of research on identification and location attacks in cellular networks. The filtering process based on an adapted PRISMA-like approach eliminated studies that used the same terms (e.g., "location", "tracking"), but investigated different technologies (e.g., GPS, Wi-Fi).

2.7. Data Extraction Diagram

After centralizing all the studies, the next stage consists of the systematic and structured collection of information. For the homogeneity of the process, a standardized data extraction scheme was defined, through which the research questions formulated above can be indirectly answered. The data extracted in this chapter will be used in the following chapters to analyze the evolution of the types of attacks and the technical mechanisms exploited in 2G–5G networks.

The studies were structured into several categories, corresponding to the research objectives and the formulated research questions, as presented in Tables 6–11.

Table 6. Technological background fields extracted from each included study, including cellular generation, architecture, network component, and analyzed scenario.

Field	Description
Network generation	2G/3G/4G/5G
Analyzed architecture	GSM, UMTS, LTE, 5G NSA, 5G SA
Analyzed network component	RAN, Core Network, NAS, RRC

Table 7. Bibliographic information extracted from each included study, including study identifier, authors, year, publication venue, and study type.

Field	Description
ID	Unique identifier of the study
Author(s)	Authors of the paper
Year of publication	Year in which the study was published
Publication type	Journal, conference paper, or book chapter

Table 8. Attack classification fields.

Field	Description
Attack type	Identification/location
Attack category	IMSI catcher, paging attack, tracking attack
Exploited mechanism	Paging, mobility update, measurement reporting, identity request
Attack level	Passive/active

Table 9. Technical vectors exploited.

Field	Description
Exploited identifier	IMSI, TMSI, GUTI, SUPI, SUCI
Exploited procedures	Attach, registration, paging, handover
Exploited radio parameters	Timing advance, RSRP, RSRQ
Used metadata	Cell ID, tracking area

Table 10. Reported results and performance metrics extracted from the included studies, including attack success rate, location-tracking accuracy, execution time, cost, detectability, and reporting limitations.

Field	Description
Attack objective	Identification/location
Attack success rate	If available
Attack limitations	Required conditions for carrying out the attack

Table 11. Countermeasures and protection mechanisms.

Field	Description
Countermeasure type	Standard mechanism/proposed solution
Implementation level	Network/terminal
Reported effectiveness	If evaluated

2.8. Quality Assessment (QA) and Risk of Bias (0–12)

For the qualitative assessment of the studies included in this report, a set of quality criteria inspired by the Kitchenham methodology, adapted to the context of cellular network security, was defined. Thus, an assessment of the degree of confidence in the results of the studies analyzed was made. The questions for assessing the quality of the studies, based on which the clarity of objectives, the rigor of the methodology and the technical contribution were assessed, are:

- QA1. Are the study objectives clearly defined?
- QA2. Is the technological context of the study clearly described?
- QA3. Are the attack model and assumptions clearly described?
- QA4. Is the methodology used described in detail for understanding the study?
- QA5. Are the exploited technical mechanisms identified?
- QA6. Does the study present relevant technical analysis?
- QA7. Are the attack metrics and results present?
- QA8. Are the limits and conditions of the attack discussed?
- QA9. Does the study reveal the impact on user security?
- QA10. Are mitigation mechanisms proposed?
- QA11. Is the research relevant to 2G–5G identification or location attacks?
- QA12. Can the attack be reproduced or understood?

Each evaluation criterion was scored on a scale where 1 indicates full compliance, 0.5 indicates partial compliance and 0 indicates non-compliance. Based on the score obtained, studies can be classified into the following quality categories:

- High (10–12): strong contribution.
- Medium (7–9): useful evidence, but with some limitations.
- Low (4–6): mainly indicative findings.
- Very low (0–3): context only.

The QA framework was applied after the final selection stage to all 86 included studies. The QA score was used to support the interpretation of the evidence base and to identify possible limitations or risk of bias in the included studies. Each study included in the Appendix B was evaluated based on the 12 quality criteria QA1–QA12 as shown in the Table A2. For each study, a score was calculated by summing the scores received for each criterion, with a maximum score of 12 points. The final score was interpreted according to the 4 categories defined previously. For each QA criterion, a three-point scale was used: 1 point if the information is clearly presented, 0.5 points if the information is partially presented, and 0 points if the information is missing. The distribution of studies by quality category is illustrated in the Table A3 and highlights a relevant evidence base for our analysis, as most of the studies fall into the categories High and Medium. The QA score was not used as an automatic exclusion criterion. Therefore, studies with lower QA scores were included when they were relevant to the research questions, but their methodological or reporting limitations were taken into account during the synthesis.

The literature review also aimed to identify potential sources of bias that could influence the results of the literature review. In the field of cellular network security, the main types of bias identified and analyzed are:

- RoB1. Selection bias: analyzing certain technologies in isolation
- RoB2. Methodological bias: the study methodology is not described clearly enough
- RoB3. Experimental bias: experiment difficult to replicate
- RoB4. Reporting bias: positive results of experiments without failures or false positives

RoB qualitative assessment:

- Low: solid method with clear assumptions.
- Moderate: credible results with limitations.
- High: incomplete method with indicative results.

2.9. Synthesis Method

The synthesis approached is narrative and classification-based, and the purpose of this stage is to process and organize the information extracted from the analyzed studies and identify trends, types of attacks, and exploited mechanisms.

The literature synthesis was organized along several axes, including the cellular network generation analyzed, namely 2G, 3G, 4G, and 5G; the type of attack, distinguishing between identification and location attacks; the attack vector, including paging, temporary identifiers such as IMSI, SUPI, SUCI, TMSI, and GUTI, radio parameters, timing advance, handover patterns, and NAS/S1AP control-plane metadata [12]; and the adversary model, classified as passive, semi-passive, or active.

In the literature synthesis, the attacks were classified into two main categories: identity attacks, which reveal the user's identity or correlate temporary identifiers with the subscriber's real identity, and location attacks, which aim to determine the user's geographical position by exploiting information available in the network.

As new generations of mobile networks have emerged, vulnerabilities related to identification and location have also evolved. In 2G GSM networks, these vulnerabilities

were mainly characterized by the direct exposure of the IMSI identifier and by limited security mechanisms. In 3G UMTS networks, they were primarily associated with signaling procedures, while in 4G LTE networks they became more closely related to control-plane vulnerabilities. In 5G networks, the attack vectors are increasingly associated with metadata exposure and mobility procedures [11].

The countermeasures proposed in the literature mainly involve encrypting unique identifiers, deploying mechanisms for detecting fake base stations, improving signaling procedures, and monitoring the behavior of networks or mobile terminals.

The flow followed to facilitate the comparison of the results reported in the reviewed literature consisted of mapping terms according to the proposed taxonomy, grouping studies by category, synthesizing the results, analyzing the evolution of networks, and concluding with a set of deliverables aligned with the research questions. These deliverables included mapping tables covering attack vector, network generation, adversary model, and reported metrics, as well as an attack taxonomy distinguishing between identification and location attacks, passive and active attacks, control-plane and radio-based attacks, and countermeasures implemented at the standard, operator, User Equipment (UE), or detection level.

The heterogeneity of the studies directly influenced the synthesis of the results, consequently this literature review aimed to identify trends and patterns in the literature, without quantitative aggregation, creating a map of 2G–5G identification and location attacks, an impact analysis and a synthesis of research gaps and countermeasures.

3. Technical Fundamentals and Conceptual Framework

To understand identification and location attacks in cellular networks, it is necessary to establish the theoretical framework of the analyzed architectures. This framework supports the evaluation of identity-management vulnerabilities, mitigation solutions, and attacker models. Telecom networks are distributed systems and regardless of the generation, a cellular network is made up of three fundamental blocks: the mobile terminal (UE), the radio access network (RAN) and the core network (CN). These three entities ensure the essential functions of the network: connection, authentication and services. The UE is the user device, such as a smartphone, modem, or IoT device, that contains the radio interface, protocol stack, and SIM or USIM, and its role is to initiate the attach/registration procedures and transmit/receive radio signals. The RAN is the base station that provides the first point of contact between the UE and the network and has the role of managing radio connections. The CN provides the main network functions, including authentication, mobility management, IP address allocation, session management, and service control. Figure 4 presents an overview of the UE–RAN–Core architecture (UE = User Equipment; RAN = Radio Access Network; CN = Core Network.).

From a functional point of view, there are two planes: the control plane that manages network configuration, signaling, and the authentication process and the user plane that actually carries user data [13]. The control plane is particularly exposed to attacks because user identity and mobility information may appear in different signaling procedures. As network architectures have evolved, these components have undergone major transformations, as seen in the evolution of the user identifier, from IMSI to SUPI and SUCI. However, identity protection does not depend exclusively on the encryption of the identifier but also on the implementation of anonymization mechanisms (TMSI, GUTI) in the attach or registration procedures. Attackers' approaches range from passive traffic observation to deploying a fake base station that impersonates a legitimate mobile network operator or exploiting interoperability mechanisms between mobile network generations. An example of an attack that will be analyzed in this study is IMSI Catcher, an attack model

that exploits structural vulnerabilities. The attention of this study is also directed towards the evolution of protection mechanisms such as two-way authentication, anonymization of unique identifiers and encryption of unique identifiers [14].



Figure 4. Simplified UE–RAN–Core architecture of a cellular network and separation between the control plane and the user plane.

3.1. Cellular Network Architecture (2G–5G)

The architecture of cellular networks, from 2G to 5G, has undergone major transformations, with each generation introducing structural changes in the RAN and CN that also affect identity and mobility management. It is important to understand these architectural differences for analyzing the attack surface on identity and location.

3.1.1. 2G/GSM Architecture

The architecture of 2G networks is circuit-switched and provides voice and data services. 2G networks use one-way authentication, meaning that the network does not authenticate itself to the mobile terminal. The IMSI is transmitted in the clear, encryption is activated after authentication, and the MSC infrastructure contains the two control and user planes. These elements allow direct attacks to impersonate mobile operator stations, IMSI capture, and downgrade attacks to weak encryption.

As shown in Figure 5, the main components are the Mobile Station (MS), which includes the terminal and SIM card; the Base Transceiver Station (BTS), which transmits and receives radio signals; the Base Station Controller (BSC), which manages radio resources and handover; the Mobile Switching Center (MSC), which manages call switching and mobility; the Home Location Register (HLR), which stores subscriber data; and the Authentication Center (AuC), which generates authentication vectors.

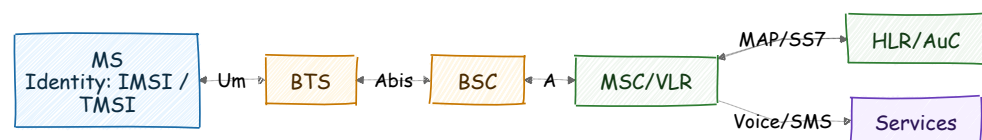


Figure 5. Simplified architecture of a 2G/GSM network and the main entities involved in identification, authentication and service provision.

3.1.2. 3G/UMTS Architecture

The architecture of 3G networks is a mixed type (circuit-switched + packet-switched) and introduces for the first time bidirectional authentication and more robust cryptographic protection. The mechanism used in the authentication process is AKA (Authentication and Key Agreement) which ensures mutual authentication. The user's identity is protected by the use of the temporary pseudonym TMSI, and voice traffic is separated from data traffic. 3G networks maintain interoperability with GSM, which offers the possibility of downgrade.

As shown in Figure 6, the main components are the User Equipment (UE), Node B, Radio Network Controller (RNC), and Core Network (CN), which is divided into the CS and PS domains.

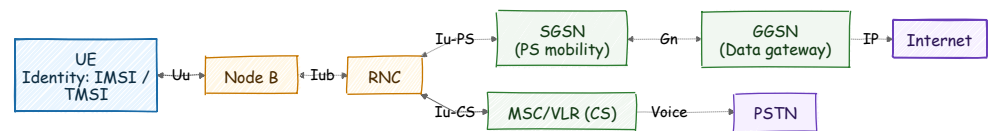


Figure 6. A simplified architecture of a 3G/UMTS network and the separation between the CS domain and the PS domain.

3.1.3. 4G/LTE Architecture

The architecture of 4G networks is a distributed IP-based one and introduces the temporary identifier GUTI, which is used instead of the IMSI, and the user plane (data) is separated from the control plane (NAS and RRC signaling). Mechanisms such as paging and GUTI reuse can provide strong signals for correlation and location attacks [15].

As shown in Figure 7, the main components are: User Equipment (UE), eNodeB (Evolved Node B), Evolved Packet Core (EPC). The EPC includes the MME, which handles mobility management and NAS signaling; the SGW, which anchors the user plane; the PGW, which provides connectivity to external packet data networks; and the HSS, which stores subscriber data (eNodeB = Evolved Node B; EPC = Evolved Packet Core; MME = Mobility Management Entity; NAS = Non-Access Stratum; SGW = Serving Gateway; PGW = Packet Data Network Gateway; HSS = Home Subscriber Server.).

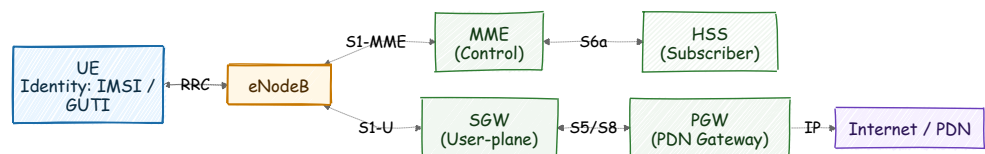


Figure 7. A simplified architecture of a 4G/LTE network and the separation between the control plane and the user plane.

3.1.4. 5G Architecture

5G introduces a service-based architecture, representing a major transformation in the world of cellular networks as network functions have been virtualized, the control plane and user plane have been completely separated and offer support for network slicing. Another innovative feature introduced by 5G networks is user identity protection via the SUCI mechanism, which encrypts the SUPI using a public key [16]. Interoperability with 4G networks and the maintenance of fallback introduce indirect vulnerabilities into 5G networks through legacy systems. 5G networks have two architectural implementations: Non-Standalone (NSA) and Standalone (SA) [17].

5G NSA and 5G SA differ in terms of identity management, mobility procedures, and privacy risks. In 5G NSA, 5G New Radio (NR) is introduced while several control-plane and mobility-management functions remain anchored in LTE/EPC. For this reason, certain vulnerabilities related to identification and location are inherited from LTE/EPC. 5G SA networks use the 5G Core and native 5G mechanisms for identity management. In this case, SUPI represents the subscriber's permanent identity, SUCI represents the encrypted form of SUPI transmitted over the radio interface, and 5G-GUTI is used as a temporary identifier for mobility and paging. Table 12 summarizes the main architectural and security-relevant differences between 5G NSA and 5G SA, with particular emphasis on identity handling, LTE/EPC dependence, 5G Core mechanisms, privacy risks, and mitigation focus.

Table 12. Architectural and security-relevant comparison between 5G NSA and 5G SA.

Characteristic	5G NSA	5G SA
Architecture and core network	Non-standalone deployment using 5G New Radio (NR) with an LTE/EPC anchor.	Standalone deployment using 5G New Radio (NR) with the 5G Core.
Subscriber identity handling	May inherit LTE/EPC identity handling, relying on IMSI, GUTI, and S-TMSI depending on the procedure and fallback scenario.	Uses SUPI as the permanent identity, SUCI as its concealed form, and 5G-GUTI as the temporary identity.
Control and mobility management	Control-plane and mobility procedures are largely LTE/EPC-dependent, commonly involving the eNodeB and MME.	Control-plane and mobility procedures are 5G-native, involving the gNodeB and AMF.
Main privacy risks	LTE anchor exposure, GUTI/S-TMSI linkability, LTE paging correlation, rogue eNodeB scenarios, and fallback/interworking risks.	5G-GUTI linkability, paging-based presence inference, SUCI/SUPI misconfiguration, and implementation-specific weaknesses.
Mitigation focus	Frequent GUTI refresh, LTE paging hardening, rogue-cell detection, secure interworking, and restriction of insecure fallback.	Correct SUCI configuration, frequent 5G-GUTI rotation, AMF policy enforcement, privacy-preserving paging, and conformance testing.

The distinction between 5G NSA and 5G SA provides a clearer understanding of how privacy risks evolve in 5G deployments. In 5G NSA, many vulnerabilities stem from reliance on LTE/EPC rather than from 5G NR itself. These vulnerabilities include GUTI/S-TMSI linkability, LTE paging correlation, spoofed eNodeB scenarios, and interactions with legacy radio technologies. In 5G SA networks, the attack surface is mainly related to 5G Core procedures for identity and mobility management, including SUPI protection through SUCI, 5G-GUTI assignment and rotation, AMF policies, registration behavior, and paging configuration.

As shown in Figure 8, the 5G SA architecture includes the gNodeB, which manages radio resources, and the 5G Core, which includes functions such as the AMF, SMF, UPF, UDM, and AUSF (gNodeB = next-generation Node B; 5GC = 5G Core; AMF = Access and Mobility Management Function; SMF = Session Management Function; PDU = Protocol Data Unit; UPF = User Plane Function; UDM = Unified Data Management; AUSF = Authentication Server Function.).

As shown in Figure 9, the 5G NSA architecture includes the UE, which supports both LTE and 5G NR through dual connectivity; the eNB, which acts as the LTE Master Node and anchors the LTE control plane; the gNB, which provides 5G NR radio resources; and the EPC, which remains responsible for mobility, authentication, and traffic routing (5G NR = 5G New Radio; eNB = evolved Node B; gNB = next-generation Node B.).

The attack surface has evolved with cellular architectures. 2G networks offer a simple architecture that exposes the identity of mobile terminals, 3G networks introduce two-way authentication, 4G networks use an IP-based architecture and separate the control plane from the user plane, and 5G networks introduce service-based architecture, virtualization, and identity encryption. A recurring issue across mobile network generations is interoperability, which can enable downgrade attacks [18]. Figure 10 illustrates the attack surface across cellular network generations from 2G to 5G.

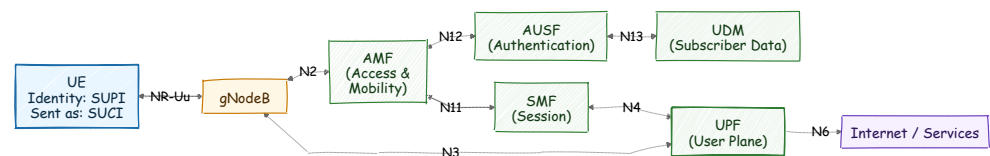


Figure 8. The simplified architecture of a 5G SA network and the main identity management mechanisms using SUPI/SUCI.

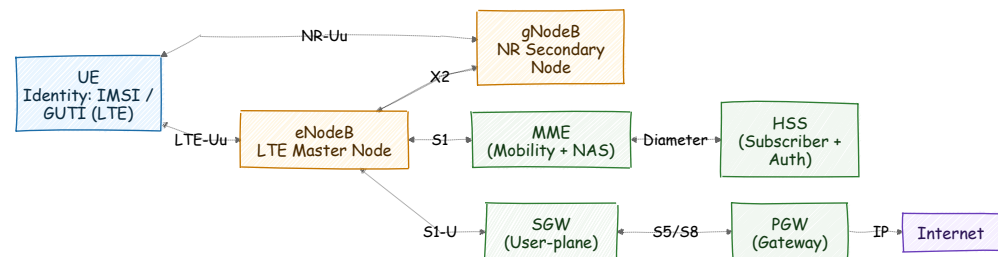


Figure 9. The simplified architecture of a 5G NSA network and its reliance on LTE/EPC infrastructure.

Causes of Identity and Location Attacks (2G-5G)

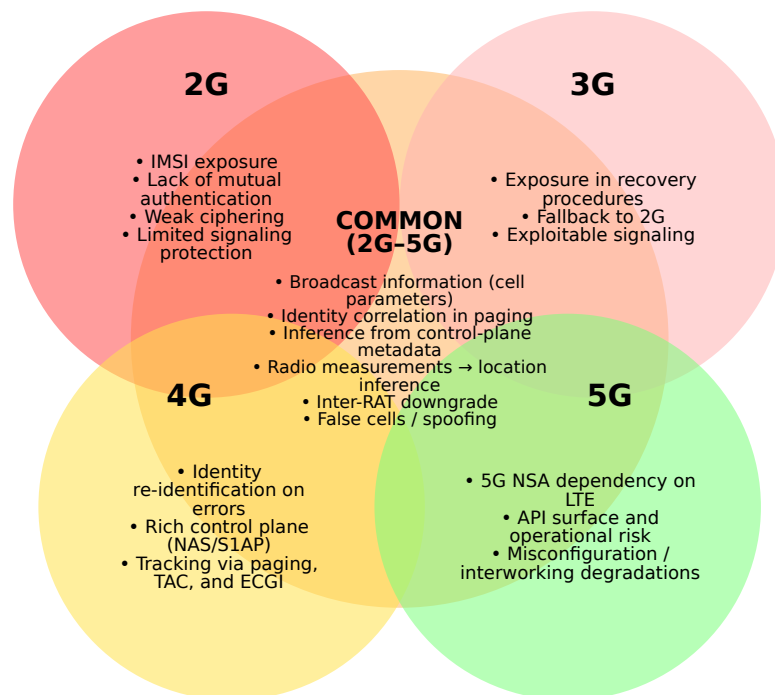


Figure 10. The attack surface for identification and location in 2G–5G networks, highlighting the vulnerabilities specific to each generation and the attack mechanisms common across generations.

3.2. Identification Mechanisms in Cellular Networks (IMSI, TMSI, GUTI, SUCI)

User identification has become a key concern across generations. In cellular networks, each user has a unique identifier that they use to connect to the network. This identifier, which may be permanent or temporary, is the basis for authentication, service provision, and location tracking [10]. A user's activity is associated with their profile through this identifier, which maintains the continuity of services. The exposure of these identifiers creates security risks that may enable the identification and location tracking of mobile terminals. In this context, mobile networks have evolved from transmitting the identifier in the clear, to using pseudonyms [19].

The IMSI is the permanent subscriber identifier. It is stored in the SIM and in the operator's HLR database and is used during network authentication. The IMSI consists of the Mobile Country Code (MCC), Mobile Network Code (MNC), and Mobile Subscription Identification Number (MSIN). In 2G networks when the user connects to the network for the first time, the IMSI is transmitted in the clear, which allowed the development of IMSI catcher attacks. Later generations introduced temporary identifiers as a response to this vulnerability [20,21].

In 2G–4G, the permanent subscriber identity is *IMSI*, while in 5G it is *SUPI*, as shown in Table 13. To limit over-the-air exposure, 5G introduces *SUCI*. Temporary identifiers (TMSI/P-TMSI in 2G/3G, GUTI in 4G/5G) are used in current signaling and should be refreshed periodically to prevent long-term correlation.

Table 13. Permanent vs. temporary identifiers across generations.

Generation	Permanent Identifier	Temporary Identifier	Over-the-Air Identifier
2G (GSM)	IMSI	TMSI	TMSI
3G (UMTS)	IMSI	P-TMSI	P-TMSI
4G (LTE)	IMSI	GUTI	GUTI [22]
5G (NR)	SUPI	5G-GUTI	SUCI, 5G-GUTI [23]

TMSI is the identity anonymization mechanism introduced in GSM and UMTS networks, it is assigned to the subscriber by the operator after the initial authentication takes place and is used instead of IMSI in most signaling mechanisms, having a limited duration of use and is only valid in certain location areas. The TMSI does not have a fixed structure; it is a temporary 32-bit (4-byte) identifier generated by the network (VLR or MME) and is unique to a specific area (LA). In practice, the TMSI alone is not sufficient to identify the network subscriber and is used in conjunction with the LAI (MCC | MNC | LAC). Even under these conditions, correlating the TMSI with other signaling information can enable user tracking [24].

GUTI was introduced in LTE networks to replace the use of IMSI in signaling mechanisms. This identifier consists of MCC, MNC, MME ID, MME code and M-TMSI. Although this identifier allows for quick identification of the subscriber, studies show that in practice the reuse of GUTI and its correlation with paging messages can lead to the identification and location of the subscriber (IMSI = International Mobile Subscriber Identity; TMSI = Temporary Mobile Subscriber Identity; SUCI = Subscription Concealed Identifier; MCC = Mobile Country Code; MNC = Mobile Network Code; MSIN = Mobile Subscription Identification Number; LAC = Location Area Code; MME = Mobility Management Entity.).

SUPI and SUCI (encrypted SUPI) have been introduced in 5G networks as a new identification mechanism based on asymmetric encryption. The concept used in 5G is that when the user connects to the operator, they generate SUCI using the network's public key, thus, the subscriber's identity is no longer disclosed [25,26]. Another advantage is that the SUCI is generated on every access procedure, a property that prevents session correlation. However, paging procedures, mobility updates, and control plane metadata can allow inferences regarding the presence or location of the user in a particular area [27].

3.3. Location Mechanisms in Cellular Networks

Cellular networks provide connectivity to users whether they are stationary or on the move. The movement of mobile terminals implies the need for their permanent location to ensure uninterrupted services. To maintain updated information on the area where mobile terminals are located, a series of signaling procedures and mobility management mechanisms are used, which, although their main purpose is the proper functioning of networks, generate metadata that can be exploited for the location of mobile terminals.

In the literature, this information is referred to as location vectors [28]. In the context of location attacks, the mechanisms used can be analyzed from two perspectives: signaling and mobility procedures, which are used by the network to obtain information about the terminal's position, and location inference vectors, which include radio parameters or metadata that allow position estimation.

Signaling procedures used in locating mobile terminals: attach, registration, mobility updates, handover, measurement reporting, paging.

The attach and registration procedures provide the first opportunity to determine the position of a mobile terminal, which at the time of connection with the base station transmits its identifier (IMSI, TMSI, GUTI or SUCI) [29], and the network can identify the cell to which the mobile terminal has connected and, thus, estimate its position. This procedure has different names depending on the generation, as shown in Table 14.

Table 14. Attach and registration procedures.

Generation	Procedure
2G	Location Update
3G	Location Area Update/Routing Area Update
4G	Attach [30]
5G	Registration [31]

Mobility update procedures occur when a mobile terminal moves into a different mobility zone defined by the network. In practice, when the mobile terminal enters a different mobility zone, it sends an update message to the network so that the network knows the approximate zone in which the terminal is located; this ensures that when a call is initiated, the search area for the mobile terminal is minimized [32]. Table 15 summarizes the main mobility update procedures across cellular technologies.

Table 15. Mobility procedures.

Technology	Procedure
GSM	Location Area Update (LAU)
UMTS	Routing Area Update (RAU)
LTE	Tracking Area Update (TAU) [33]
5G	Registration Update/Mobility Registration Update [7]

The paging procedure is initiated by the network when a mobile terminal is in an inactive state (idle mode), a situation in which the network only knows the mobility area in which the terminal is located, not the cell, and to establish a new connection, the network transmits a paging message to all cells in the mobility area in which the mobile terminal is known to be located. Mobile terminals continuously monitor paging messages and respond when they receive a message addressed to them. This mechanism for scanning paging messages can indicate a user's presence in a specific geographic area [34]. Table 16 summarizes the paging procedures used across cellular technologies.

Table 16. Paging procedures across technologies.

Technology	Procedure
GSM	Paging Request
UMTS	Paging
LTE	Paging Message [15]
5G	Paging [7]

The handover procedure handles the process of transferring a mobile terminal's connection from one cell to another as the terminal moves. This procedure is initiated by

the network when the signal level from the current cell drops or the neighboring cell offers better signal quality [35]. The main goal is to maintain the continuity of mobile services and avoid connection interruptions. This process is controlled by the network, which periodically receives radio measurements of the cells in the area of the mobile terminal, and based on these measurements the network determines whether or not to transfer to another cell [36]. There are several types of handover:

- Intra-cell handover: connection transfer within the same cell (between different radio channels)
- Inter-cell handover: the connection is transferred between two different base stations
- Inter-RAT handover: the connection is transferred between different radio technologies (LTE to 3G)

All generations of cellular networks offer the handover procedure, but the mechanism and terminology differ, as shown in Table 17.

Table 17. Handover mechanisms by cellular generation.

Generation	Mechanism
2G (GSM)	Handover controlled by the BSC
3G (UMTS)	Soft handover managed by the RNC
4G (LTE)	X2 handover/S1 handover [37]
5G (NR)	NG handover [38]

Mobile terminals periodically provide radio reports containing essential data in optimizing the connection such as: detected neighboring cells, signal level and signal quality. The disadvantage of this procedure occurs in a succession of handovers that can provide information about the user's movement and direction, since each connection transfer indicates the change of cell associated with the mobile terminal, which can be observed by an attacker [38].

The location vectors generated by cellular networks and used for location are: Cell-ID, power parameters, Timing Advance, signal quality parameters, system information and neighboring cells. The identity of the cell to which a mobile terminal is connected can estimate the user's position within the cell's coverage area [39,40]. Timing Advance determines the propagation time of the radio signal from the terminal to the base station. The signal strength and quality parameters (RSRP and RSRQ) can be used in estimating the terminal position by triangulation or signal analysis. The information in the SIB is also used in reconstructing the cell structure and identifying the position. By combining the mechanisms described above, attackers may estimate the position of a mobile terminal within a given geographical area.

3.4. Attacker Model

To understand identification and location attacks, it is necessary to define the attacker models used to assess vulnerabilities and the capabilities required to access signaling information or interact with network procedures [41]. In the context of telecommunications, attacks can be classified according to their ability to generate traffic, intercept traffic and interact with the system as follows: passive, semi-passive and active attacker. Passive attackers can monitor traffic without directly interacting with mobile terminals or operator infrastructure. Semi-passive attackers analyze paging messages, temporary identifiers, radio parameters, signaling metadata and by correlating them can deduce the presence of a user in a certain area. Semi-passive attackers can generate certain types of traffic or trigger signaling procedures such as paging (calls, SMS messages, or data traffic to the location vector) [42,43]. Active attacks are the most powerful and consist of transmitting

radio signals and simulating the behavior of a base station. In this way, the attacker can request the identity of mobile terminals, manipulate authentication procedures and force mobile terminals to connect to a specific cell. The main capabilities of attackers identified in the literature are interception of radio traffic, signaling message analysis, controlled traffic generation and operating a fake base station.

Attacks can be differentiated based on network interaction and required resources (MIB = Master Information Block; SIB = System Information Block; RNTI = Radio Network Temporary Identifier; TMSI = Temporary Mobile Subscriber Identity; RSRP = Reference Signal Received Power; RSRQ = Reference Signal Received Quality; OAI = OpenAirInterface; srsRAN = open-source software radio access network suite.). Passive attacks rely on sniffing broadcast or control-plane information using SDR equipment and antennas, and may involve decoding MIB/SIB messages, capturing paging messages, tracking temporary identifiers such as RNTI, TMSI, or GUTI, measuring RSRP/RSRQ values, and exploiting timing advance information [44]. Semi-passive attacks extend passive capabilities by inducing specific triggers, such as short calls, instant messages, or VoLTE events, in order to correlate the triggered event with paging activity. Active attacks, including fake BTS, eNB, or gNB scenarios and downgrade attacks, require SDR equipment together with a radio access network stack such as OAI or srsRAN to emulate a fake base station [45], manipulate cell selection or handover procedures, issue Identity Request messages, or force downgrade scenarios.

The outcomes also differ according to the attack type. Passive attacks can enable location inference without direct interaction with the UE, mainly by confirming the presence of a mobile device within the coverage area of a cell. Semi-passive attacks can reduce the search space by correlating induced events with observable paging behavior, while active attacks can lead to direct identity exposure, including IMSI disclosure.

3.5. IMSI Catcher Concept

An IMSI catcher is a system that imitates the behavior of a base station and impersonates the infrastructure of a mobile network operator, with the aim of connecting nearby phones to a fake BTS. In the literature, such systems are referred to as rogue base stations [46], fake base stations, or cell-site simulators and it exploits the way in which phones select and connect to an operator's cell. The mobile terminal chooses the most attractive cell (best signal) and if the authentication mechanism is weak and this step is skipped, the attacker can initiate various procedures for the phone to reveal its permanent (IMSI) or temporary (TMSI, GUTI) identity. An IMSI Catcher can also be used to locate mobile terminals by observing the signal level or the moment the mobile terminal responds to paging. The authentication mechanisms used in cellular networks directly influence the success rate of an IMSI catcher [22].

In GSM networks, it is easy to impersonate a base station because authentication is unidirectional as shown in Figure 11.

Although a bidirectional authentication mechanism has been introduced in LTE networks, compatibility with GSM technology maintains the possibility of IMSI catcher attacks as shown in Figure 12.

Even in 5G NSA networks, although the SUCI mechanism no longer exposes identity in the clear, interoperability with LTE infrastructure maintains certain attack surfaces as shown in Figure 13.

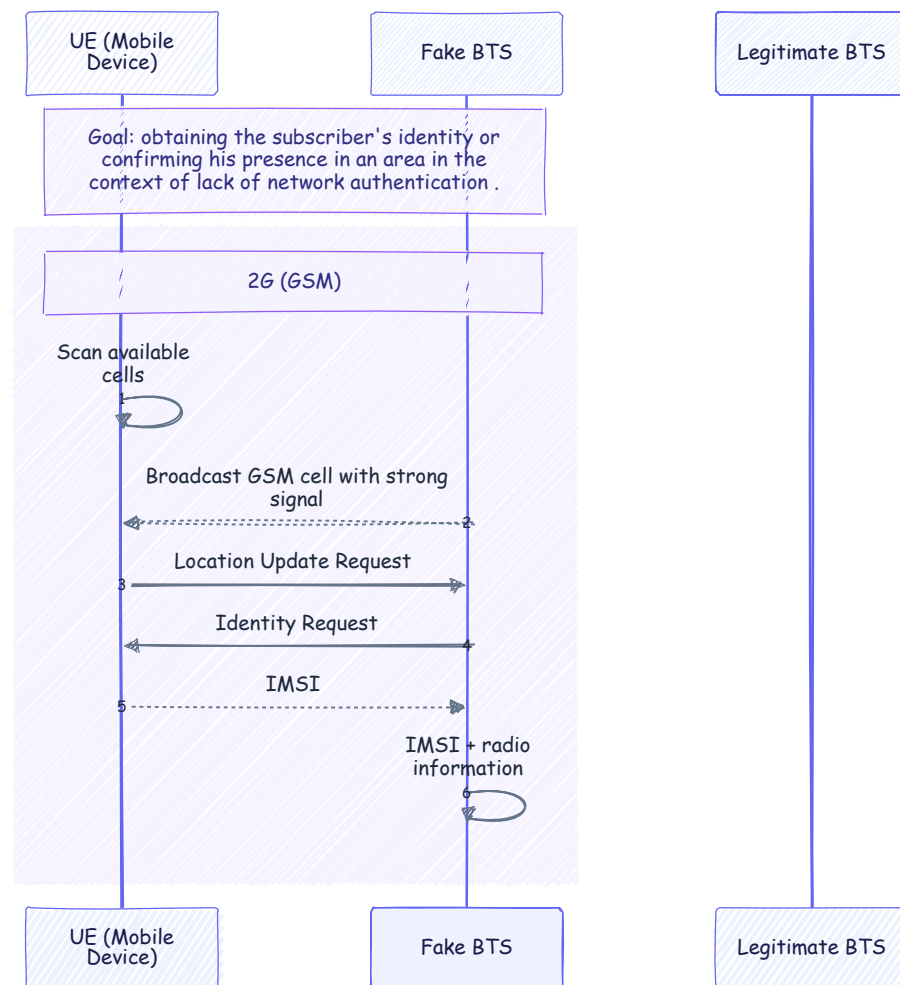


Figure 11. Simplified sequence of a 2G/GSM BTS spoofing attack to obtain a subscriber's identity or confirm their presence in an area.

Understanding the concept of IMSI catcher is essential for identifying existing vulnerabilities in radio access mechanisms in cellular networks, and these vulnerabilities can be exploited in identification and location attacks in cellular networks from 2G to 5G.

3.6. Evolution of Protection Mechanisms (2G to 5G)

As vulnerabilities in cellular networks have been identified and their complexity has increased, new security mechanisms have been developed such as subscriber identity protection, two-way authentication (user and network), delimiting the control plane from the user plane, integrity protection for multiple message types. 2G networks introduced user authentication using the A3 and A8 algorithms, and radio traffic was encrypted using the A5 algorithm. Although these mechanisms provide a level of protection for communications, GSM networks have a limitation given by unilateral authentication. Only the network authenticates the mobile terminals, not vice versa. 3G networks introduced the AKA protocol that implements bilateral authentication between the terminal and the network, which allows mobile terminals to detect attempts to impersonate mobile operator base stations. 4G networks introduced a separation between user plane and control plane, the AKA protocol was retained [31], but the identity management mechanisms were improved by using temporary identifiers GUTI or S-TMSI assigned by the network. Radio communication is also protected by stronger encryption algorithms. 5G networks introduce the concept of SUCI and SUPI. SUPI represents the permanent identity of the user, which is

not transmitted in the clear on the network, but is encrypted using the operator's public key, resulting in SUCI [47,48].

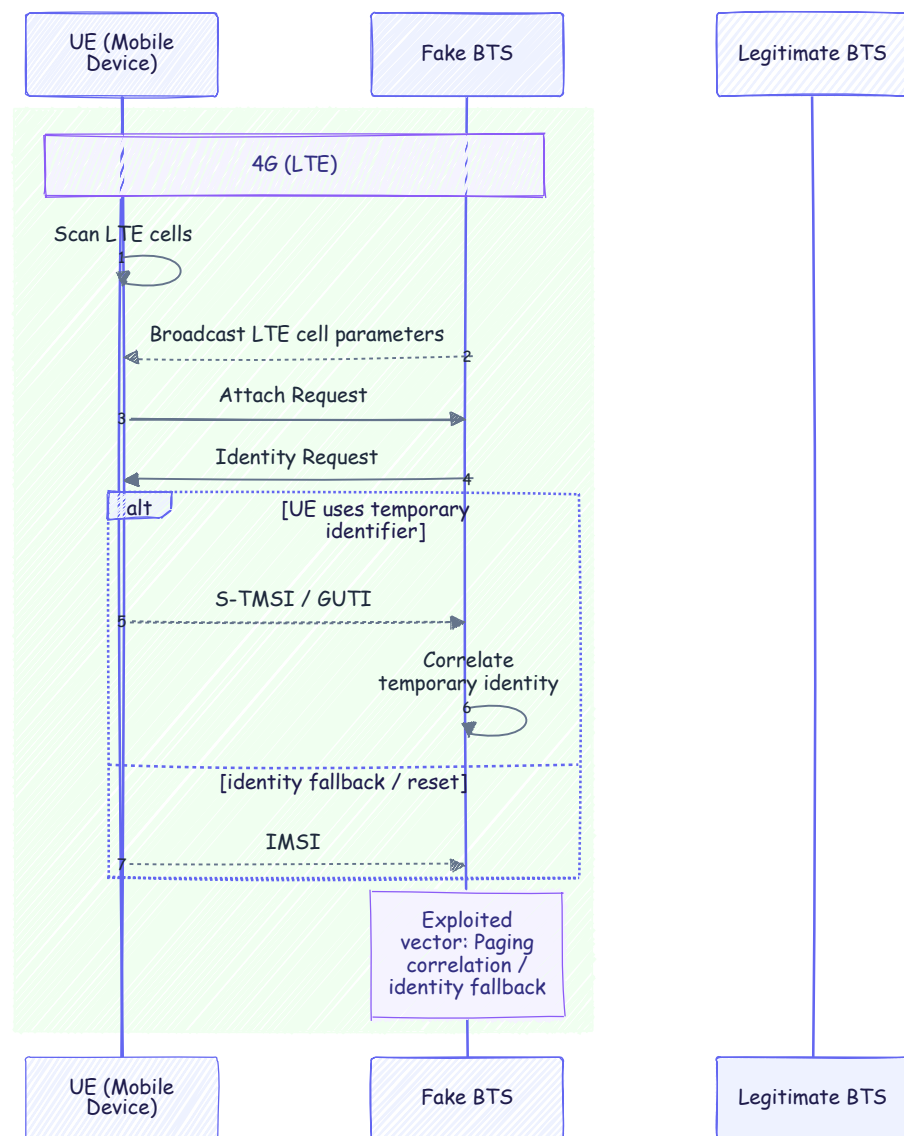


Figure 12. Simplified sequence of an identity attack in 4G/LTE, highlighting the use of temporary S-TMSI/GUTI identifiers, the possibility of correlating them, and the exposure of the IMSI in fallback or identity reset scenarios.

However, compatibility with GSM networks, interoperability between generations, and the use of hybrid operating modes maintain certain attack surfaces common to all generations. The evolution of encryption algorithms by generation is illustrated in Table 18.

Table 18. Cryptographic algorithms used in cellular networks and qualified security status.

Algorithm	Generation	Qualified Security Status	References
A5/1	2G	Legacy cipher; practically broken.	[5,48]
A5/2	2G	Legacy weakened cipher; broken.	[5,48]
COMP128-1	2G	Legacy authentication algorithm; vulnerable.	[5,48]
KASUMI	3G	Standardized, but affected by academic cryptanalysis.	[48]
SNOW 3G	3G/4G	Standardized; no practical break reported in reviewed studies.	[48]
AES	4G/5G	Standardized; security depends on mode, key length, and implementation.	[48]
ZUC	4G/5G	Standardized; no practical break reported in reviewed studies.	[48]

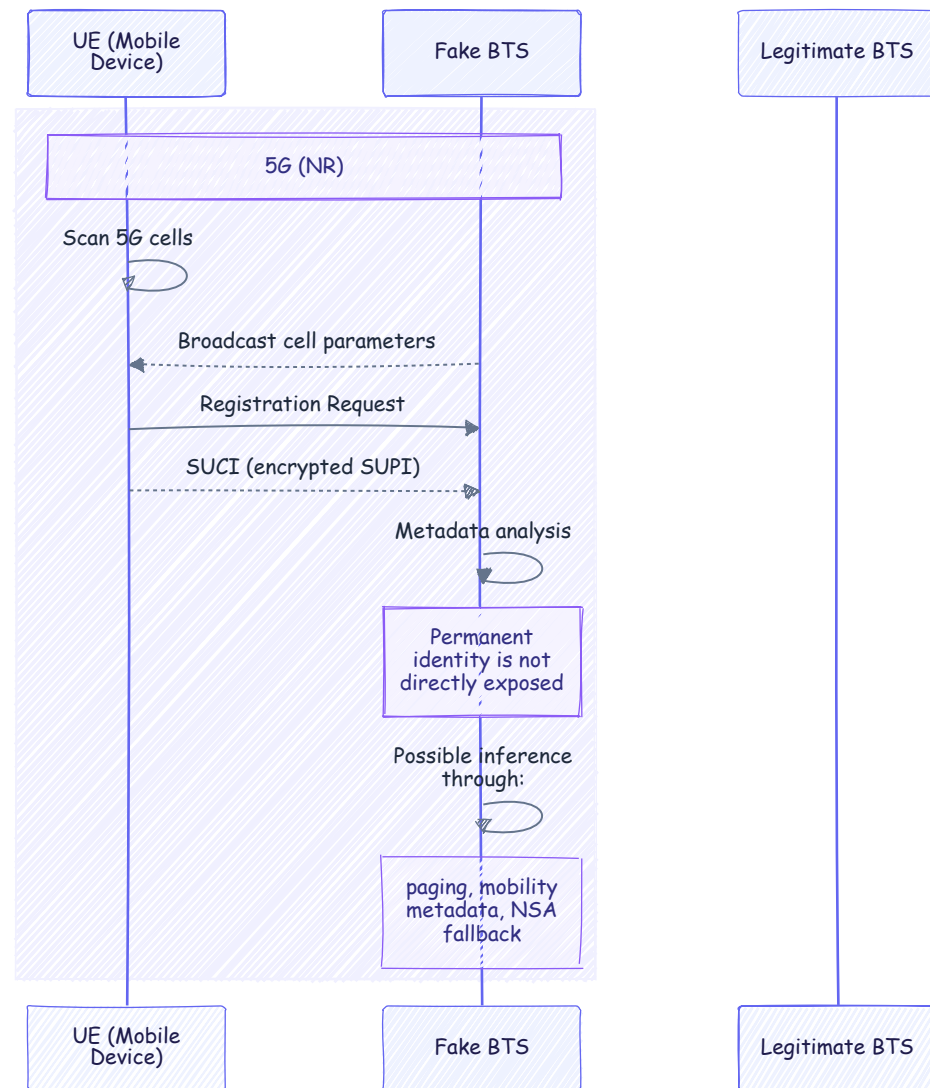


Figure 13. Simplified sequence of an identity attack in 5G/NR, where the permanent identity is not directly exposed, but there may be risks of inference through paging, metadata, and NSA fallback.

4. Review Results

The analysis of the 86 included studies revealed two main research directions. The first direction concerns attacks on radio infrastructure and the use of fake base stations. In the literature, these systems are also referred to as rogue base stations or cell-site simulators. These attacks can be easily demonstrated experimentally in laboratories. The second direction identified in the literature is the protection of subscriber identity in the authentication process. Researchers pay increased attention to permanent and temporary identifiers that are exposed in mobile network protocols. IMSI/SUPI exposure, SUCI protection, and 5G-AKA-associated vulnerabilities are topics addressed in the included studies [23].

4.1. Distribution of Studies

As part of this literature review, the included studies were categorized according to several criteria: publication type, year of publication, field, and type of attack. The collection of studies includes both conference papers and journal articles, though there is a slight predominance of conference papers. The distribution of included studies shows that conference papers represent the majority, with 49 studies (57.0%), while journal articles total 37 studies (43.0%). In terms of the topics covered, most studies focus on attacks

based on rogue base stations [49] and the confidentiality of mobile device identities and authentication. There are also papers dedicated to the location and protection of subscriber metadata. Table 19 presents the distribution of the included studies by thematic domain.

Table 19. Distribution of included studies by thematic domain.

Thematic Domain	Number of Studies	Percentage
Fake base stations	28	32.6%
Authentication privacy	27	31.4%
Location tracking	12	14.0%
Cellular privacy	10	11.6%
Protocol and signalling security	6	7.0%
Reviews	2	2.3%
Paging and mobility management	1	1.2%

In terms of attack type, the studies included in this literature review cover all three types of attacks (passive, semi-passive, and active attacks), the most popular being semi-passive and active attacks, as shown in Table 20.

Table 20. Distribution of included studies by attack type.

Attack Type	Number of Studies	Percentage
Semi-passive	37	43.0%
Active	32	37.2%
Passive	17	19.8%

The distribution of studies by publication year shows a growing research interest during the 2018–2025 period. Although the increase is not perfectly linear, the trend suggests that the topic is not a marginal one and that interest in it has grown alongside the evolution of mobile networks, with researchers focusing their attention particularly on rogue/fake base stations, identity and authentication privacy, location tracking and inference.

4.2. Taxonomy of Identification and Location Attacks

Based on the studies included in this article, identification attacks in 2G–5G networks can be classified according to the capabilities of the adversary, the technical mechanism exploited, the operational result of the attack, the targeted identifier, and the network generation.

To fully capture the differences between generations of cellular networks, the overview was expanded to include a cross-generational comparative perspective covering 2G, 3G, 4G, 5G NSA, and 5G SA. Appendix B, through Table A4, provides a comparative analysis of attacks based on the attack vector, the affected identifier, the exploited procedure, the adversary's capabilities, the reported metrics, the limitations, the mitigation measures, and representative studies.

4.2.1. Classification by Adversary's Capabilities

Passive attacks consist of observing broadcast, paging, and signaling traffic without changing the network state or modifying packets exchanged between the network and the mobile terminal. By simply observing the control plane and metadata, the presence of a user can be determined, his re-identification or the correlation of sessions. The advantage of this type of attack would be high stealth, and the limitations would be the dependence on accessibility to radio channels and communication encryption [50].

Semi-passive attacks can indirectly influence the behavior of the network or subscribers by triggering procedures. The adversary can trigger events (call/SMS/push) without transmitting as a base station. Studies show that paging, tracking area update or mobility

management mechanisms can be used in identification and location attacks. The limitation of this type of attack would be the need for a triggering and correlation channel.

Active attacks interact directly with the network infrastructure (injection/manipulation). In the literature, a scenario has been identified in which a fake base station impersonates the network and may request the permanent subscriber identity or force fallback and downgrade procedures. The limitations of this attack would be complex hardware requirements and detectability.

4.2.2. Classification by the Exploited Technical Mechanism

Identification attacks can be classified according to the technical mechanism exploited, including attacks based on the correlation of permanent and temporary identifiers, such as IMSI, SUPI, SUCI, and TMSI; attacks based on authentication and access procedures, including fallback between generations, attach or registration procedures, and authentication procedures; attacks based on malicious radio infrastructure, such as fake base stations, fake eNodeB/gNodeB scenarios, and other forms of emulated radio infrastructure [30]; signaling- and metadata-based attacks that exploit control-plane metadata and particularities of NAS/RRC procedures [51]; and attacks based on paging, mobility, and location-management mechanisms, which reduce the search space and correlate terminal behavior with a specific subscriber.

4.2.3. Classification by Operational Result of the Attack

Depending on the outcome of the attack and its effects, the identification attacks reported in the literature can be grouped into direct identification attacks, in which the subscriber's identity, such as IMSI or SUPI, is revealed; re-identification attacks, which correlate multiple sessions or repeated occurrences [52]; presence-confirmation attacks, which determine whether a particular user is located in a specific area; and identity–location correlation attacks, which link the subscriber's identity to a position.

4.2.4. Classification by Target Identifier

Another criterion used in classifying attacks is the targeted identifier:

- Permanent identifiers: SUPI (5G), IMSI (2G–4G)
- Temporary identifiers: 5G-GUTI (5G), TMSI (2G), GUTI/S-TMSI (4G)
- Protected identifiers: SUCI (5G)

4.2.5. Classification by Network Generation

The effectiveness of identification attacks also depends on the cellular network generation in which they are implemented. In 2G GSM networks, IMSI catcher attacks are facilitated by the lack of network authentication and weaker encryption mechanisms. In 3G UMTS networks, mutual authentication improves security, although exposure scenarios may still occur through specific procedures and paging mechanisms. In 4G LTE networks, temporary identifiers are used to reduce direct identity exposure, but paging and control-plane metadata remain relevant attack vectors. In 5G NR networks, the main risks are increasingly associated with metadata exposure and interoperability mechanisms.

The analysis of the research included in this study shows that identification attacks in cellular networks are not limited to a single technology, but are the result of multiple factors such as network design, signaling mechanisms, and adversary capabilities. The researchers' attention is directed towards identity protection in authentication procedures and the exploitation of fake base stations as a tool for identification and tracking. Although technologies have evolved, privacy issues related to user identification persist, often being transferred or transformed depending on the new technologies introduced [53].

4.3. Experimental Techniques Used in Studies

Following the analysis of the studies included in this literature review, identification and location attacks prove to be an interdisciplinary field and are based on several experimental techniques, being exemplified by laboratory experiments, simulation of radio infrastructures, machine learning techniques and signaling analysis, practical evaluation of active attacks, location and re-identification based on metadata [54].

4.3.1. LTE/5G Radio Infrastructure Emulation

The authors reproduce attack scenarios in isolated environments such as fake base stations, fake eNodeB/gNodeB scenarios, IMSI catcher attacks, and downgrade attacks [55]. These attacks consist of emulating a radio infrastructure and analyzing the behavior of the mobile terminal to observe whether the subscriber retransmits a permanent identifier, accepts a fake base station or accepts the transition to a more vulnerable technology [56].

4.3.2. Measurements in Real-World Networks

This approach moves the focus from theory to practice, with measurements taken in real commercial networks, resulting in captures of control traffic, signaling metadata, and differences in operators' network configurations. The studies examine the presence of IMSI catchers in the field, paging behavior, identification risks, and investigate the security of attachment procedures [57].

4.3.3. Signal Analysis

This technique demonstrates that identification can also be achieved through metadata correlation, without knowing the permanent identifier explicitly. The experimental method consists of modeling and correlating message sequences (paging, signaling) between the terminal and the network to reduce the difficulty of locating and identifying the subscriber [58].

4.3.4. Simulation of Mobility and Paging Scenarios

Many studies use mathematical models and optimization algorithms to show how architectural tradeoffs in a network can influence the attack surface. Techniques identified in the literature use clustering algorithms or performance models for location management.

4.3.5. RF Fingerprinting and Machine Learning

Some of the studies analyzed use RF fingerprinting to detect fake base stations, and the methodology followed consists of collecting radio signals, extracting features and comparing them [59]. Studies show an increasing interest in automated detection techniques, such that the detection of network anomalies and rogue base stations is also achieved by using machine learning algorithms or data-driven methods. These studies aim at recognizing malicious patterns, real-time detection of illegitimate behaviors with the aim of building automated detection mechanisms [60].

4.3.6. Cryptographic Evaluation

There are studies that propose new authentication schemes, identity anonymization mechanisms, or solutions based on post-quantum cryptography [61], which shows that protection against identification attacks is also addressed at the protocol level, not just at the operational or radio level. The authors propose new authentication protocols that are analyzed from a security point of view and compare them with those existing in operator implementations, including in terms of implementation cost [62].

5. Analysis and Discussions

5.1. Answers to RQs

The answers to the research questions formulated above were built based on data extracted from the included studies and provide an overview of identification and location attacks in 2G–5G networks.

RQ1. The attacks documented in the literature can be classified according to the mechanisms exploited and the operational objectives. The main types of identification attacks are IMSI catcher, fake base station attacks [22,63], attacks exploiting attach/registration procedures [24], temporary identifier correlation attacks, attacks based on paging correlation, re-identification attacks through metadata and linkability. The main types of location attacks are attacks based on paging and triggering (call/SMS/push), for presence detection (LAC/TAI/TAC), attacks based on Timing Advance, for distance estimation, attacks based on radio parameters, attacks based on handover and mobility (TAU/RAU/LAU), for movement trajectory detection [37]. In 2G networks, identification and location attacks exploit the one-way authentication mechanism, which allows an attacker to request or directly observe subscriber identifiers; these attacks rely on the use of fake base stations, IMSI catching, and paging monitoring. By introducing two-way authentication, 3G networks reduce some of the risks associated with direct identity exposure, but mechanisms such as paging, mobility management, and fallback procedures remain relevant for tracking and linkability. Attacks on 4G networks target another area of interest that includes GUTI/S-TMSI linkability, exploitation of the Tracking Area Update procedure, and fallback between radio technologies. The architecture of 5G NSA networks is based on the LTE architecture and partially inherits the LTE/EPC control plane interfaces. 5G SA networks introduce the SUCI identifier, which enhances identity protection; however, attacks remain possible due to paging behavior and specific implementation or deployment vulnerabilities. A consolidated cross-generational comparison of these attack categories is presented in the Appendix B.

RQ2. The adversary's capabilities vary depending on the type of attack and can be grouped into three categories [58].

Passive attacks (sniffing) they have capabilities of receiving and decoding channels (broadcast/paging/control-plane), the resources used are commercial equipment, SDRs and opensource software. These attacks have a low operational risk, but are limited by the accessibility of some channels and the need for a compatible radio configuration.

Semi-passive attacks (observation + trigger) are based on triggering specific actions toward a target to generate events on the network (calls, text messages, notifications) and to establish correlations. The necessary resources include access to a trigger channel, which offers the advantage of a high probability of event-target association.

Active attacks (injection/downgrade) impersonates an operator's base station and forces fallback/downgrade or reattachment. The required resources are radio equipment such as SDR, amplifiers and filters, software stack (OsmoBTS, OpenBTS, srsRAN), and the advantage is that it can force identity disclosure. The limitations would be detectability and fine control of radio parameters [64].

In contrast to 2G, where attacks such as fake base stations and IMSI catcher attacks are possible due to the lack of mutual authentication, attacks on 4G and 5G networks generally require specialized SDR devices, a thorough understanding of the protocol, or the use of pre-authentication, interworking, paging, or specific implementation weaknesses.

RQ3. Depending on the type of attack and the deployment environment, it has been observed that for identification attacks the success rate is high in the case of 2G networks, in the case of 4G and 5G networks the success rate depends on the network configurations.

In the case of location attacks, the accuracy varies depending on the technique used, attacks based on radio signals have a more precise estimate than attacks based on paging.

The performance of identification attacks can be summarized in metrics such as identification rate and time to success. The performance of location attacks can be summarized in metrics such as location area, tracking stability and location error. Common to both types of attacks are metrics such as cost, scalability and detectability.

RQ3 investigates the performance information reported by the reviewed studies, including attack success rate or impact, location or localization accuracy, execution time, cost and equipment assumptions, detectability, and deployment conditions. Table 21 provides a concise synthesis of the quantitative evidence explicitly reported in the primary studies. Because these results are heterogeneous and were obtained using different experimental scenarios, adversary models, network configurations, datasets, and evaluation objectives, they could not be standardized onto a single numerical scale for direct comparison.

Table 21. Concise summary of quantitative performance evidence reported in the reviewed studies.

Performance Aspect	Studies	Directly Measured Metrics	Reported Quantitative Evidence
Location-tracking quality	S019, S015, S017	Mobility-pattern recovery; signal-strength indicators; CRB-based privacy indicators	No common location-error metric; qualitative or indirect tracking indicators only.
Attack impact/service disruption	S014	Time to system collapse	System collapse in approximately 30 s.
Signalling overhead/network cost	S001, S013, S033, S008, S009	Messages per UE; MME load events; signalling-overhead reduction; TAU reduction; paging-request reduction; signalling-cost reduction	500–800 and up to 1500 messages/UE; 34% MME load events; 92% overhead reduction; 8% fewer TAUs; 30% fewer paging requests; >30% signalling-cost reduction.
Execution time/algorithmic convergence	S014, S033	Collapse time; number of GA runs; stopping iterations	30 s collapse time; 100 GA runs; 300 stopping iterations.
Detection performance	S014, S024	Detection rate; false-positive rate; detection probability	Detection rate > 96%; false-positive rate < 3.8%; detection probability close to 1 for NCD/MNCD and <0.5 for SpD.

Note. This table provides a concise synthesis of the quantitative evidence reported in the reviewed studies. A complete comparison organized by attack family, including metrics marked as “Not reported” is provided in Appendix B. NCD = Normalized Cumulative Difference; MNCD = Modified Normalized Cumulative Difference; SpD = Spatial Distribution; DoS = Denial of Service; UE = User Equipment; TAU = Tracking Area Update; MME = Mobility Management Entity; GA = Genetic Algorithm; CRB = Cramér–Rao Bound.

To provide a systematic comparison across attack categories, Appendix B presents a complementary table organized by attack family. For each attack family, the appendix reports the available evidence regarding attack success or impact, localization accuracy, time to success, cost and equipment assumptions, detectability, and deployment conditions. Metrics that were not provided by the reviewed studies are explicitly marked as “Not reported.”.

RQ4. Countermeasures identified in the literature can be grouped into three levels: 3GPP standard level measures, operator-implemented measures, and mobile terminal level measures. Measures at the 3GPP level include bidirectional authentication in 3G, 4G, and 5G networks, the method for allocating temporary identifiers with varying efficiency from one generation to the next, protection of the SUPI identifier through the SUCI identifier introduced in 5G networks, innovation of the AKA protocol in 4G and 5G networks, and the

introduction of more restrictive rules regarding the interoperability of mobile networks (2G–5G) [24,37]. Operators can reduce identification and location risks by managing temporary identifiers more strictly in 2G–5G networks, by optimizing paging and Tracking Area policies in 3G–5G networks, and by implementing anomaly detection mechanisms in 4G/5G infrastructures. [22,63]. Regarding mobile terminals, the measures introduced consist of warning applications when suspicious cells are detected and validations at the baseband level, applicable in 3G, 4G and 5G networks [37]. The effectiveness of these countermeasures is limited by compatibility with legacy technologies, operator configurations, and the use of pre-authentication procedures or paging (present in all generations) [24,37].

RQ5. Although security mechanisms have improved from one generation to the next, the attack surface remains significant because of cross-generation compatibility and the continued exposure of signaling metadata.

The attack area differs across cellular network generations. In 2G networks, the main weaknesses are related to identifiers being sent in clear text and to the use of one-way authentication. In 4G networks, the attack area is mainly associated with vulnerabilities in the control plane and signaling procedures [13]. In 5G networks, vulnerabilities are increasingly related to metadata exposure, mobility procedures, and network interoperability [65].

The answers to the research questions highlight that identification and location attacks are evolving along with cellular networks. Although new protection mechanisms have been introduced, the attack surface has remained relatively constant, partly due to interoperability constraints. The attack surface has evolved from the direct exposure of identity in legacy networks (2G) to more subtle forms of linkability, paging correlation, and deployment-dependent privacy leaks in newer generations (4G/5G).

5.2. Persistent Vulnerabilities Between Generations

Each generation of telecommunications technology emerged as a response to the shortcomings of previous networks; however, certain vulnerabilities have persisted alongside the network architecture, not as a result of implementation errors, but as a consequence of architectural design decisions [66]. The underlying factors are interoperability with older generations of mobile networks and multi-RAT coexistence, network mechanism requirements (paging, mobility) and metadata exposure in control-plane and radio procedures. Studies show that there is a constant gap between the standard specifications and the operators' implementations, visible in paging and mobility configuration, temporary identifier configuration, how mobility is handled and fallback mechanism configuration [67]. Persistent vulnerabilities between generations can be observed in Figure 14.

5.3. Mitigation Measures

Mitigation measures against identification and location attacks identified in the literature can be grouped into three categories: standardized measures (3GPP), academic measures, and commercial measures [14]. Each category targets a specific level of the architecture (Core, RAN, UE). The literature promotes the idea that effective mitigation results from combining standardized solutions, which reduce vulnerabilities at the architectural and protocol level, with academic solutions that propose new mechanisms, and with commercial solutions that provide operational protection [68].

5.3.1. Standardized Solutions (3GPP)

In the literature, these solutions are considered to be the most important and appear in the context of the transition from 4G to 5G. These solutions are implemented at the protocol level and at the cellular network architecture level. The identified solutions are:

- Mutual authentication: reduces the attack surface for fake base station attacks [69];
- Use of temporary identifiers (TMSI/GUTI): replacing IMSI with temporary identifiers and relocating them more frequently without being reused frequently;
- Permanent identity protection (SUCI): rsignificantly reduces permanent identity exposure at the time of authentication [70];
- Paging and mobility mechanisms: reducing the predictability of messages from the paging, tracking area update and registration update mechanisms [71,72];
- Downgrade prevention/inter-RAT: network policies to limit the transition to legacy 2G technologies;

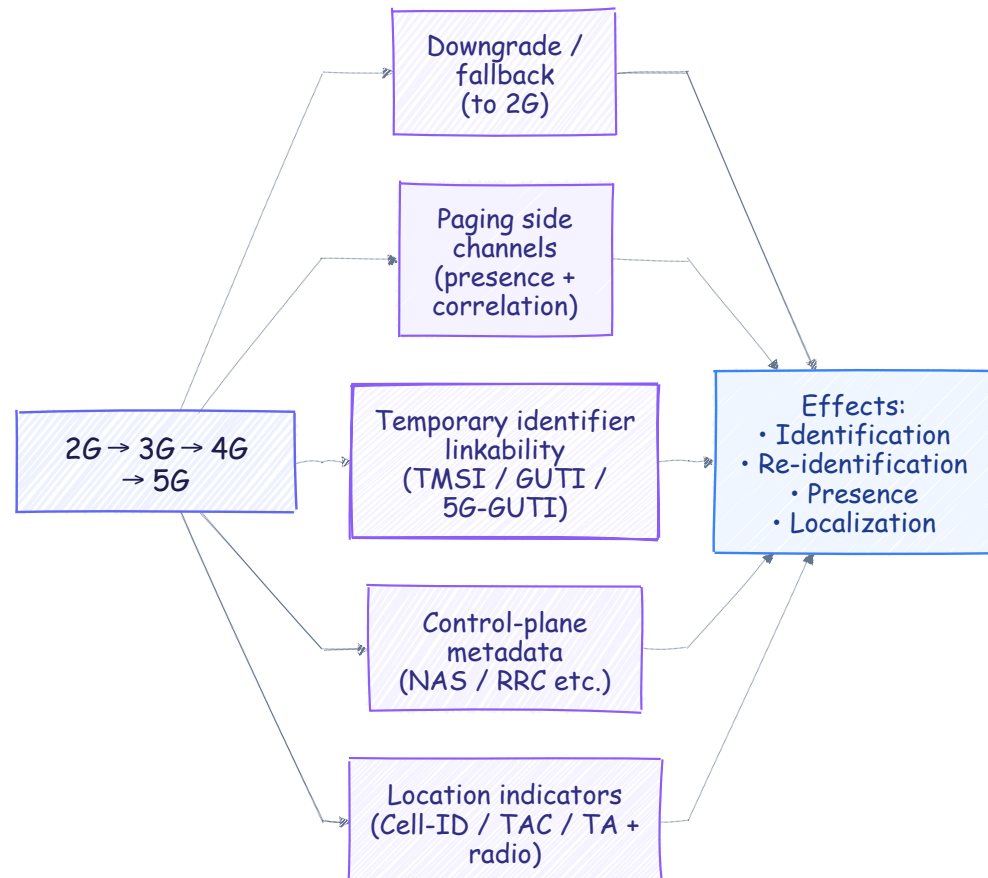


Figure 14. Mobile generation vulnerabilities.

Limitations of standardized solutions are operator implementation dependency, interoperability with older generations, overhead resulting from multiple reallocations, coverage constraints make a downgrade necessary, implementation costs [73].

5.3.2. Academic Solutions

Academic solutions offer a variety of defensive mechanisms for detecting identification and location attacks [33]. Although they are innovative solutions, their implementation in real networks is difficult to achieve. The most ambitious solutions identified are:

- Methods for detecting fake base stations, including IMSI catcher and rogue base station scenarios: are based on the detection of inconsistencies (unusual cell parameters, lack of encryption, sudden changes), protocol inconsistency, machine learning models to distinguish legitimate from suspicious cells, Crowd-sourcing (aggregation of observations), machine learning models for classification [74].

- New authentication methods: schemes based on public-key cryptography, solutions for post-quantum security [63,75,76].
- New identity protection schemes: pseudonym changes to prevent correlation, synchronized change mechanisms [77].
- Detection methods for fake base stations: automatic neighbour relation [78], signaling analysis techniques [41], RF fingerprinting, machine learning anomaly detection [79].
- Identifier protection: improved cryptographic schemes for identifiers.
- Reducing the possibility of paging correlation: paging randomization.

Limitations of academic solutions are signaling overhead or latency, validation only in the laboratory and not on a large scale, incompatibility with current infrastructures and difficult to integrate into standards, energy and computational consumption, dependence on access to mobile terminal parameters, complexity in identifier management, metadata-based inference attacks persist [80].

5.3.3. Commercial Solutions

These solutions aim to detect attacks and monitor mobile networks and can be implemented at the operational level as follows:

- Fake base station and IMSI catcher detection systems (operator-side): commercial Mobile Threat Defense (MTD) products;
- Terminal applications (UE-side): to detect abnormal network behavior and alert the user;
- Threat intelligence and monitoring solutions: systems for detecting patterns associated with abuse [81];

Commercial solutions also have several limitations, including operational complexity, the need for continuous tuning, incomplete coverage, incompatibilities with certain network configurations, proprietary constraints, and dependence on operator policies. In addition, many solutions focus on detection rather than eliminating the root causes of identification and location attacks [82].

5.3.4. Comparisons

The three categories of mitigation have complementary roles. Standardized solutions are oriented toward long-term protection and reduce vulnerabilities at the protocol level by limiting identity exposure and strengthening authentication. Academic solutions propose new protocols and introduce innovative detection approaches, but many remain at the experimental stage. Commercial solutions support practical deployment and operation, but they do not fully eliminate architectural vulnerabilities. For this reason, the literature promotes a multi-layered mitigation approach [83]. Table 22 compares the main categories of mitigation solutions in terms of advantages, disadvantages, and implementation level.

In addition to classifying mitigation solutions, it is necessary to assess the feasibility of implementing them in operators' network infrastructure. The evaluation takes into account criteria such as applicability in operational networks, operator constraints, scalability, compatibility with existing infrastructure, computational cost, and the risk of false positives or false negatives. Table 22 summarizes this critical assessment by comparing the solutions identified in the report in terms of their advantages, practical limitations, implementation conditions, and the targeted architectural level.

Table 22. Critical evaluation matrix of mitigation solutions identified in the reviewed literature.

Mitigation Solution	Category	Level	Advantages	Practical Limitations/Operational Constraints	Representative Studies
Temporary identifier reallocation	Standardized/operator	Core/mobility management	Reduces long-term tracking through TMSI, GUTI, S-TMSI, and 5G-GUTI refresh.	Frequent refresh may increase signalling; infrequent refresh preserves linkability risks.	[7,8,10,48]
SUPI concealment through SUCI	Standardized	UE/Core/NAS	Protects permanent 5G identity; reduces direct SUPI/IMSI exposure.	Depends on correct SUCI configuration, key management, UE support, and avoidance of weak/null profiles.	[23,25,29,48,73]
Paging policy hardening and paging optimization	Standardized/operator/academic	Core/RAN	Limits paging correlation, presence inference, and idle-mode exposure.	May affect reachability, latency, and signalling load; requires privacy-efficiency trade-offs.	[7,27,34,51,72]
Restriction of insecure fallback and inter-RAT mobility	Standardized/operator	Core/RAN/interworking	Reduces downgrade and legacy-procedure exposure.	Constrained by service continuity, roaming, emergency services, and legacy UE support.	[18,22,48,82]
Tracking area/registration area optimization	Academic/operator	Core/mobility management	Reduces unnecessary paging and can limit coarse location exposure.	May increase update overhead or conflict with signalling efficiency.	[32,34,39,40,72]
Rogue base station detection	Academic/commercial	RAN/terminal/monitoring	Detects fake BTS/eNodeB/gNodeB and supports operator or terminal alerts.	Accuracy depends on coverage, thresholds, radio conditions, and attacker behavior; false alarms may occur.	[22,49,55,57,74,78,80,83,84]
Cryptographic enhancements to authentication and identity protection	Academic/standard-oriented	UE/Core/protocol	Improves anonymity, unlinkability, and resistance to replay, downgrade, or fake-network attacks.	Often needs protocol changes, extra computation, standardization, and infrastructure compatibility.	[3,6,9,14,25,31,47,77]
Terminal-side suspicious cell detection	Academic/commercial	UE/terminal	Warns about suspicious cells, abnormal radio conditions, or identity requests.	Limited by OS/baseband access, device diversity, battery cost, and false positives/negatives.	[22,48,55,57]
Anomaly detection in signalling behavior	Academic/commercial	Core/RAN/monitoring	Identifies abnormal paging, attach, registration, or mobility-management patterns.	Requires visibility, baseline models, threshold tuning, and adaptation to roaming/heterogeneous traffic.	[2,28,41,50,64]
Operator-side monitoring and audit tools	Commercial/operator	Operator/RAN/core	Provides operational visibility, rogue-cell detection, anomaly monitoring, and audits.	Limited by vendor dependency, cost, integration complexity, transparency, and operator policies.	[22,49,50,84,85]

The mitigation measures identified in the literature do not all have the same level of maturity and cannot be evaluated solely in terms of the theoretical protection they offer. The effectiveness of many proposed measures depends on proper configuration by operators, as well as roaming, fallback, paging, and mobility management policies. Therefore, each identified security measure was critically analyzed, taking into account practical feasibility, the level of technological development, operating costs, scalability, and compatibility with existing mobile networks.

5.4. Limitations of the Review

With regard to the interpretation of the results, this review has a number of limitations. Although the search strategy included major scientific databases and platforms, such as IEEE Xplore, ScienceDirect/Elsevier, and Springer, it is possible that certain relevant studies indexed in other sources or technical reports from operators and commercial providers were not identified by the search process used.

To avoid misinterpretation, publications from the year 2026 were included in the final corpus only if they were published, indexed, or available online before the systematic

search date, 19 March 2026, and met the inclusion criteria. However, 2026 was excluded from the temporal-evolution graph because it was an incomplete publication year at the time of the search.

Identification and location attacks in cellular networks are described in the literature using a variety of terms; consequently, the results are influenced by the selected search terms and the structure of the queries. The studies identified primarily describe successfully demonstrated attacks and promising mitigation solutions, while failed experiments, internal assessments by operators, or commercial limitations are less frequently published.

Another important limitation is the heterogeneity of the studies analyzed, which limits the possibility of a direct comparison between the reported results. Some studies are based on simulations or formal models, others on SDR prototypes, commercial devices or measurements in operational networks. These are the reasons why the article provides a qualitative and comparative synthesis of the literature, supported by critical discussions.

5.5. Recommendations for Future Research

The literature shows significant progress in the study of identification and location attacks. However, several technical gaps remain, especially in multi-RAT contexts. Given the complexity of new mobile network architectures [86], the field remains far from being exhausted.

Based on the synthesis presented above, several recommendations can be formulated for future research. Future studies should investigate new anonymization and identification mechanisms, with particular attention to indirect identification attacks, and should include experiments in real commercial networks rather than relying only on controlled environments. Additional research is also needed on attacks resulting from intergenerational interoperability, as well as on vulnerabilities in paging and mobility procedures, which are consequences of fundamental network functions.

The evolution of the attack surface should also be analyzed in the context of new O-RAN architectures and the virtualization of network functions. Furthermore, future work should examine the security compromises introduced to ensure network efficiency, develop mechanisms for protecting signaling messages, and evaluate the computational cost, overhead, and latency of mitigation measures. Another important direction is the development of fake base station detection mechanisms that can be integrated into both mobile terminals and operators' infrastructure.

Finally, because the comparison between 5G NSA and 5G SA shows that architecture, identity management, and privacy risks depend strongly on operator configurations and implementation choices, future research should include real-world network measurements.

5.6. Responsible Use Statement

This study analyzes identification and location attacks in cellular networks for strictly defensive and academic purposes, with the aim of protecting user identity and improving mobile communication security. The review does not encourage unauthorized experimentation on public or private cellular networks and does not facilitate unauthorized access, interception, impersonation, or disruption.

The attacks identified in the literature are discussed at a conceptual and analytical level. They are compared from a taxonomic perspective, with emphasis on exploited procedures, affected entities, limitations, and mitigation solutions. Implementation steps, exploitation procedures, configuration details, or other elements that could facilitate misuse are intentionally avoided.

Any experimental evaluation of cellular security mechanisms should be performed only in controlled, isolated, and authorized environments, in accordance with applicable

legislation. Testing on commercial networks is outside the scope of this article. The purpose of this review is to consolidate the literature, support defensive research, raise awareness among operators, and contribute to the design of more secure cellular systems.

6. Conclusions

This study conducted a systematic review of identification and location attacks in cellular networks from 2G to 5G. The analysis was structured around clear research questions designed to identify existing vulnerabilities, exploited mechanisms, limitations of current solutions, and opportunities for future research. The attacks identified in the literature were classified according to the exploited vector, the adversary's capabilities, the cellular generation and the scenario used.

The results show that although security mechanisms have evolved with cellular networks, vulnerabilities and the scope of attacks on identity and location have migrated along with new generations of cellular networks. Persistent vulnerabilities between generations have been grouped into five classes: downgrade, paging, temporary identifiers, control plane, and location indicators. Mitigation mechanisms are divided into standard solutions, academic solutions, and commercial solutions, but these countermeasures are less effective against inferences due to trade-offs between security, performance, and compatibility.

One of the important results of this study is highlighting the impact on security of interoperability between generations, which maintains the attack surface that includes everything from passive monitoring attacks to the use of SDR equipment and open-source software.

Another result of the review is the identification of an intensification of research on identification and location attacks in 4G–5G networks in recent years, which shows that the problem of these attacks has not been solved by the new, more complex cellular generations. In order to reduce the risks, it was concluded that a combination of operator-side, terminal-side policies and detection and audit tools is necessary [85]. The results of this study were influenced by the multidisciplinary and interdisciplinary nature of the field and the heterogeneity of the studies, so that in order to respond to the challenges, it is necessary to develop cryptographic mechanisms at the level of protocols and interaction between network components.

Funding: This research received no external funding. The APC was fully waived through a 100% discount.

Data Availability Statement: The data supporting the findings of this study are available within the article and its appendices. No new external dataset was generated.

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

Abbreviations

BTS	Base Transceiver Station
CN	Core Network
ECGI	E-UTRAN Cell Global Identifier
eNB	evolved NodeB
EPS-AKA	Evolved Packet System Authentication and Key Agreement
GGSN	Gateway GPRS Support Node
gNB	next generation NodeB
GUTI	Globally Unique Temporary UE Identity
5G-GUTI	5G Globally Unique Temporary UE Identity
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
MIB	Master Information Block

MME	Mobility Management Entity
MS	Mobile Station
MSC	Mobile Switching Center
NAS	Non-Access Stratum
NSA	Non-Standalone
O-RAN	Open Radio Access Network
HLR	Home Location Register
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
inter-RAT	inter-Radio Access Technology
LAI	Location Area Identity
LTE	Long-Term Evolution
PDN	Packet Data Network
VLR	Visitor Location Register
SA	Standalone
SDR	Software-Defined Radio
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
BSC	Base Station Controller
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIB	System Information Block
S1AP	S1 Application Protocol
SMF	Session Management Function
SS7	Signaling System No. 7
TAC	Tracking Area Code
TAI	Tracking Area Identity
TAU	Tracking Area Update
PGW	Packet Data Network Gateway
PHY	Physical Layer
PSTN	Public Switched Telephone Network
RAN	Radio Access Network
RNC	Radio Network Controller
RRC	Radio Resource Control
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
UPF	User Plane Function
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UMTS	Universal Mobile Telecommunications System

Appendix A. Included Studies and Extracted Data

Table A1. Complete list of included studies and extracted data.

ID	Authors	Title	Year	Source	Attack Type/Category	Generation	Exploited Mechanism	Adversary Model	Reported Metrics	Countermeasures/Solutions
S001	A. A. R. Alsaedy; E. K. P. Chong [72]	Tracking Area Update Procedure Unnecessary in 5G: Improving User Experience and Offloading Signaling Overhead	2018	IEEE Xplore; https://repository.qu.edu.iq/wp-content/uploads/sites/31/2024/09/Tracking-Area-Update.pdf (accessed on 19 March 2026)	Location tracking & mobility privacy; Semi-passive	5G	paging; tracking area/update; mobility/location management	Semi-passive	Signaling overhead; UE power consumption; paging reachability/efficiency	gNB-based UE Mobility Tracking (UeMT); shifting location tracking from UE-triggered TAU to gNB/network-side tracking
S002	L. Abdelrazek; M. A. Azer [5]	User Privacy in Legacy Mobile Network Protocols	2018	IEEE Xplore; https://doi.org/10.1109/icsrs.2018.8688870 (accessed on 19 March 2026)	Identity and authentication privacy; Semi-passive	2G/3G/4G legacy networks	IMSI/subscriber identity; paging/location management; signalling security	Semi-passive	Not reported	Privacy-preserving identifier, pseudonym, SUCI/SUPI protection or protocol hardening
S003	R. Ghannam; F. Sharevski; A. Chung [28]	User-targeted Denial-of-Service Attacks in LTE Mobile Networks	2018	IEEE Xplore; https://www.researchgate.net/publication/329953228_User-targeted_Denial-of-Service_Attacks_in_LTE_Mobile_Networks (accessed on 19 March 2026)	Rogue/fake base stations; Active	4G/LTE	authentication privacy; rogue base station; signalling security	Active	Attack feasibility in LTE testbed; user-targeted service disruption; DoS impact	Not reported
S004	Garima SinghDeepti Shrimankar [35]	A privacy-preserving authentication protocol with secure handovers for the LTE/LTE-A networks	2018	SpringerLink; https://www.ias.ac.in/public/Volumes/sadh/043/08/0128.pdf (accessed on 19 March 2026)	Identity and authentication privacy; Passive	4G/LTE-A	Authentication/key agreement; subscriber identity protection; handover security	Passive	Not reported	Privacy-preserving authentication protocol with secure handovers for LTE/LTE-A
S005	Mohsin KhanPhilip GinzboorgKimmo JärvinenValtteri Niemi [18]	Defeating the Downgrade Attack on Identity Privacy in 5G	2018	SpringerLink; https://arxiv.org/abs/1811.02293 (accessed on 19 March 2026)	Identity and authentication privacy; Active	5G	privacy	Active adversary, typically rogue/fake base station or malicious network element	Not reported	LTE pseudonym-based identity protection; LTE pseudonym update integrated into 5G identity privacy procedure
S006	Mihajlo Pavloski [42]	Signalling Attacks in Mobile Telephony	2018	SpringerLink; https://doi.org/10.1007/978-3-319-95189-8_12 (accessed on 19 March 2026)	Protocol and signalling security; Passive	Not reported	signalling security	Passive	Not reported	Not reported
S007	Alaa A. R. Alsaedy and Edwin K. P. Chong [7]	Tracking Area Update and Paging in 5G Networks: a Survey of Problems and Solutions	2018	SpringerLink; https://www.researchgate.net/publication/328579958_Tracking_Area_Update_and_Paging_in_5G_Networks_a_Survey_of_Problems_and_Solutions (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	5G	paging; tracking area/update; mobility/location management	Not applicable/survey or review	Paging overhead; Tracking Area Update (TAU) overhead; signaling overhead	Surveyed solutions for TAU reduction, paging optimization and tracking-area/location-management design
S008	H. Kim; J. Lee; E. Lee; Y. Kim [15]	Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane	2019	IEEE Xplore; https://doi.org/10.1109/SP.2019.000038 (accessed on 19 March 2026)	Protocol and signalling security; Active	4G/LTE	LTE control-plane procedures; unauthenticated signalling messages; protocol-state and implementation vulnerabilities	Active	Security vulnerabilities and practical control-plane attacks	Dynamic security analysis; control-plane message protection; protocol-state validation
S009	B. Aamer; H. Chergui; N. Chergui; K. Tourki; M. Benjillali; C. Verikoukis; M. Debbah [40]	Self-Tuning Spectral Clustering for Adaptive Tracking Areas Design in 5G Ultra-Dense Networks	2019	IEEE Xplore; https://arxiv.org/abs/1902.01342 (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	5G	paging; tracking area/update; mobility/location management	Semi-passive	Q-metric; silhouette score; number of TAs; TAUs; paging requests/average paging requests per TA	Self-tuning spectral clustering for adaptive tracking-area design
S010	A. Ali; G. Fischer [37]	Symbol-Based Statistical RF Fingerprinting for Fake Base Station Identification	2019	IEEE Xplore; https://doi.org/10.1109/RADIOE.LEK.2019.8733585 (accessed on 19 March 2026)	Rogue/fake base stations; Active	Cellular networks	RF fingerprinting; amplitude and phase error characteristics; fake base station identification	Active adversary operating a fake or rogue base station	Amplitude and phase error statistics; RF fingerprinting classification and detection indicators	Symbol-based statistical RF fingerprinting for fake base station identification

Table A1. Cont.

ID	Authors	Title	Year	Source	Attack Type/Category	Generation	Exploited Mechanism	Adversary Model	Reported Metrics	Countermeasures/Solutions
S011	A. Koutsos [47]	The 5G-AKA Authentication Protocol Privacy	2019	IEEE Xplore; https://arxiv.org/abs/1811.06922 (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	Authentication/key agreement; subscriber identity protection; handover security	Active	Formal/privacy proof metrics; sigma-unlinkability; mutual authentication proof	Modified 5G-AKA protocol to prevent privacy attacks while retaining cost/efficiency constraints
S012	A. Ali; G. Fischer [79]	The Phase Noise and Clock Synchronous Carrier Frequency Offset based RF Fingerprinting for the Fake Base Station Detection	2019	IEEE Xplore; https://ieeexplore.ieee.org/document/8765471/ (accessed on 19 March 2026)	Rogue/fake base stations; Active	Not reported	Rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	Phase noise; clock-synchronous carrier frequency offset; RF fingerprint separability/detection indicators	RF fingerprinting using phase noise and clock-synchronous CFO for fake base station detection
S013	Hashim A. Hashim and Mohammad A. Abido [32]	Location management in LTE networks using multi-objective particle swarm optimization	2019	ScienceDirect; https://arxiv.org/abs/1905.01136 (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	4G/LTE	paging; tracking area/update; mobility/location management	Semi-passive	Total signaling overhead; TAU and paging cost; inter-list handover; power/battery consumption; comparison with MINLP	Multi-objective particle swarm optimization (MOPSO) for LTE location-management optimization
S014	Ginés Escudero-AndreuKonstantinos KyriakopoulosJames A. FlintSangarapillai Lambodharan [41]	Detecting Signalling DoS Attacks on LTE Networks	2019	SpringerLink; https://repository.lboro.ac.uk/articles/conference_contribution/Detecting_signalling_DoS_attacks_on_LTE_networks/9548273/files/17179283.pdf (accessed on 19 March 2026)	Protocol and signalling security; Active	4G/LTE	signalling security	Active	Time to collapse system; request rate (500 service requests/s); signalling DoS detection performance	Detection of LTE signalling DoS attacks using observable signalling/request behavior
S015	F. Xu; Z. Tu; Y. Li [53]	Connecting the Dots: User Privacy is not Preserved in ID-Removed Cellular Data	2020	IEEE Xplore; https://www.researchgate.net/publication/315870338_Trajectory_Recovery_From_Ash_User_Privacy_Is_NOT_Preserved_in_Aggregated_Mobility_Data (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	Not reported	privacy	Passive or semi-passive adversary using mobility/signalling/location data	Re-identification/record association effectiveness; trajectory/mobility pattern recovery	ID removal is shown insufficient; privacy implication is need for stronger anonymization than simple identifier removal
S016	Fardan; Istikmal; I. Mawaldi; T. Anugraha; I. Ginting; N. Karna [30]	Experimental Security Analysis for Fake eNodeB Attack on LTE Network	2020	IEEE Xplore; https://doi.org/10.1109/isriti51436.2020.9315427 (accessed on 19 March 2026)	Rogue/fake base stations; Active	4G/LTE	IMSI/subscriber identity; fake base station; fake eNodeB	Active	Not reported	Not reported
S017	M. Saedi; A. Moore; P. Perry; M. Shojafar; H. Ullah; J. Synnott; R. Brown; I. Herwono [46]	Generation of realistic signal strength measurements for a 5G Rogue Base Station attack scenario	2020	IEEE Xplore; https://pure.ulster.ac.uk/files/90882336/09162275.pdf (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	Signal strength measurements; synthetic/realistic RSRP/RSSI-style datasets for RBS investigation	Generation of realistic signal-strength data to support rogue base station detection/investigation
S018	H. Qi; Y. Shen; B. Yin [13]	Intelligent Trajectory Inference Through Cellular Signaling Data	2020	IEEE Xplore; https://www.researchgate.net/publication/312668648_On_location_privacy_in_LTE_networks (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	Not reported	tracking/inference; location privacy/inference; signalling security	Passive or semi-passive adversary using mobility/signalling/location data	Not reported	Not reported
S019	J. J. Checa; S. Tomasín [4]	Location-Privacy-Preserving Technique for 5G mmWave Devices	2020	IEEE Xplore; https://www.researchgate.net/publication/343782892_Location-Privacy_Preserving_Technique_for_5G_mmWave_Devices (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	fake base station; location privacy/inference; privacy	Active	Location privacy metric based on localization information/CRB-style evaluation	Location-privacy-preserving technique for 5G mmWave devices; beamforming/location privacy protection
S020	M. Pauliac [70]	USIM in 5G Era	2020	IEEE Xplore; https://www.researchgate.net/publication/393945539_A_survey_of_existing_attacks_on_5G_SA (accessed on 19 March 2026)	Identity and authentication privacy; Passive	5G	authentication privacy; privacy	Passive	Not applicable; overview article	USIM/5G privacy and security features: authentication schemes, subscriber privacy, Steering of Roaming, UE Parameters Update over NAS, Long-Term Key Update

Table A1. Cont.

ID	Authors	Title	Year	Source	Attack Type/Category	Generation	Exploited Mechanism	Adversary Model	Reported Metrics	Countermeasures/Solutions
S021	Haibat Khan and Keith M. Martin [48]	A survey of subscription privacy on the 5G radio interface - The past, present and future	2020	ScienceDirect; https://eprint.iacr.org/2020/101.pdf (accessed on 19 March 2026)	General cellular security/privacy; Passive	5G	privacy	Not applicable/survey or review	Not applicable; survey paper	Countermeasures classified into cryptographic methods, human factors, and intrusion detection methods
S022	An Braeken [6]	Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability	2020	ScienceDirect; https://www.researchgate.net/publication/342979788_Symmetric_key_based_5G_AKA_authentication_protocol_satisfying_anonymity_and_unlinkability (accessed on 19 March 2026)	Identity and authentication privacy; Passive	5G	authentication/key agreement; subscriber identity protection; handover security	Passive	Computational/communication efficiency; security properties: anonymity and unlinkability	Symmetric-key-based 5G-AKA protocol satisfying anonymity and unlinkability
S023	S. Sivasankar; R. Challa [27]	Closed Loop Paging Optimization for Efficient Mobility Management	2021	IEEE Xplore; https://researchr.org/publication/ccnc-2021 (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	Not reported	paging; tracking area/update; mobility/location management	Semi-passive	Paging efficiency/signaling overhead	Closed-loop paging optimization for mobility management
S024	D. Orlando; I. Palamà; S. Bartoletti; G. Bianchi; N. B. Melazzi [57]	Design and Experimental Assessment of Detection Schemes for Air Interface Attacks in Adverse Scenarios	2021	IEEE Xplore; https://arxiv.org/abs/2106.07199 (accessed on 19 March 2026)	Rogue/fake base stations; Active	Not reported	rogue base station	Active	Detection probability (Pd) curves; performance under adverse scenarios; SDR LTE experiment	Three GLRT-based detection schemes using data from off-the-shelf receivers
S025	I. Bang; T. Kim; H. S. Jang; D. K. Sung [24]	Impact of Uplink Power Control on User Location Tracking Attacks in Cellular Networks	2021	IEEE Xplore; https://icc2021.ieee-icc.org/program/technical-symposia.html (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	Not reported	tracking/inference; location privacy/inference; privacy	Passive or semi-passive adversary using mobility/signalling/location data	Location tracking performance under uplink power control	Uplink power control considered as factor/mitigation for user location tracking attacks
S026	I. Karim; S. R. Hussain; E. Bertino [2]	ProChecker: An Automated Security and Privacy Analysis Framework for 4G LTE Protocol Implementations	2021	IEEE Xplore; https://www.researchgate.net/publication/399371469_Leveraging_Hardware_Hacking_Tools_for_Unveiling_Vulnerabilities_in_Internet_of_Things_IoT_Devices_A_Comprehensive_Review (accessed on 19 March 2026)	Protocol and signalling security; Active	4G/4G/LTE	privacy	Active	Number/types of detected specification violations or logical vulnerabilities	Automated security and privacy checking framework for 4G LTE protocol implementations
S027	F. Liu; L. Su; B. Yang; H. Du; M. Qi; S. He [25]	Security Enhancements to Subscriber Privacy Protection Scheme in 5G Systems	2021	IEEE Xplore; https://www.researchgate.net/publication/367620100_Latest_Advances_on_Security_Architecture_for_5G_Technology_and_Services (accessed on 19 March 2026)	Identity and authentication privacy; Passive	5G	SUCI/concealed identifier; SUPI/permanent identifier; privacy	Passive	Not reported	Security enhancements to subscriber privacy protection scheme in 5G systems
S028	Ivan Palamà and Francesco Gringoli and Giuseppe Bianchi and Nicola Blefari-Melazzi [22]	IMSI Catchers in the wild: A real world 4G/5G assessment	2021	ScienceDirect; https://www.researchgate.net/publication/393170131_FlashCatch_Minimizing_Disruption_in_IMSI_Catcher_Operations (accessed on 19 March 2026)	Rogue/fake base stations; Active	4G/5G	rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	Not reported	IMSI catcher assessment; mitigation not reported
S029	Tong ZhangMeihua XiaoRi Ouyang [69]	Proving Mutual Authentication Property of 5G-AKA Protocol Based on PCL	2021	SpringerLink; https://doi.org/10.1007/978-981-16-7443-3_13 (accessed on 19 March 2026)	Identity and authentication privacy; Passive	5G	authentication/key agreement; subscriber identity protection; handover security	Passive	Not reported	Authentication/key-agreement or handover-security protocol proposed

Table A1. Cont.

ID	Authors	Title	Year	Source	Attack Type/Category	Generation	Exploited Mechanism	Adversary Model	Reported Metrics	Countermeasures/Solutions
S030	J. Zhao; Q. Li; Z. Yuan; Z. Zhang; S. Lu [44]	5G Messaging: System Insecurity and Defenses	2022	IEEE Xplore; https://www.researchgate.net/publication/365604755_5G_Messaging_System_Insecurity_and_Defenses (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	5G	5G messaging service; unauthenticated or weakly protected messaging procedures	Semi-passive	Not reported	Defenses for 5G messaging service insecurity
S031	I. Bang; T. Kim; H. S. Jang; D. K. Sung [33]	An Opportunistic Power Control Scheme for Mitigating User Location Tracking Attacks in Cellular Networks	2022	IEEE Xplore; https://ieeexplore.ieee.org/document/9715139/ (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	Not reported	tracking/inference; location privacy/inference; privacy	Passive or semi-passive adversary using mobility/signalling/location data	Not reported	Opportunistic power control scheme for mitigating user location tracking attacks
S032	J. Shin; Y. Shin; J. -G. Park [78]	Network Detection of Fake Base Station Using Automatic Neighbour Relation in Self-Organizing Networks	2022	IEEE Xplore; https://doi.org/10.1109/ictc55196.2022.9952901 (accessed on 19 March 2026)	Rogue/fake base stations; Active	Not reported	Rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	Not reported	Detection, localization, or blacklisting method proposed
S033	L. A. N. Oliveira; M. S. Alencar; W. T. A. Lopes; F. Madeiro [51]	On the Performance of Location Management in 5G Network Using RRC Inactive State	2022	IEEE Xplore; https://www.researchgate.net/publication/360907319_On_the_Performance_of_Location_Management_in_5G_Network_Using_RRC_Inactive_State (accessed on 19 March 2026)	Location tracking and mobility privacy; Active	5G	paging; tracking area/update; mobility/location management	Active	Signaling cost; delay cost; simulator-based location-management performance	Genetic algorithm/optimized design using RRC Inactive State, RNA/TA association to reduce signaling cost
S034	Tengshun Yang and Shuling Wang and Bohua Zhan and Naijun Zhan and Jinghui Li and Shuangqin [26]	Formal Analysis of 5G Authentication and Key Management for Applications (AKMA)	2022	ScienceDirect; https://doi.org/10.1016/j.sysarc.2022.102478 (accessed on 19 March 2026)	Identity and authentication privacy; Passive	5G	authentication/key agreement; subscriber identity protection; handover security	Passive	Not reported	Authentication/key-agreement or handover-security protocol proposed
S035	Mohamed Taoufiq Damir and Valtteri Niemi [10]	Location Privacy, 5G AKA, and Enhancements	2022	SpringerLink; https://doi.org/10.1007/978-3-031-22295-5_3 (accessed on 19 March 2026)	Identity and authentication privacy; Semi-passive	5G	authentication/key agreement; subscriber identity protection; handover security	Semi-passive	Not reported	Authentication/key-agreement or handover-security protocol proposed
S036	B. Aamer; H. Chergui; M. Benjillali [39]	Clustering-Enabled Tracking Areas Design for Beyond-5G Networks: A Live Network Demo	2023	IEEE Xplore; https://www.researchgate.net/publication/371811401_Clustering-Enabled_Tracking_Areas_Design_for_Beyond-5G_Networks_A_Live_Network_Demo (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	5G	paging; tracking area/update; mobility/location management	Semi-passive	Not reported	Clustering-enabled tracking area design for B5G networks
S037	S. Kriaa; A. Feki; S. Papillon; T. Chene; I. Ouattara [74]	Detecting Fake Base Stations Using Knowledge Graphs and ML-Based Techniques	2023	IEEE Xplore; https://www.researchgate.net/publication/352806426_SecKG_Leveraging_attack_detection_and_prediction_using_knowledge_graphs (accessed on 19 March 2026)	Rogue/fake base stations; Active	Not reported	Rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	ML/knowledge graph detection metrics	Knowledge graph and ML-based fake base station detection
S038	J. -H. Huang; S. -M. Cheng; R. Kaliski; C. -F. Hung [49]	Developing xApps for Rogue Base Station Detection in SDR-Enabled O-RAN	2023	IEEE Xplore; https://www.researchgate.net/publication/373500416_Developing_xApps_for_Rogue_Base_Station_Detection_in_SDR-Enabled_O-RAN (accessed on 19 March 2026)	Rogue/fake base stations; Active	Not reported	Rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	Signal stability metrics; UE-reported metrics; Near-RT RIC/xApp processing not reported	xApp-based rogue base station detection in SDR-enabled O-RAN; distribution of detection outputs/metrics to UEs
S039	C. Yu; S. Chen; Z. Cai [43]	LTE Phone Number Catcher: A Practical Attack Against Mobile Privacy	2019	Security and Communication Networks; https://doi.org/10.1155/2019/7425235 (accessed on 19 March 2026)	Identity and location privacy; Active	4G/LTE	paging procedure; temporary identifiers; silent communication triggering; phone-number-to-radio-identifier correlation	Active	Practical association between the target phone number and LTE temporary identifiers; target presence confirmation and location tracking	Protection of paging identifiers; frequent temporary-identifier refresh; prevention of unauthorized paging triggering and identifier correlation

Table A1. Cont.

ID	Authors	Title	Year	Source	Attack Type/Category	Generation	Exploited Mechanism	Adversary Model	Reported Metrics	Countermeasures/Solutions
S040	S. Basheer; G. Kumar; A. H. Nalband; C. Raveendran [83]	Securing 5G Networks: Strategies for Prevention, Detection, and Mitigation of Rogue Base Stations	2023	IEEE Xplore; https://doi.org/10.1109/icstce60504.2023.10585168 (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	Not reported	Detection, localization, or blacklisting method proposed
S041	Zaher Haddad [77]	Blockchain-enabled anonymous mutual authentication and location privacy-preserving scheme for 5G networks	2023	ScienceDirect; https://www.scribd.com/document/637788795/Blockchain-enabled-anonymous-mutual-authentication-and-location (accessed on 19 March 2026)	Identity and authentication privacy; Semi-passive	5G	authentication/key agreement; subscriber identity protection; handover security	Semi-passive	Security analysis; performance evaluation/efficiency compared with existing schemes	Blockchain + pseudonym-based anonymous mutual authentication and location privacy preservation
S042	Teng Fei and Wenye Wang [31]	The vulnerability and enhancement of AKA protocol for mobile authentication in LTE/5G networks	2023	ScienceDirect; https://doi.org/10.1016/j.comnet.2023.109685 (accessed on 19 March 2026)	Identity and authentication privacy; Semi-passive	4G/LTE/5G	authentication/key agreement; subscriber identity protection; handover security	Semi-passive	Not reported	Authentication/key-agreement or handover-security protocol proposed
S043	Lie YangChien-Erh WengHsing-Chung ChenYang-Cheng-Kuang ChenYung-Cheng Yao [11]	Attacks and Threats Verification Based on 4G/5G Security Architecture	2023	SpringerLink; https://doi.org/10.1007/978-3-031-35836-4_26 (accessed on 19 March 2026)	General cellular security/privacy; Passive	4G/5G	cellular security relevance	Passive	Not reported	Not reported
S044	Daniel FraunholzDominik BrunkLorenz DumanskiHartmut Koenig [60]	Automating Device Fingerprinting Attacks in 4G and 5G NSA Mobile Networks	2023	SpringerLink; https://doi.org/10.1007/978-3-031-30122-3_12 (accessed on 19 March 2026)	Rogue/fake base stations; Semi-passive	4G/5G	RF fingerprinting; signal features of base stations/devices	Semi-passive	Not reported	Not reported
S045	U. Dixit; S. Vittal; A. F. A [19]	A Systematic Study for Understanding the Security Risks in 5G Core Network	2024	IEEE Xplore; https://doi.org/10.1109/comsnet59351.2024.10427440 (accessed on 19 March 2026)	Protocol and signalling security; Active	5G	5G core security	Active	Not reported	Not reported
S046	S. Sun; I. Abualhao; G. Poitau; A. Esswie; M. Repeta [64]	An Ensemble Approach for Fake Base Station Detection using Temporal Graph Analysis and Anomaly Detection	2024	IEEE Xplore; https://doi.org/10.1109/wts60164.2024.10536680 (accessed on 19 March 2026)	Rogue/fake base stations; Active	Not reported	Rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	Not reported	Detection, localization, or blacklisting method proposed
S047	S. Purification; S. Wuthier; J. Kim; J. Kim; S. -Y. Chang [84]	Fake Base Station Detection and Blacklisting	2024	IEEE Xplore; https://doi.org/10.1109/icccn61486.2024.10637542 (accessed on 19 March 2026)	Rogue/fake base stations; Active	Not reported	Rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	Not reported	Detection, localization, or blacklisting method proposed
S048	W. Fan; B. Shi; C. Peng [12]	NReplay: 5G Key Reinstallation Attack Based on NAS Layer Vulnerabilities	2024	IEEE Xplore; https://doi.org/10.1109/milcom61039.2024.10773741 (accessed on 19 March 2026)	Identity and authentication privacy; Active	5G/5G NR	privacy	Active adversary, typically rogue/fake base station or malicious network element	Not reported	Defense or mitigation discussed
S049	B. C. Tedeschini; G. Kwon; M. Nicoli; M. Z. Win [54]	Real-Time Bayesian Neural Networks for 6G Cooperative Positioning and Tracking	2024	IEEE Xplore; https://doi.org/10.1109/jsac.2024.3413950 (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	6G	tracking/inference; location privacy/inference	Semi-passive	Not reported	Location-management, paging, or tracking mitigation/optimization discussed
S050	S. Purification; K. Park; J. Kim; J. Kim; S. -Y. Chang [81]	Wireless Link Routing to Secure Against Fake Base Station in 5G	2024	IEEE Xplore; https://doi.org/10.1109/svcc61185.2024.10637367 (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	Not reported	Not reported
S051	Samuthira Pandi V and Anitha Juliette Albert and K. Naresh Kumar Thapa and R. Krishnaprasa [86]	A novel enhanced security architecture for sixth generation (6G) cellular networks using authentication and acknowledgement (AA) approach	2024	ScienceDirect; https://doi.org/10.1016/j.rine.2023.101669 (accessed on 19 March 2026)	Identity and authentication privacy; Passive	6G	authentication/key agreement; subscriber identity protection; handover security	Passive	Not reported	Authentication/key-agreement or handover-security protocol proposed

Table A1. Cont.

ID	Authors	Title	Year	Source	Attack Type/Category	Generation	Exploited Mechanism	Adversary Model	Reported Metrics	Countermeasures/Solutions
S052	Z. Haddad [62]	Enhancing Privacy and Security in 5G Networks with an Anonymous Handover Protocol Based on Blockchain and Zero Knowledge Proof	2024	ScienceDirect; https://doi.org/10.1016/j.comnet.2024.110544 (accessed on 19 March 2026)	Identity, authentication, and location privacy; Active	5G	anonymous authentication; handover authentication; blockchain; zero-knowledge proof; subscriber identity and location privacy protection	Active adversary attempting impersonation, replay, man-in-the-middle, or identity-tracing attacks	Security analysis; computational and communication overhead; comparison with related authentication and handover protocols	Anonymous 5G handover authentication protocol based on blockchain and zero-knowledge proof
S053	Chuan Yu and Shuhui Chen and Qianqian Xing and Ziling Wei [3]	Protecting unauthenticated messages in LTE/5G mobile networks: A two-level Hierarchical Identity-Based Signature (HIBS) solution	2024	ScienceDirect; https://doi.org/10.1016/j.comnet.2024.110814 (accessed on 19 March 2026)	Location tracking and mobility privacy; Active	4G/LTE/5G	tracking/inference; location privacy/inference; signalling security	Active	Not reported	Not reported
S054	Danmarl ButadSteven Matthew TaoHarlee TadtudAlvin Joseph MacapagalPhilip Virgil AstilloGau [80]	Fake Base Station Detection and Localization in 5G Network: A Proof of Concept	2024	SpringerLink; https://doi.org/10.1007/978-981-97-4465-7_1 (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	rogue/fake base station; subscriber identity exposure; radio access security	Active adversary, typically rogue/fake base station or malicious network element	Not reported	Detection, localization, or blacklisting method proposed
S055	A. Triesch; T. Barsch; V. Moonsamy; M. Große-Kampmann [56]	5G Under Siege: A Comprehensive Guide to Threats and Penetration Testing in 5G Campus Networks	2025	IEEE Xplore; https://doi.org/10.1109/iwcm65282.2025.11059676 (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	5G	tracking/inference; 5G core security	Semi-passive	Not reported	Surveyed countermeasures and open challenges
S056	Z. Sun; C. Peng [76]	5G-HCLS: An Authentication Protocol to Protect Bootstrapping Messages in 5G Network	2025	IEEE Xplore; https://doi.org/10.1109/WCNC61545.2025.10978357 (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	Bootstrapping-message authentication; base-station authentication; subscriber protection	Active	Not reported	Authentication protocol proposed to protect 5G bootstrapping messages against fake-base-station attacks
S057	S. Fukuda; T. Akimoto; T. Hattori; Y. Murakami; H. Kawakami [34]	Applying Causal Inference to Quantify Effects of TA Allocation Optimization on Paging Load	2025	IEEE Xplore; https://doi.org/10.23919/icm65253.2025.11219122 (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	Not reported	Paging; tracking area /update; mobility/location management	Semi-passive	Not reported	Location-management, paging, or tracking mitigation/optimization discussed
S058	A. Tripathi; A. Rajput; A. K. Subudhi; K. Kondep; A. Thakur; B. R. Tamra [45]	Denial of Service Attacks Targeting Layer 2 in 5G RAN	2025	IEEE Xplore; https://doi.org/10.1109/fnw66845.2025.11317524 (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	authentication privacy; fake base station	Active	Not reported	Defense or mitigation discussed
S059	M. Saifuzzaman; K. Xie; T. Xie; X. Zhang; X. Lei [8]	Dissecting Privacy-Exposing Identifiers in 5G/4G Networks	2025	IEEE Xplore; https://doi.org/10.1109/dsc65356.2025.11260885 (accessed on 19 March 2026)	Identity and authentication privacy; Semi-passive	4G/5G	persistent or linkable identifiers; mobility/networking behavior correlation	Semi-passive	Not reported	Privacy-preserving identifier, pseudonym, SUCI/SUPI protection or protocol hardening
S060	I. J. Matheus Edward; H. Situmorang; S. N. Wijaya [1]	Exposing IMSI Vulnerabilities in 5G Non-Standalone Networks	2025	IEEE Xplore; https://doi.org/10.1109/icwt66752.2025.11181903 (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	IMSI/subscriber identity; SUCI/concealed identifier; rogue base station	Active	Not reported	Privacy-preserving identifier, pseudonym, SUCI/SUPI protection or protocol hardening
S061	M. Aoude [29]	Hardening 5G Network Registration: An Analysis of ECIES Profiles and SHNIP	2025	IEEE Xplore; https://doi.org/10.1109/actea66485.2025.11189931 (accessed on 19 March 2026)	Identity and authentication privacy; Passive	5G	IMSI/subscriber identity; SUCI/concealed identifier; authentication privacy	Passive	Not reported	Not reported
S062	M. Ouassia; M. Ouassia; A. Rhattay [63]	An Efficient and Secure Authentication and Key Agreement Protocol of LTE Mobile Network for an IoT System	2019	International Journal of Intelligent Engineering and Systems; https://doi.org/10.22266/ijies2019.0831.20 (accessed on 19 March 2026)	Identity and authentication privacy; Active	4G/LTE; IoT	authentication and key agreement; subscriber identity protection; mutual authentication; session-key establishment	Active	Computational cost; communication overhead; security-property comparison with existing authentication protocols	Lightweight mutual-authentication and key-agreement protocol designed to resist replay, impersonation and man-in-the-middle attacks
S063	S. Ramisetty; G. S. P. Ghantasala; R. Sharma R.; P. Vidyullatha; A. Sungheetha [68]	Mitigating Physical Layer Security Vulnerabilities in 4G and 5G Cellular Networks	2025	IEEE Xplore; https://doi.org/10.23919/indiacom66777.2025.11115596 (accessed on 19 March 2026)	Rogue/fake base stations; Active	4G/5G	IMSI/subscriber identity; authentication privacy; rogue base station	Active	Not reported	Not reported

Table A1. Cont.

ID	Authors	Title	Year	Source	Attack Type/Category	Generation	Exploited Mechanism	Adversary Model	Reported Metrics	Countermeasures/Solutions
S064	Q. Khan; S. Purification; S. -Y. Chang [61]	Post-Quantum Key Exchange and ID Encryption Analyses for 5G Mobile Networking	2025	IEEE Xplore; https://doi.org/10.1109/noms57970.2025.11073683 (accessed on 19 March 2026)	Identity and authentication privacy; Passive	5G	SUCI/concealed identifier; 5G core security; privacy	Passive	Not reported	Not reported
S065	R. P. Bhatt; S. Shetty; D. M.R.; S. N. P. [20]	Random Interleaving at MAC Layer for Privacy Protection in 6G RAN	2025	IEEE Xplore; https://doi.org/10.1109/smartnets65254.2025.11106854 (accessed on 19 March 2026)	Location tracking and mobility privacy; Active	6G	tracking/inference; signalling security; privacy	Active	Not reported	Privacy-preserving identifier, pseudonym, SUCI/SUPI protection or protocol hardening
S066	S. R. Hussain; O. Chowdhury; S. Mehnaz; E. Bertino [66]	LTInspector: A Systematic Approach for Adversarial Testing of 4G LTE	2018	NDSS Symposium; https://doi.org/10.14722/nds.s.2018.23313 (accessed on 19 March 2026)	Protocol and signalling security; Active	4G/LTE	LTE attach, authentication, paging, detach and mobility-management procedures; unauthenticated control-plane messages; protocol-state inconsistencies	Active	Ten new attacks identified; attacks affecting authentication, confidentiality, availability and location privacy	Formal model checking and adversarial testing; integrity protection for pre-authentication messages; correction of protocol-state weaknesses
S067	Y. Bi; C. Jia [36]	Towards Resilience 5G-V2N: Efficient and Privacy-Preserving Authentication Protocol for Multi-Service Access and Handover	2025	IEEE Xplore; https://doi.org/10.1109/tmc.2025.3532120 (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	authentication/key agreement; subscriber identity protection; handover security	Active	Not reported	Authentication/key-agreement or handover-security protocol proposed
S068	A. Szczegiński-Rekiel; K. Kanciak; J. M. Kelnar [16]	Zero-Knowledge Proof in 5G and Beyond Technologies: State of the Arts, Practical Aspects, Applications, Security Issues, Open Challenges, and Future Trends	2025	IEEE Xplore; https://doi.org/10.1109/accss.2025.3596122 (accessed on 19 March 2026)	Identity and authentication privacy; Active	5G	authentication privacy; tracking/inference; location privacy/inference	Active	Not reported	Surveyed countermeasures and open challenges
S069	Rajendra Patil and Zixu Tian and Mohan Gurusamy and Joshua McCloud [50]	5G core network control plane: Network security challenges and solution requirements	2025	ScienceDirect; https://doi.org/10.1016/j.comcom.2024.107982 (accessed on 19 March 2026)	Identity and authentication privacy; Passive	5G	authentication privacy; signalling security; 5G core security	Passive	Not reported	Not reported
S070	Andrea Paci and Matteo Chiacchia and Giuseppe Bianchi [85]	5GMap: Enabling external audits of access security and attach procedures in real-world cellular deployments	2025	ScienceDirect; https://doi.org/10.1016/j.comcom.2025.108091 (accessed on 19 March 2026)	Identity and authentication privacy; Active	5G	IMSI/subscriber identity; signalling security; privacy	Active	Not reported	Not reported
S071	Kinzah Noor, Agbotiname Lucky Imoize, Michael Adedosu Adelabu, Cheng-Chi Lee [21]	A Comprehensive Survey on AI-Assisted Multiple Access Enablers for 6G and beyond Wireless Networks	2025	ScienceDirect; https://doi.org/10.32604/cmes.2025.073200 (accessed on 19 March 2026)	General cellular security/privacy; Passive	6G	location privacy/inference; privacy	Not applicable/survey or review	Not reported	Surveyed countermeasures and open challenges
S072	Stefan Rommer and Catherine Mulligan and Peter Hedman and Magnus Olsson and Lars Frid and Shabnam Sultana [17]	Chapter 6 - Security	2025	ScienceDirect; https://doi.org/10.1016/b978-0-443-29188-3.00010-7 (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	Not reported	tracking/inference; location privacy/inference; privacy	Not applicable/survey or review	Not reported	Surveyed countermeasures and open challenges
S073	Yomna Ibrahim and Mai A. Abdel-Malek and Mohamed Azab and Mohamed RM Rizk [9]	Privacy-preserved mutually-trusted 5G communications in presence of pervasive attacks	2025	ScienceDirect; https://doi.org/10.1016/j.ijot.2025.101491 (accessed on 19 March 2026)	Identity and authentication privacy; Active	5G	5G-AKA/authentication; authentication privacy; location privacy/inference	Active	Not reported	Privacy-preserving identifier, pseudonym, SUCI/SUPI protection or protocol hardening
S074	James WrightStephen Wolthusen [55]	A Fail-Safe Challenge-Response Mechanism for User Equipment to Detect Rogue IMSI/SUPI Catchers	2025	SpringerLink; https://doi.org/10.1007/978-3-031-81888-2_8 (accessed on 19 March 2026)	Rogue/fake base stations; Active	Not reported	Rogue/fake base station; subscriber identity exposure; radio access security	Active	Not reported	Privacy-preserving identifier, pseudonym, SUCI/SUPI protection or protocol hardening
S075	Wenao ZhangShuhui ChenZiling WeiXinyu ZhangQianqian XingJinshu Su [59]	Cellular-Snooper: A General and Real-Time Mobile Application Fingerprinting Attack in LTE Networks	2025	SpringerLink; https://doi.org/10.1007/978-981-96-9872-1_4 (accessed on 19 March 2026)	Rogue/fake base stations; Semi-passive	4G/LTE	RF fingerprinting; signal features of base stations/devices	Semi-passive	Not reported	Not reported
S076	Julian Parkin andMahesh Tripunitara [73]	Countering Subscription Concealed Identifier (SUCI)-Catchers in Cellular Communications	2025	SpringerLink; https://doi.org/10.1007/978-3-031-80020-7_6 (accessed on 19 March 2026)	Rogue/fake base stations; Active	Not reported	Persistent or linkable identifiers; mobility/networking behavior correlation	Active	Not reported	Privacy-preserving identifier, pseudonym, SUCI/SUPI protection or protocol hardening

Table A1. Cont.

ID	Authors	Title	Year	Source	Attack Type/Category	Generation	Exploited Mechanism	Adversary Model	Reported Metrics	Countermeasures/Solutions
S077	K. SowjanyaPabitra PalAman VermaBijoy DasDhiman SahaAnand M. BaswadeBrajesh Lall [23]	SUPI-Rear: Privacy-Preserving Subscription Permanent Identification Strategy in 5G-AKA	2025	SpringerLink; https://doi.org/10.1007/978-3-031-74498-3_22 (accessed on 19 March 2026)	Identity and authentication privacy; Passive	5G	authentication/key agreement; subscriber identity protection; handover security	Passive	Not reported	Authentication/key-agreement or handover-security protocol proposed
S078	S. Feng; B. Cui; J. Fu; M. Jiang; S. Chang [58]	Adaptive Target Device Model Identification Attack in 5G Mobile Network	2026	IEEE Xplore; https://doi.org/10.1109/tnsm.2025.3626804 (accessed on 19 March 2026)	Protocol and signalling security; Passive	5G	signalling security	Passive	Not reported	Not reported
S079	S. Duan; F. Lyu; S. Wang; Y. Ding; X. He; Y. Zhang [52]	Exploring Cellular User Re-Identification Risks With Networking Behaviors Analysis and Modeling	2026	IEEE Xplore; https://doi.org/10.1109/tmc.2025.3607772 (accessed on 19 March 2026)	Location tracking and mobility privacy; Semi-passive	Not reported	Persistent or linkable identifiers; mobility/networking behavior correlation	Passive or semi-passive adversary using mobility/signalling/location data	Not reported	Not reported
S080	Y. Bi; C. Jia [38]	From Preparation to Execution: Security Protocol for Third-Party MES-Enabled 5G Support Handover Authentication and Key Evolution	2026	IEEE Xplore; https://doi.org/10.1109/tmc.2025.3599376 (accessed on 19 March 2026)	Rogue/fake base stations; Active	5G	authentication/key agreement; subscriber identity protection; handover security	Active	Not reported	Authentication/key-agreement or handover-security protocol proposed
S081	D. Scotece; G. Santaromita; C. Fiandrino; L. Foschini; D. Giustiniano [71]	On the Scalability of Access and Mobility Management Function: The Localization Management Function Use Case	2026	IEEE Xplore; https://doi.org/10.1109/tnsm.2026.3664546 (accessed on 19 March 2026)	Identity and authentication privacy; Semi-passive	Not reported	authentication privacy; location privacy/inference; signalling security	Semi-passive	Not reported	Detection, localization, or blacklisting method proposed
S082	T. N. Turnip; B. Andersen; C. Vargas-Rosales [75]	Toward 6G Authentication and Key Agreement Protocol: A Survey on Hybrid Post Quantum Cryptography	2026	IEEE Xplore; https://doi.org/10.1109/comst.2025.3567439 (accessed on 19 March 2026)	Identity and authentication privacy; Semi-passive	6G	authentication/key agreement; subscriber identity protection; handover security	Not applicable/survey or review	Not reported	Surveyed countermeasures and open challenges
S083	Muhammad Asim and Abdelhamied A. Ateya and Mudasir Ahmad Wani and Gauthar Ali and Mohammed [65]	A Comprehensive Survey on Blockchain-Enabled Techniques and Federated Learning for Secure 5G/6G Networks: Challenges, Opportunities, and Future Directions	2026	ScienceDirect; https://doi.org/10.32604/cmc.2025.070684 (accessed on 19 March 2026)	General cellular security/privacy; Active	5G/6G	privacy	Not applicable/survey or review	Not reported	Surveyed countermeasures and open challenges
S084	T. Fei; W. Wang [67]	LTE Is Vulnerable: Implementing Identity Spoofing and Denial-of-Service Attacks in LTE Networks	2019	IEEE Xplore; https://doi.org/10.1109/GLOBECOM38437.2019.9013397 (accessed on 19 March 2026)	Identity and authentication attacks; Active	4G/LTE	unprotected pre-authentication signalling; identity procedures; attach and authentication messages; LTE control-plane weaknesses	Active	Practical identity-spoofing and denial-of-service attacks implemented and evaluated in an LTE test environment	Integrity protection for initial signalling; stronger identity verification; authentication of pre-authentication control-plane messages
S085	M. Chlosta; D. Rupperecht; T. Holz; C. Pöpper [82]	LTE Security Disabled: Misconfiguration in Commercial Networks	2019	ACM Digital Library; https://doi.org/10.1145/3317549.3324927 (accessed on 19 March 2026)	Protocol and signalling security; Semi-passive	4G/LTE	null encryption and integrity configurations; weak or disabled LTE security algorithms; network-security misconfiguration	Semi-passive	Measurements of security configurations in commercial LTE networks; insecure deployments and disabled protection mechanisms identified	Correct network configuration; mandatory secure encryption and integrity algorithms; rejection of null or downgraded security configurations
S086	Jignesh B. JoshiSankita J. PatelBalu L. ParneVivaksha J. JariwalaVishruti V. Desai [14]	DS-AKA: Digital Signature-Based Authentication and Key Agreement Protocol to Mitigate Fake Serving Network for 5G Communication Networks	2026	SpringerLink; https://doi.org/10.1007/978-981-95-2196-8_9 (accessed on 19 March 2026)	Identity and authentication privacy; Passive	5G	authentication/key agreement; subscriber identity protection; handover security	Passive	Not reported	Authentication/key-agreement or handover-security protocol proposed

Appendix B. Quality Assessment

Table A2. Quality assessment results for each included study.

ID	QA1	QA2	QA3	QA4	QA5	QA6	QA7	QA8	QA9	QA10	QA11	QA12	Total	Category
S001	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S002	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S003	1	1	1	0.5	1	1	1	1	1	0	1	0.5	10	High
S004	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S005	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S006	1	0	1	0	1	0.5	0	0.5	0.5	0	0.5	0	5	Low
S007	1	1	0.5	1	1	1	1	1	1	1	1	1	11.5	High
S008	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S009	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S010	1	0	1	1	1	1	1	0.5	1	1	0.5	1	10	High
S011	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S012	1	0	1	1	1	1	1	0.5	1	1	0.5	1	10	High
S013	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S014	1	1	1	1	1	1	1	1	0.5	1	1	1	11.5	High
S015	1	0	1	1	1	1	1	0.5	1	1	1	1	10.5	High
S016	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S017	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S018	1	0	1	0	1	0.5	0	0.5	1	0	1	0	6	Low
S019	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S020	1	1	1	1	1	1	0.5	1	1	1	1	1	11.5	High
S021	1	1	0.5	1	1	1	0.5	1	1	1	1	1	11	High
S022	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S023	1	0	1	1	1	1	1	0.5	1	1	1	1	10.5	High
S024	1	0	1	1	1	1	1	0.5	1	1	0.5	1	10	High
S025	1	0	1	1	1	1	1	0.5	1	1	1	1	10.5	High
S026	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S027	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S028	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S029	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S030	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S031	1	0	1	0.5	1	0.5	0	0.5	1	1	1	0.5	8	Medium
S032	1	0	1	0.5	1	0.5	0	0.5	1	1	0.5	0.5	7.5	Medium
S033	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S034	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S035	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S036	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S037	1	0	1	1	1	1	1	0.5	1	1	0.5	1	10	High
S038	1	0	1	1	1	1	1	0.5	1	1	0.5	1	10	High
S039	1	0	1	0	1	0.5	0	0.5	1	0	0.5	0	5.5	Low
S040	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S041	1	1	1	1	1	1	1	1	1	1	1	1	12	High
S042	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S043	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S044	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S045	1	1	1	0	1	0.5	0	0.5	0.5	0	1	0	6.5	Low
S046	1	0	1	0.5	1	0.5	0	0.5	1	1	0.5	0.5	7.5	Medium
S047	1	0	1	0.5	1	0.5	0	0.5	1	1	0.5	0.5	7.5	Medium
S048	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S049	1	1	1	0.5	1	0.5	0	0.5	1	1	0.5	0.5	8.5	Medium
S050	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S051	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S052	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S053	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S054	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S055	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S056	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S057	1	0	1	0.5	1	0.5	0	0.5	1	1	1	0.5	8	Medium
S058	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S059	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S060	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S061	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S062	1	0	1	0	1	0.5	0	0.5	1	0	0.5	0	5.5	Low
S063	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S064	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S065	1	1	1	0.5	1	0.5	0	0.5	1	1	0.5	0.5	8.5	Medium
S066	1	0	1	0.5	1	0.5	0	0.5	1	1	1	0.5	8	Medium
S067	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S068	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S069	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S070	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S071	1	1	0.5	0.5	1	0.5	0	0.5	1	1	1	0.5	8.5	Medium
S072	0.5	0	0.5	0.5	1	0.5	0	0.5	1	1	0.5	0.5	6.5	Low
S073	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S074	1	0	1	0.5	1	0.5	0	0.5	1	1	1	0.5	8	Medium
S075	1	1	1	0	1	0.5	0	0.5	1	0	1	0	7	Medium
S076	1	0	1	0.5	1	0.5	0	0.5	1	1	1	0.5	8	Medium
S077	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S078	1	1	1	0	1	0.5	0	0.5	0.5	0	1	0	6.5	Low
S079	1	0	1	0	1	0.5	0	0.5	1	0	1	0	6	Low
S080	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium
S081	1	0	1	0.5	1	0.5	0	0.5	1	1	0.5	0.5	7.5	Medium
S082	1	1	0.5	0.5	1	0.5	0	0.5	1	1	0.5	0.5	8	Medium
S083	1	1	0.5	0.5	1	0.5	0	0.5	1	1	1	0.5	8.5	Medium
S084	1	0	1	0	1	0.5	0	0.5	1	0	1	0	6	Low
S085	1	0	1	0	1	0.5	0	0.5	1	0	0.5	0	5.5	Low
S086	1	1	1	0.5	1	0.5	0	0.5	1	1	1	0.5	9	Medium

Table A3. Distribution of included studies by QA score category.

QA Category	Score Interval	Number of Studies
High	10–12	24
Medium	7–9.5	52
Low	4–6.5	10
Very low	0–3.5	0

Appendix C. Cross-Generation Comparative Matrix

Table A4. Cross-generation comparative matrix of identification and location attacks in cellular networks.

Generation	Attack Vector	Affected Identifier	Exploited Procedure	Adversary Capability	Reported Metrics	Limitations	Mitigation	Representative Studies
2G	Passive or semi-passive paging observation	TMSI, IMSI, paging identity	Paging procedure and temporary identifier reuse	Passive or semi-passive adversary monitoring broadcast and control channels	Paging correlation, user presence detection, coarse location inference	Requires knowledge of paging occasions or repeated observations; accuracy depends on cell size and paging policy	Frequent TMSI reallocation; paging policy randomization; reduction of identifier reuse; monitoring abnormal paging patterns	[7,27,42]
2G	Fake base station/IMSI catcher	IMSI, TMSI	Location update, identity request, paging response	Active adversary operating a rogue BTS and attracting the UE	IMSI disclosure rate, attachment success, paging response, tracking feasibility	No mutual authentication; attack success depends on radio proximity, signal strength, and UE/operator configuration	Disable or restrict 2G where possible; operator-side anomaly detection; terminal warnings for suspicious cell behavior; stronger identity protection in later generations	[5,22,48]
2G	Silent SMS/signalling-triggered localization	TMSI, IMSI, MSISDN-linked identity	Paging, SMS delivery, mobility management signalling	Semi-active adversary capable of triggering network events and observing radio responses	Location confirmation, paging response timing, user reachability	Requires ability to trigger signalling events; localization granularity is usually limited to cell or location area	Filtering abnormal signalling triggers; operator-side SMS and paging abuse detection; improved subscriber privacy policies	[28,42,43]
3G	Paging and mobility-area tracking	TMSI, IMSI, location-area identifiers	Paging, routing area update, location area update	Passive or semi-passive adversary observing control-plane signalling	User presence detection, movement correlation, paging response behavior	Tracking precision depends on location area size, paging configuration, and identifier refresh frequency	More frequent temporary identifier refresh; optimized paging; mobility-management privacy controls; operator-side monitoring	[7,13,27]
3G	Rogue base station forcing identity exposure or downgrade	IMSI, TMSI	Cell selection, identity request, fallback to 2G	Active adversary with rogue base station capability and possible downgrade strategy	IMSI capture, downgrade success, attachment attempt behavior	3G introduces mutual authentication, but privacy may still be affected before full security activation or through fallback	Enforce mutual authentication; prevent unnecessary fallback to 2G; detect rogue cells; configure networks to avoid insecure interworking	[5,18,48]
3G	Authentication and AKA-related privacy analysis	IMSI, temporary identifiers, authentication vectors	Authentication and key agreement, identity request, resynchronization behavior	Passive, semi-passive, or active adversary depending on the scenario	Linkability, identity exposure, authentication failure behavior	Practical feasibility depends on implementation details and access to signalling observations	Strict implementation of AKA procedures; improved error handling; privacy-preserving authentication responses; avoidance of unnecessary permanent identity requests	[31,47,48]
4G	Paging-based location tracking	S-TMSI, GUTI, paging identity	Paging, tracking area update, idle-mode mobility	Passive or semi-passive adversary monitoring LTE control channels	Paging correlation, location-area inference, user presence detection, localization granularity	Requires repeated observations; accuracy depends on tracking area size and paging strategy	Frequent GUTI reallocation; paging obfuscation; optimized tracking area configuration; operator-side anomaly detection	[7,27,32,33]
4G	LTE rogue eNodeB/fake base station	IMSI, GUTI, S-TMSI	Attach, identity request, tracking area update, security mode setup	Active adversary operating rogue LTE equipment or modified SDR stack	IMSI disclosure, attach behavior, downgrade feasibility, UE response patterns	LTE improves authentication but some procedures before security activation remain privacy-sensitive	Minimize IMSI requests; enforce proper GUTI allocation; rogue-cell detection; baseband and network-side validation mechanisms	[22,30,66,67]
4G	Linkability through temporary identifier reuse	GUTI, S-TMSI	Attach, TAU, paging, idle-to-connected transition	Passive or semi-passive adversary correlating repeated identifiers or signalling patterns	Identifier lifetime, linkability rate, tracking duration	Effectiveness depends on operator policy for GUTI refresh and mobility patterns	Strict GUTI reallocation policies; shortened temporary identifier lifetime; unlinkability-aware mobility management	[8,15,53,66]

Table A4. Cont.

Generation	Attack Vector	Affected Identifier	Exploited Procedure	Adversary Capability	Reported Metrics	Limitations	Mitigation	Representative Studies
4G	Downgrade or interworking abuse	IMSI, TMSI, GUTI	CSFB, fallback to 2G/3G, inter-RAT mobility	Active adversary influencing radio conditions or exploiting interworking procedures	Downgrade success, identity exposure, service disruption indicators	Requires suitable network configuration and UE support for legacy RATs	Disable insecure fallback where possible; restrict 2G interworking; monitor abnormal RAT changes; prefer VoLTE/secure services	[18,22,48,82]
5G NSA	Fake base station or downgrade-assisted identification	IMSI, GUTI, S-TMSI, SUCI/SUPI depending on fallback path	LTE/NR interworking, fallback, identity request, registration-related signalling	Active adversary with rogue LTE/NR or downgrade capability	Identity exposure, fallback success, attach/registration response behavior	Attack feasibility depends heavily on deployment, UE configuration, and operator fallback policy	Restrict legacy fallback; validate network configurations; detect rogue cells; enforce privacy-preserving identity procedures	[1,18,22,46]
5G NSA	LTE anchor-based privacy exposure	GUTI, S-TMSI, 5G temporary identifiers depending on deployment	EN-DC operation, LTE attach, tracking area update, paging through LTE anchor	Passive, semi-passive, or active adversary targeting the LTE control-plane anchor	Paging correlation, temporary identifier linkability, tracking feasibility	5G NSA still depends on LTE/EPC or LTE control-plane elements, so some LTE privacy limitations persist	Strong LTE-side GUTI refresh; secure interworking policies; paging optimization; migration toward 5G SA where feasible	[1,8,22,60]
5G NSA	Paging and mobility tracking across LTE-NR deployment	GUTI, S-TMSI, paging identity	Paging, tracking area management, idle-mode mobility	Passive or semi-passive adversary observing LTE/NR signalling patterns	Presence detection, paging correlation, mobility-area inference	Granularity depends on tracking area design and paging strategy; NSA deployments may inherit LTE weaknesses	Temporary identifier rotation; optimized tracking area planning; paging randomization; operator-side monitoring of paging abuse	[7,39,40,51]
5G SA	Temporary identifier linkability	5G-GUTI, temporary UE identifiers	Registration update, paging, mobility management	Passive or semi-passive adversary correlating temporary identifiers or signalling events	Linkability duration, paging correlation, tracking feasibility	Risk persists if 5G-GUTI is not refreshed frequently or if paging behavior is predictable	Frequent 5G-GUTI rotation; unlinkability-aware AMF policies; paging optimization; privacy-preserving mobility management	[8,10,23,25]
5G SA	SUPI protection bypass or misconfiguration	SUPI, SUCI, 5G-GUTI	Registration, identity request, SUCI handling	Active adversary exploiting misconfiguration, implementation weakness, or forced identity procedure	SUPI exposure, SUCI misuse, registration failure behavior	5G introduces SUCI, but protection depends on correct home-network public key configuration and UE implementation	Correct SUCI configuration; home network public key validation; avoid null-scheme misuse; strict SUPI exposure policies	[29,47,48,73]
5G SA	Paging-based location and presence inference	5G-GUTI, paging identity	Paging, idle-mode reachability, registration area management	Passive or semi-passive adversary monitoring broadcast/control signalling	User presence detection, paging response behavior, coarse localization	Localization is generally coarse and depends on registration area size, paging configuration, and observation capability	Paging policy hardening; registration area optimization; reduction of predictable paging patterns; operator-side anomaly detection	[7,27,51,72]
5G SA	Implementation or deployment-specific privacy weakness	SUPI, SUCI, 5G-GUTI	Registration, authentication, paging, mobility management	Active or semi-active adversary exploiting vendor, configuration, or deployment weaknesses	Identity exposure, linkability, failed authentication behavior, tracking feasibility	Security guarantees depend on correct implementation and deployment; practical attacks may be operator- or device-specific	Conformance testing; implementation hardening; privacy audits; AMF policy enforcement; correct SUCI configuration and 5G-GUTI rotation	[31,47,50,85]

Appendix D. Full-Text Eligibility Exclusions

Table A5. Studies excluded during the full-text eligibility assessment.

Study ID	Citation	Applied Exclusion Criterion	Reason for Exclusion
S087	[87]	EC1	The study proposes a GPS-based forest-fire detection and alert system and does not investigate identification or location attacks targeting cellular-network users or protocols.
S088	[88]	EC1	The study develops a personal-safety device using fingerprint authentication and location reporting, rather than analyzing identification or location attacks in cellular networks.
S089	[89]	EC1	The study presents an IoT-based assistive walking stick for visually impaired users and does not examine cellular-network identification or location vulnerabilities.
S090	[90]	EC1	The study uses location tracking to support accident detection and emergency-response notification, without analyzing attacks against cellular-network location or identity mechanisms.
S091	[91]	EC1	The study presents a voice-activated distress-detection and location-reporting system and is unrelated to identification or location attacks in cellular networks.
S092	[92]	EC1	The study proposes an accident-detection, location-tracking, and notification application rather than an analysis of cellular identification or location attacks.
S093	[93]	EC1	The study develops a fall-detection and location-tracking system for elderly users and does not investigate cellular-network identity or location vulnerabilities.
S094	[94]	EC1	The study focuses on GPS navigation and live tracking for visually impaired travelers, rather than attacks exploiting cellular identification or location procedures.
S095	[95]	EC1	The study presents a tracking and fall-detection solution for elderly users and does not analyze identification or location attacks in cellular networks.
S096	[96]	EC1	The study concerns RFID-based identification and tracking of construction components, not the identification or location of subscribers in cellular networks.
S097	[97]	EC4/EC5	The study focuses on control and optimization intelligence for future 6G mobile networks and, therefore, falls outside the review scope limited to identification and location attacks in 2G–5G networks.
S098	[98]	EC4/EC5	The study investigates hybrid quantum-classical optimization for tracking-area management in future networks, rather than identification or location attacks within the 2G–5G scope.
S099	[99]	EC4/EC5	The study addresses NextG positioning resilience against relay jamming and is outside the review scope restricted to identification and location attacks in 2G–5G cellular networks.
S100	[100]	EC4/EC5	The study proposes a quantum-resistant blockchain architecture for vehicular networks and does not analyze identification or location attacks in 2G–5G cellular systems.
S101	[101]	EC4/EC5	The study concerns secure LoRa ad-hoc communications in coverage dead zones and is not focused on identification or location attacks in 2G–5G cellular networks.
S102	[102]	EC4/EC5	The study investigates privacy-aware query processing in vehicular ad-hoc networks rather than identification or location attacks involving 2G–5G cellular protocols.
S103	[103]	EC2	The study optimizes signaling-overhead costs in 5G networks but does not analyze an attack targeting subscriber identification or location confidentiality.
S104	[104]	EC2	The study proposes a mobility-management mechanism for reducing power consumption and signaling overhead in 5G IoT devices, without examining identification or location attacks.
S105	[105]	EC2	The study predicts mobility-management demand from user behavior for network-planning purposes and does not investigate attacks against cellular identity or location mechanisms.
S106	[106]	EC2	The study addresses mobility management for 5G network slicing but does not analyze adversarial identification or location tracking.
S107	[107]	EC2	The study focuses on the authenticity and verifiability of public-warning messages and does not investigate subscriber identification or location attacks.
S108	[108]	EC2	The study surveys mobility management in ultra-dense cellular networks but does not provide an analysis of identification or location attacks relevant to the review questions.
S109	[109]	EC2	The study optimizes 5G-MEC service relocation with performance, availability, and privacy objectives but does not analyze attacks against cellular subscriber identity or location.

Table A5. Cont.

Study ID	Citation	Applied Exclusion Criterion	Reason for Exclusion
S110	[110]	EC2	The study proposes O-RAN-based anomaly recognition and network sensing but does not specifically analyze identification or location attacks against cellular users.
S111	[111]	EC2	The study develops carrier-phase positioning methods for tracking XR devices and does not investigate adversarial location tracking or subscriber-identification attacks.
S112	[112]	EC2	The study proposes a seamless handover and mobility-management mechanism for device-to-device communication, without analyzing identification or location attacks.
S113	[113]	EC2	The study aims to reduce signaling overhead associated with IoT-device mobility and does not examine attacks against cellular identification or location procedures.
S114	[114]	EC2	The study proposes a paging-occasion allocation mechanism for beyond-5G networks but does not analyze paging-based identification or location attacks.
S115	[115]	EC2	The study presents a general intrusion-detection method for the 5G core but does not specifically analyze subscriber-identification or location attacks.
S116	[116]	EC2	The study uses aggregated mobile-network signaling data to observe road-freight traffic and does not examine adversarial identification or location attacks against subscribers.
S117	[117]	EC2	The study proposes a privacy-preserving authentication protocol for medical IoT devices but does not analyze identification or location attacks exploiting cellular-network procedures.
S118	[118]	EC2	The study proposes an enhanced authentication and key-agreement protocol for LTE/LTE-A IoT systems but does not investigate identification or location attacks.
S119	[119]	EC2	The study applies machine learning to tracking-area selection and handover security but does not provide an analysis of subscriber-identification or location-tracking attacks within the review scope.
S120	[120]	EC2	The study optimizes UAV trajectories and resource allocation in 5G networks and does not address identification or location attacks against cellular subscribers.
S121	[121]	EC2	The study proposes a blockchain-based data-privacy mechanism for industrial IoT environments but does not analyze cellular identification or location attacks.
S122	[122]	EC2/EC6	The publication is a short poster survey of general 5G-IoT security challenges and does not provide a sufficiently detailed analysis or evaluation of a specific identification or location attack.
S123	[123]	EC2/EC6	The study provides a broad conceptual discussion of trustworthy communications in NextG networks without a detailed technical analysis of a cellular identification or location attack.
S124	[124]	EC2/EC6	The study surveys public-safety communication technologies in terrorism scenarios but does not investigate identification or location attacks against cellular subscribers.
S125	[125]	EC2/EC6	The study examines the limitations of inferring device location from the nearest cellular antenna for mobility-data analysis, rather than an adversarial identification or location attack.
S126	[126]	EC2/EC6	The study proposes a privacy-preservation algorithm for location-based services but does not analyze an attack exploiting cellular-network identification or location procedures.
S127	[127]	EC2/EC6	The study proposes a differential-privacy method for protecting location datasets but does not investigate identification or location attacks at the cellular-protocol level.
S128	[128]	EC2/EC6	The study applies generative adversarial networks to enhance location privacy but does not provide an attack-specific analysis of cellular identification or location procedures.
S129	[129]	EC2/EC6	The study addresses privacy preservation in 5G-enabled mobile crowdsensing but does not analyze an identification or location attack against cellular-network users or signaling procedures.
S130	[130]	EC2/EC6	The study proposes a privacy-preserving contact-tracing architecture using 5G and blockchain but does not investigate cellular identification or location attacks.
S131	[131]	EC2/EC6	The study proposes a privacy-preserving framework for collecting location data in edge-computing systems but does not analyze attacks against cellular identity or location mechanisms.
S132	[132]	EC2/EC6	The study proposes privacy-preservation mechanisms for location and trajectory data in vehicular social-network services but does not investigate identification or location attacks at the cellular-protocol level.
S133	[133]	EC1	The study focuses on general cybersecurity measures for next-generation connected electric vehicles and does not provide a relevant technical analysis of identification or location attacks in 2G–5G cellular networks.

Appendix E. Performance Metrics by Attack Family

Table A6. Reported quantitative and operational metrics organized by attack family.

Attack Family	Representative Studies	Attack Success Rate or Impact	Localization Accuracy	Time to Success	Cost and Equipment Assumptions	Detectability	Deployment Conditions and Assumptions
Paging-based location and presence tracking	S015, S017, S019, S007, S025, S036, S012, S028, S075, S033, S034, S049, S073	Not reported as a common numerical success rate. Successful tracking was generally assessed through paging correlation, user-presence detection, or mobility-pattern recovery.	No common positioning-error metric was reported. The studies used indirect indicators such as paging correlation, signal strength, mobility patterns, or CRB-based privacy measures.	Not reported.	Passive or semi-passive monitoring of paging and control channels was assumed. Complete equipment specifications and monetary costs were not reported.	Not reported consistently. Repeated paging observations or artificially triggered paging events may be detectable through operator-side monitoring.	Requires observable paging traffic, repeated observations, and a sufficiently stable association between a temporary identifier and the target UE. Accuracy depends on cell size, tracking-area configuration, and paging policy.
Fake base station and IMSI-catcher attacks	S005, S044, S041, S068, S069, S048, S001, S017, S040	Not reported consistently. The reviewed studies generally demonstrated UE attraction, identity disclosure, attachment attempts, or paging responses, but did not provide a common numerical attack-success rate.	Not reported. Localization was generally limited to confirming that the target was located within the coverage area of the rogue cell.	Not reported.	An active rogue BTS, eNodeB, or gNodeB, usually implemented through software-defined radio equipment or a cellular test platform, was assumed. Complete monetary costs were generally not reported.	Not reported consistently. Detection may rely on abnormal cell parameters, unexpected signal-strength changes, invalid network identifiers, or network- and UE-side rogue-cell detection mechanisms.	Requires radio proximity, sufficient transmit power to attract or retain the UE, appropriate frequency and network configuration, and support for the targeted cellular generation or fallback procedure.
Silent-SMS and signalling-triggered localization	S036, S026, S037	Not reported as a common numerical success rate. Impact was evaluated through paging activation, reachability confirmation, or observable radio and mobility-management responses.	Generally limited to cell-, location-area-, tracking-area-, or registration-area-level inference. Exact distance errors were not reported.	Not reported.	Requires the ability to trigger an SMS, call, paging event, or another network-generated signalling transaction and to observe the corresponding radio response. Monetary cost was not reported.	Not reported. Repeated silent-SMS or paging triggers may be identifiable through operator-side anomaly detection or signalling-abuse monitoring.	Requires target reachability, successful generation of a network-triggered event, and access to the corresponding paging or mobility-management signalling.
Temporary-identifier linkability and reuse	S019, S068, S014, S008, S051, S001, S058, S041, S018, S045, S023	Not reported as a common numerical success rate. Effectiveness was evaluated through identifier correlation, mobility-pattern recovery, subscriber linkability, or tracking feasibility.	No common localization-error metric was reported. The achievable granularity depends on the cell, location area, tracking area, or registration area in which the identifier is observed.	Not reported.	Passive or semi-passive observation of paging, attachment, registration, and mobility-management signalling was assumed. Equipment costs were not reported.	Not reported consistently. Purely passive correlation may be difficult to detect because it does not require transmission by the adversary.	Requires temporary identifiers to remain unchanged or otherwise linkable across multiple signalling events. Feasibility depends strongly on operator policies for TMSI, GUTI, S-TMSI, and 5G-GUTI reallocation.
Downgrade and interworking attacks	S017, S084, S041, S044, S001, S040	Not reported consistently. The reviewed studies demonstrated downgrade feasibility, permanent-identity exposure, insecure fallback, or service degradation, but no common numerical downgrade-success rate was available.	Not reported. Location inference is generally obtained indirectly after the UE is forced onto a less secure radio access technology.	Not reported.	Requires an active radio adversary, rogue base-station capability, radio interference, or the ability to influence radio-access-technology selection. Complete monetary costs were not reported.	Not reported consistently. Abnormal RAT transitions, repeated fallback events, or suspicious neighboring cells may be detectable by the operator or UE.	Requires legacy RAT support, permissive fallback or interworking policies, suitable radio conditions, and a UE and operator configuration that permits inter-RAT mobility.
Authentication- and AKA-related privacy attacks	S042, S043, S044, S018, S045, S023, S074, S027	Not reported consistently. Reported impact included subscriber linkability, identity exposure, distinguishable authentication failures, or privacy leakage through authentication-related responses.	Not reported.	Not reported.	Passive, semi-passive, or active access to authentication and identity-related signalling was assumed, depending on the attack model. Equipment and monetary costs were generally not reported.	Not reported consistently. Detection may depend on identifying repeated authentication failures, unusual synchronization requests, or abnormal permanent identity requests.	Requires access to authentication, identity-request, resynchronization, or error-handling exchanges and may depend on protocol implementation and operator configuration.

Table A6. *Cont.*

Attack Family	Representative Studies	Attack Success Rate or Impact	Localization Accuracy	Time to Success	Cost and Equipment Assumptions	Detectability	Deployment Conditions and Assumptions
Signalling-overload and mobility-management attacks	S001, S008, S009, S013, S014, S033	Reported impact included 500–800 and up to 1500 messages per UE, 34% MME load events, and system collapse in approximately 30 s. Mitigation-oriented studies reported 92% signalling-overhead reduction, 8% fewer TAUs, 30% fewer paging requests, and more than 30% signalling-cost reduction.	Not applicable or not reported, because the primary objective was signalling load or service disruption rather than localization.	Approximately 30 s to system collapse was reported in S014. S033 used 100 GA runs and 300 stopping iterations, although these values describe algorithmic evaluation rather than direct attack execution time.	The studies assumed the ability to generate, amplify, or repeatedly trigger registration, attachment, paging, TAU, or other mobility-management procedures. Complete monetary equipment costs were not reported.	S014 reported a detection rate above 96% and a false-positive rate below 3.8%. Detectability was not reported consistently by the remaining studies.	Depends on the signalling volume, number of affected UEs, MME or AMF capacity, mobility behavior, paging configuration, tracking-area policy, and the adversary's ability to repeatedly trigger control-plane procedures.
Radio- and signal-based location inference	S015, S017, S024	A common numerical attack-success rate was not reported. Effectiveness was assessed using tracking feasibility, signal-derived indicators, spatial distributions, or detection probability.	No directly comparable distance-error metric was reported. Some studies used signal-strength measurements or CRB-derived privacy indicators instead of localization error.	Not reported.	Requires access to radio measurements, signal-strength information, carrier phase, or control-channel observations. Hardware configurations and monetary costs were not consistently reported.	S024 reported detection probabilities close to 1 for NCD and MNCD and below 0.5 for SpD. Other studies did not report consistent detection-rate or false-positive-rate values.	Depends on propagation conditions, target mobility, cell geometry, measurement density, observation duration, and the availability of radio or spatial-distribution information.
Paging- and control-plane anomaly detection	S014, S024	The studies primarily evaluated attack-detection or mitigation effectiveness rather than direct attack-success rates. S014 reported a detection rate above 96%, while S024 reported detection probability values for different indicators.	Not applicable or not reported.	Not reported as attack time. Detection and processing times were not reported consistently.	Assumes access to operator-side signalling traces, radio observations, or control-plane measurements and sufficient computational resources for anomaly analysis. Monetary costs were not reported.	Detection rate above 96% and false-positive rate below 3.8% were reported in S014. Detection probability was close to 1 for NCD and MNCD and below 0.5 for SpD in S024.	Performance depends on the availability and quality of signalling data, selection of detection thresholds, attack intensity, network configuration, training data, and the representativeness of normal traffic.
SUPI/SUCI protection and permanent-identity exposure	S001, S043, S044, S045, S023, S074, S027	Not reported consistently. The reported impact included SUPi exposure, incorrect SUCI processing, use of an unprotected identity scheme, registration failure, or permanent-identity disclosure.	Not reported.	Not reported.	Requires active interaction with registration or identity procedures, access to a rogue or misconfigured network, or exploitation of implementation and configuration weaknesses. Monetary cost was not reported.	Not reported consistently. Detection may depend on registration logs, invalid SUCI use, repeated identity requests, or home-network validation mechanisms.	Depends on correct home-network public-key configuration, UE implementation, SUCI protection-scheme selection, operator policy, and the prevention of unnecessary SUPi requests.
Implementation- and deployment-specific privacy weaknesses	S042, S043, S086, S047	Not reported consistently. Demonstrated impact included identity exposure, temporary-identifier linkability, authentication failure behavior, paging correlation, or tracking feasibility.	Not reported.	Not reported.	Requires access to vulnerable devices, operator configurations, protocol implementations, or registration and mobility-management exchanges. Complete monetary costs were not reported.	Not reported consistently. Detectability depends on vendor logging, conformance testing, privacy audits, and network-side anomaly detection.	Feasibility is vendor-, UE-, operator-, and deployment-specific and may depend on incorrect SUCI configuration, insufficient temporary-identifier rotation, predictable paging behavior, or non-compliant protocol implementation.

References

1. Matheus Edward, I.J.; Situmorang, H.; Wijaya, S.N. Exposing IMSI Vulnerabilities in 5G Non-Standalone Networks. In Proceedings of the 2025 11th International Conference on Wireless and Telematics (ICWT), Lampung, Indonesia, 3–4 July 2025. <https://doi.org/10.1109/ICWT66752.2025.11181903>.
2. Karim, I.; Hussain, S.R.; Bertino, E. ProChecker: An Automated Security and Privacy Analysis Framework for 4G LTE Protocol Implementations. In Proceedings of the 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), Virtual Conference, 7–10 July 2021; pp. 773–785. <https://doi.org/10.1109/ICDCS51616.2021.00079>.
3. Yu, C.; Chen, S.; Xing, Q.; Wei, Z. Protecting unauthenticated messages in LTE/5G mobile networks: A two-level Hierarchical Identity-Based Signature (HIBS) solution. *Comput. Netw.* **2024**, *254*, 110814. <https://doi.org/10.1016/j.comnet.2024.110814>.
4. Checa, J.J.; Tomasini, S. Location-Privacy-Preserving Technique for 5G mmWave Devices. *IEEE Commun. Lett.* **2020**, *24*, 2692–2695. <https://doi.org/10.1109/lcomm.2020.3018165>.
5. Abdelrazek, L.; Azer, M.A. User Privacy in Legacy Mobile Network Protocols. In Proceedings of the 2018 3rd International Conference on System Reliability and Safety (ICSRS), Barcelona, Spain, 23–25 November 2018. <https://doi.org/10.1109/ICSRS.2018.8688870>.
6. Braeken, A. Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability. *Comput. Netw.* **2020**, *181*, 107424. <https://doi.org/10.1016/j.comnet.2020.107424>.
7. Alsaeedy, A.A.R.; Chong, E.K.P. Tracking Area Update and Paging in 5G Networks: A Survey of Problems and Solutions. *Mob. Netw. Appl.* **2019**, *24*, 578–595. <https://doi.org/10.1007/s11036-018-1160-6>.
8. Saifuzzaman, M.; Xie, K.; Xie, T.; Zhang, X.; Lei, X. Dissecting Privacy-Exposing Identifiers in 5G/4G Networks. In Proceedings of the 2025 IEEE Conference on Dependable and Secure Computing (DSC), Taipei, Taiwan, 18–20 October 2025. <https://doi.org/10.1109/DSC65356.2025.11260885>.
9. Ibrahim, Y.; Abdel-Malek, M.A.; Azab, M.; Rizk, M.R. Privacy-preserved mutually-trusted 5G communications in presence of pervasive attacks. *Internet Things* **2025**, *30*, 101491. <https://doi.org/10.1016/j.iot.2025.101491>.
10. Damir, M.T.; Niemi, V. Location Privacy, 5G AKA, and Enhancements. In *Secure IT Systems*; Springer: Cham, Switzerland, 2022. https://doi.org/10.1007/978-3-031-22295-5_3.
11. Yang, L.; Weng, C.-E.; Chen, H.-C.; Chen, Y.-C.-K.; Yao, Y.-C. Attacks and Threats Verification Based on 4G/5G Security Architecture. In *Innovative Mobile and Internet Services in Ubiquitous Computing*; Springer: Cham, Switzerland, 2023; pp. 240–249. https://doi.org/10.1007/978-3-031-35836-4_26.
12. Fan, W.; Shi, B.; Peng, C. NReplay: 5G Key Reinstallation Attack Based on NAS Layer Vulnerabilities. In Proceedings of the MILCOM 2024—2024 IEEE Military Communications Conference (MILCOM), Washington, DC, USA, 28 October–1 November 2024. <https://doi.org/10.1109/milcom61039.2024.10773741>.
13. Qi, H.; Shen, Y.; Yin, B. Intelligent Trajectory Inference Through Cellular Signaling Data. *IEEE Trans. Cogn. Commun. Netw.* **2020**, *6*, 586–596. <https://doi.org/10.1109/tccn.2019.2961660>.
14. Joshi, J.B.; Patel, S.J.; Parne, B.L.; Jariwala, V.J.; Desai, V.V. DS-AKA: Digital Signature-Based Authentication and Key Agreement Protocol to Mitigate Fake Serving Network for 5G Communication Networks. In *Information Security, Privacy and Digital Forensics*; Springer: Singapore, 2026; pp. 151–163. https://doi.org/10.1007/978-981-95-2196-8_9.
15. Kim, H.; Lee, J.; Lee, E.; Kim, Y. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1153–1168. <https://doi.org/10.1109/SP.2019.00038>.
16. Szczegielniak-Rekiel, A.; Kanciak, K.; Kelner, J.M. Zero-Knowledge Proof in 5G and Beyond Technologies: State of the Arts, Practical Aspects, Applications, Security Issues, Open Challenges, and Future Trends. *IEEE Access* **2025**, *13*, 138352–138380. <https://doi.org/10.1109/ACCESS.2025.3596122>.
17. Rommer, S.; Mulligan, C.; Hedman, P.; Olsson, M.; Frid, L.; Sultana, S. Chapter 6—Security. In *The Core Network for 5G Advanced*, 2nd ed.; Elsevier: Amsterdam, The Netherlands, 2025. <https://doi.org/10.1016/B978-0-443-29188-3.00010-7>.
18. Khan, M.; Ginzboorg, P.; Järvinen, K.; Niemi, V. Defeating the Downgrade Attack on Identity Privacy in 5G. In *Security Standardisation Research*; Springer: Cham, Switzerland, 2018. https://doi.org/10.1007/978-3-030-04762-7_6.
19. Dixit, U.; Vittal, S.; A, A.F. A Systematic Study for Understanding the Security Risks in 5G Core Network. In Proceedings of the 2024 16th International Conference on COMMunication Systems & NETworks (COMSNETS), Bengaluru, India, 3–7 January 2024. <https://doi.org/10.1109/comsnets59351.2024.10427440>.
20. Bhatt, R.P.; Shetty, S.; S. N. P., D.M.R. Random Interleaving at MAC Layer for Privacy Protection in 6G RAN. In Proceedings of the 2025 International Conference on Smart Applications, Communications and Networking (SmartNets), Istanbul, Türkiye, 22–24 July 2025. <https://doi.org/10.1109/SmartNets65254.2025.11106854>.
21. Noor, K.; Imoize, A.L.; Adelabu, M.A. A Comprehensive Survey on AI-Assisted Multiple Access Enablers for 6G and beyond Wireless Networks. *CMES-Comput. Model. Eng. Sci.* **2025**, *145*, 1575–1664. <https://doi.org/10.32604/cmes.2025.073200>.

22. Palamà, I.; Gringoli, F.; Bianchi, G.; Blefari-Melazzi, N. IMSI Catchers in the wild: A real world 4G/5G assessment. *Comput. Netw.* **2021**, *194*, 108137. <https://doi.org/10.1016/j.comnet.2021.108137>.
23. Sowjanya, K.; Pal, P.; Verma, A.; Das, B.; Saha, D.; Baswade, A.M.; Lall, B. SUPI-Rear: Privacy-Preserving Subscription Permanent Identification Strategy in 5G-AKA. In *Stabilization, Safety, and Security of Distributed Systems*; Springer: Cham, Switzerland, 2025. https://doi.org/10.1007/978-3-031-74498-3_22.
24. Bang, I.; Kim, T.; Jang, H.S.; Sung, D.K. Impact of Uplink Power Control on User Location Tracking Attacks in Cellular Network. In Proceedings of the ICC 2021—IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021. <https://doi.org/10.1109/ICC42927.2021.9500553>.
25. Liu, F.; Su, L.; Yang, B.; Du, H.; Qi, M.; He, S. Security Enhancements to Subscriber Privacy Protection Scheme in 5G Systems. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin, China, 28 June–2 July 2021; pp. 451–456. <https://doi.org/10.1109/IWCMC51323.2021.9498591>.
26. Yang, T.; Wang, S.; Zhan, B.; Zhan, N.; Li, J.; Xiang, S.; Xiang, Z.; Mao, B. Formal Analysis of 5G Authentication and Key Management for Applications (AKMA). *J. Syst. Archit.* **2022**, *126*, 102478. <https://doi.org/10.1016/j.sysarc.2022.102478>.
27. Sivasankar, S.; Challa, R. Closed Loop Paging Optimization for Efficient Mobility Management. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021. <https://doi.org/10.1109/CCNC49032.2021.9369589>.
28. Ghannam, R.; Sharevski, F.; Chung, A. User-targeted Denial-of-Service Attacks in LTE Mobile Networks. In Proceedings of the 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Limassol, Cyprus, 15–17 October 2018. <https://doi.org/10.1109/wimob.2018.8589140>.
29. Aoude, M. Hardening 5G Network Registration: An Analysis of ECIES Profiles and SHNIP. In Proceedings of the 2025 Sixth International Conference on Advances in Computational Tools for Engineering Applications (ACTEA), Zouk Mosbeh, Lebanon, 24–26 September 2025. <https://doi.org/10.1109/ACTEA66485.2025.11189931>.
30. Fardan, I.; Mawaldi, I.; Anugraha, T.; Ginting, I.; Karna, N. Experimental Security Analysis for Fake eNodeB Attack on LTE Network. In Proceedings of the 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 10 December 2020; pp. 140–145. <https://doi.org/10.1109/ISRITI51436.2020.9315427>.
31. Fei, T.; Wang, W. The vulnerability and enhancement of AKA protocol for mobile authentication in LTE/5G networks. *Comput. Netw.* **2023**, *228*, 109685. <https://doi.org/10.1016/j.comnet.2023.109685>.
32. Hashim, H.A.; Abido, M.A. Location management in LTE networks using multi-objective particle swarm optimization. *Comput. Netw.* **2019**, *157*, 78–88. <https://doi.org/10.1016/j.comnet.2019.04.009>.
33. Bang, I.; Kim, T.; Jang, H.S.; Sung, D.K. An Opportunistic Power Control Scheme for Mitigating User Location Tracking Attacks in Cellular Networks. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1131–1144. <https://doi.org/10.1109/tifs.2022.3152403>.
34. Fukuda, S.; Akimoto, T.; Hattori, T.; Murakami, Y.; Kawakami, H. Applying Causal Inference to Quantify Effects of TA Allocation Optimization on Paging Load. In Proceedings of the 2025 Fifteenth International Conference on Mobile Computing and Ubiquitous Networking (ICMU), Busan, Republic of Korea, 10–12 September 2025. <https://doi.org/10.23919/icmu65253.2025.11219122>.
35. Singh, G.; Shrimankar, D. A Privacy-Preserving Authentication Protocol with Secure Handovers for the LTE/LTE-A Networks. *Sādhanā* **2018**, *43*, 128. <https://doi.org/10.1007/s12046-018-0891-1>.
36. Bi, Y.; Jia, C. Towards Resilience 5G-V2N: Efficient and Privacy-Preserving Authentication Protocol for Multi-Service Access and Handover. *IEEE Trans. Mob. Comput.* **2025**, *24*, 5446–5463. <https://doi.org/10.1109/TMC.2025.3532120>.
37. Ali, A.; Fischer, G. Symbol-Based Statistical RF Fingerprinting for Fake Base Station Identification. In Proceedings of the 2019 29th International Conference Radioelektronika (RADIOELEKTRONIKA), Pardubice, Czech Republic, 16–18 April 2019; pp. 1–5. <https://doi.org/10.1109/RADIOELEK.2019.8733585>.
38. Bi, Y.; Jia, C. From Preparation to Execution: Security Protocol for Third-Party MES-Enabled 5G Support Handover Authentication and Key Evolution. *IEEE Trans. Mob. Comput.* **2026**, *25*, 1009–1026. <https://doi.org/10.1109/tmc.2025.3599376>.
39. Aamer, B.; Chergui, H.; Benjillali, M. Clustering-Enabled Tracking Areas Design for Beyond-5G Networks: A Live Network Demo. In Proceedings of the 2023 International Wireless Communications and Mobile Computing (IWCMC), Marrakesh, Morocco, 19–23 June 2023; pp. 375–379. <https://doi.org/10.1109/IWCMC58020.2023.10182686>.
40. Aamer, B.; Chergui, H.; Chergui, N.; Tourki, K.; Benjillali, M.; Verikoukis, C.; Debbah, M. Self-Tuning Spectral Clustering for Adaptive Tracking Areas Design in 5G Ultra-Dense Networks. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019. <https://doi.org/10.1109/wcnc.2019.8885586>.
41. Escudero-Andreu, G.; Kyriakopoulos, K.; Flint, J.A.; Lambrotharan, S. Detecting Signalling DoS Attacks on LTE Networks. In *Industrial Networks and Intelligent Systems*; Springer: Cham, Switzerland, 2019; pp. 283–301. https://doi.org/10.1007/978-3-030-30149-1_23.
42. Pavloski, M. Signalling Attacks in Mobile Telephony. In *Security in Computer and Information Sciences*; Springer: Cham, Switzerland, 2018; pp. 130–141. https://doi.org/10.1007/978-3-319-95189-8_12.

43. Yu, C.; Chen, S.; Cai, Z. LTE phone number catcher: A practical attack against mobile privacy. *Secur. Commun. Netw.* **2019**, 2019, 7425235. <https://doi.org/10.1155/2019/7425235>.
44. Zhao, J.; Li, Q.; Yuan, Z.; Zhang, Z.; Lu, S. 5G Messaging: System Insecurity and Defenses. In Proceedings of the 2022 IEEE Conference on Communications and Network Security (CNS), Austin, TX, USA, 3–5 October 2022. <https://doi.org/10.1109/cns56114.2022.9947238>.
45. Tripathi, A.; Rajput, A.; Subudhi, A.K.; Kondepu, K.; Thakur, A.; Tamma, B.R. Denial of Service Attacks Targeting Layer 2 in 5G RAN. In Proceedings of the 2025 IEEE Future Networks World Forum (FNWF), Bengaluru, India, 10–12 November 2025; pp. 1–6. <https://doi.org/10.1109/FNWF66845.2025.11317524>.
46. Saedi, M.; Moore, A.; Perry, P.; Shojaifar, M.; Ullah, H.; Synnott, J.; Brown, R.; Herwono, I. Generation of Realistic Signal Strength Measurements for a 5G Rogue Base Station Attack Scenario. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020; pp. 1–7. <https://doi.org/10.1109/CNS48642.2020.9162275>.
47. Koutsos, A. The 5G-AKA Authentication Protocol Privacy. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; pp. 464–479. <https://doi.org/10.1109/EuroSP.2019.00041>.
48. Khan, H.; Martin, K.M. A survey of subscription privacy on the 5G radio interface—the past, present and future. *J. Inf. Secur. Appl.* **2020**, 53, 102537. <https://doi.org/10.1016/j.jisa.2020.102537>.
49. Huang, J.-H.; Cheng, S.-M.; Kaliski, R.; Hung, C.-F. Developing xApps for Rogue Base Station Detection in SDR-Enabled O-RAN. In Proceedings of the IEEE INFOCOM 2023—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Hoboken, NJ, USA, 20 May 2023; pp. 1–6. <https://doi.org/10.1109/INFOCOMWKSHPS57453.2023.10225868>.
50. Patil, R.; Tian, Z.; Gurusamy, M.; McCloud, J. 5G Core Network Control Plane: Network Security Challenges and Solution Requirements. *Comput. Commun.* **2025**, 229, 107982. <https://doi.org/10.1016/j.comcom.2024.107982>.
51. Oliveira, L.A.N.; Alencar, M.S.; Lopes, W.T.A.; Madeiro, F. On the Performance of Location Management in 5G Network Using RRC Inactive State. *IEEE Access* **2022**, 10, 65520–65532. <https://doi.org/10.1109/access.2022.3178383>.
52. Duan, S.; Lyu, F.; Wang, S.; Ding, Y.; He, X.; Zhang, Y. Exploring Cellular User Re-Identification Risks With Networking Behaviors Analysis and Modeling. *IEEE Trans. Mob. Comput.* **2026**, 25, 2462–2479. <https://doi.org/10.1109/TMC.2025.3607772>.
53. Xu, F.; Tu, Z.; Li, Y. Connecting the Dots: User Privacy Is Not Preserved in ID-Removed Cellular Data. *IEEE Trans. Netw. Serv. Manag.* **2020**, 17, 147–159. <https://doi.org/10.1109/TNSM.2019.2926488>.
54. Tedeschini, B.C.; Kwon, G.; Nicoli, M.; Win, M.Z. Real-Time Bayesian Neural Networks for 6G Cooperative Positioning and Tracking. *IEEE J. Sel. Areas Commun.* **2024**, 42, 2322–2338. <https://doi.org/10.1109/JSAC.2024.3413950>.
55. Wright, J.; Wolthusen, S. A Fail-Safe Challenge-Response Mechanism for User Equipment to Detect Rogue IMSI/SUPI Catchers. In *Critical Infrastructure Protection XVIII*; Springer: Cham, Switzerland, 2025; pp. 155–178. https://doi.org/10.1007/978-3-031-81888-2_8.
56. Triesch, A.; Barsch, T.; Moonsamy, V.; Große-Kampmann, M. 5G Under Siege: A Comprehensive Guide to Threats and Penetration Testing in 5G Campus Networks. In Proceedings of the 2025 International Wireless Communications and Mobile Computing Conference (IWCMC), Abu Dhabi, United Arab Emirates, 12–16 May 2025; pp. 1312–1317. <https://doi.org/10.1109/IWCMC65282.2025.11059676>.
57. Orlando, D.; Palamà, I.; Bartoletti, S.; Bianchi, G.; Melazzi, N.B. Design and Experimental Assessment of Detection Schemes for Air Interface Attacks in Adverse Scenarios. *IEEE Wirel. Commun. Lett.* **2021**, 10, 1989–1993. <https://doi.org/10.1109/lwc.2021.3089636>.
58. Feng, S.; Cui, B.; Fu, J.; Jiang, M.; Chang, S. Adaptive Target Device Model Identification Attack in 5G Mobile Network. *IEEE Trans. Netw. Serv. Manag.* **2026**, 23, 1028–1042. <https://doi.org/10.1109/tnsm.2025.3626804>.
59. Zhang, W.; Chen, S.; Wei, Z.; Zhang, X.; Xing, Q.; Su, J. Cellular-Snooper: A General and Real-Time Mobile Application Fingerprinting Attack in LTE Networks. In *Advanced Intelligent Computing Technology and Applications*; Springer: Singapore, 2025; pp. 39–53. https://doi.org/10.1007/978-981-96-9872-1_4.
60. Fraunholz, D.; Brunke, D.; Dumanski, L.; Koenig, H. Automating Device Fingerprinting Attacks in 4G and 5G NSA Mobile Networks. In *Foundations and Practice of Security*; Springer: Cham, Switzerland, 2023; pp. 192–207. https://doi.org/10.1007/978-3-031-30122-3_12.
61. Khan, Q.; Purification, S.; Chang, S.-Y. Post-Quantum Key Exchange and ID Encryption Analyses for 5G Mobile Networking. In Proceedings of the NOMS 2025—2025 IEEE/IFIP Network Operations and Management Symposium, Honolulu, HI, USA, 12–16 May 2025; pp. 1–9. <https://doi.org/10.1109/NOMS57970.2025.11073683>.
62. Haddad, Z. Enhancing Privacy and Security in 5G Networks with an Anonymous Handover Protocol Based on Blockchain and Zero Knowledge Proof. *Comput. Netw.* **2024**, 250, 110544. <https://doi.org/10.1016/j.comnet.2024.110544>.
63. Ouaisa, M.; Ouaisa, M.; Rhattoy, A. An efficient and secure authentication and key agreement protocol of LTE mobile network for an IoT system. *Int. J. Intell. Eng. Syst.* **2019**, 12, 212–222. <https://doi.org/10.22266/ijies2019.0831.20>.
64. Sun, S.; Abualhaol, I.; Poitau, G.; Esswie, A.; Repeta, M. An Ensemble Approach for Fake Base Station Detection Using Temporal Graph Analysis and Anomaly Detection. In Proceedings of the 2024 Wireless Telecommunications Symposium (WTS), Oakland, CA, USA, 10–12 April 2024; pp. 1–6. <https://doi.org/10.1109/WTS60164.2024.10536680>.

65. Asim, M.; Ateya, A.A.; Wani, M.A.; Ali, G.; ElAffendi, M.; Abd El-Latif, A.A.; Siyal, R. A Comprehensive Survey on Blockchain-Enabled Techniques and Federated Learning for Secure 5G/6G Networks: Challenges, Opportunities, and Future Directions. *Comput. Mater. Contin.* **2026**, *86*, 3. <https://doi.org/10.32604/cmc.2025.070684>.
66. Hussain, S.; Chowdhury, O.; Mehnaz, S.; Bertino, E. LTEInspector: A systematic approach for adversarial testing of 4G LTE. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2018, San Diego, CA, USA, 18–21 February 2018. <https://doi.org/10.14722/ndss.2018.23313>.
67. Fei, T.; Wang, W. LTE Is Vulnerable: Implementing Identity Spoofing and Denial-of-Service Attacks in LTE Networks. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6. <https://doi.org/10.1109/GLOBECOM38437.2019.9013397>.
68. Ramisetty, S.; Ghantasala, G.S.P.; Sharma, R.R.; Vidyullatha, P.; Sungheetha, A. Mitigating Physical Layer Security Vulnerabilities in 4G and 5G Cellular Networks. In Proceedings of the 2025 12th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2–4 April 2025. <https://doi.org/10.23919/INDIACom66777.2025.11115596>.
69. Zhang, T.; Xiao, M.; Ouyang, R. Proving Mutual Authentication Property of 5G-AKA Protocol Based on PCL. In *Theoretical Computer Science*; Springer: Singapore, 2021; pp. 222–233. https://doi.org/10.1007/978-981-16-7443-3_13.
70. Pauliac, M. USIM in 5G Era. *J. ICT Stand.* **2020**, *8*, 29–40. <https://doi.org/10.13052/jicts2245-800x.813>.
71. Scotece, D.; Santaromita, G.; Fiandrino, C.; Foschini, L.; Giustiniano, D. On the Scalability of Access and Mobility Management Function: The Localization Management Function Use Case. *IEEE Trans. Netw. Serv. Manag.* **2026**, *23*, 2624–2635. <https://doi.org/10.1109/TNSM.2026.3664546>.
72. Alsaedy, A.A.R.; Chong, E.K.P. Tracking Area Update Procedure Unnecessary in 5G: Improving User Experience and Offloading Signaling Overhead. In Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 8–10 November 2018; pp. 967–973. <https://doi.org/10.1109/UEMCON.2018.8796728>.
73. Parkin, J.; Tripunitara, M. Countering Subscription Concealed Identifier (SUCI)-Catchers in Cellular Communications. In Proceedings of the 20th International Conference on Information Systems Security (ICISS 2024), Jaipur, India, 16–20 December 2024; Springer: Cham, Switzerland, 2025; pp. 107–126. https://doi.org/10.1007/978-3-031-80020-7_6.
74. Kriaa, S.; Feki, A.; Papillon, S.; Chene, T.; Ouattara, I. Detecting Fake Base Stations Using Knowledge Graphs and ML-Based Techniques. In Proceedings of the 2023 IEEE Virtual Conference on Communications (VCC), Online, 28–30 November 2023; pp. 37–42. <https://doi.org/10.1109/VCC60689.2023.10474891>.
75. Turnip, T.N.; Andersen, B.; Vargas-Rosales, C. Towards 6G Authentication and Key Agreement Protocol: A Survey on Hybrid Post-Quantum Cryptography. *IEEE Commun. Surv. Tutor.* **2025**, *28*, 3311–3345. <https://doi.org/10.1109/COMST.2025.3567439>.
76. Sun, Z.; Peng, C. 5G-HCLS: An Authentication Protocol to Protect Bootstrapping Messages in 5G Network. In Proceedings of the 2025 IEEE Wireless Communications and Networking Conference (WCNC), Milan, Italy, 24–27 March 2025; pp. 1–6. <https://doi.org/10.1109/WCNC61545.2025.10978357>.
77. Haddad, Z. Blockchain-enabled anonymous mutual authentication and location privacy-preserving scheme for 5G networks. *J. King Saud. Univ.-Comput. Inf. Sci.* **2023**, *35*, 101458. <https://doi.org/10.1016/j.jksuci.2022.11.018>.
78. Shin, J.; Shin, Y.; Park, J.-G. Network Detection of Fake Base Station Using Automatic Neighbour Relation in Self-Organizing Networks. In Proceedings of the 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 19–21 October 2022; pp. 968–970. <https://doi.org/10.1109/ICTC55196.2022.9952901>.
79. Ali, A.; Fischer, G. The Phase Noise and Clock Synchronous Carrier Frequency Offset Based RF Fingerprinting for the Fake Base Station Detection. In Proceedings of the 2019 IEEE 20th Wireless and Microwave Technology Conference (WAMICON), Cocoa Beach, FL, USA, 8–9 April 2019; pp. 1–6. <https://doi.org/10.1109/WAMICON.2019.8765471>.
80. Butad, D.; Tao, S.M.; Tudtud, H.; Macapagal, A.J.; Astillo, P.V.; Choudhary, G.; Dragoni, N. Fake Base Station Detection and Localization in 5G Network: A Proof of Concept. In *Mobile Internet Security*; Springer: Singapore, 2024; pp. 3–17. https://doi.org/10.1007/978-981-97-4465-7_1.
81. Purification, S.; Park, K.; Kim, J.; Kim, J.; Chang, S.-Y. Wireless Link Routing to Secure Against Fake Base Station in 5G. In Proceedings of the 2024 Silicon Valley Cybersecurity Conference (SVCC), Seoul, Republic of Korea, 17–19 June 2024. <https://doi.org/10.1109/SVCC61185.2024.10637367>.
82. Chlost, M.; Rupprecht, D.; Holz, T.; Pöpper, C. LTE security disabled: Misconfiguration in commercial networks. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 261–266. <https://doi.org/10.1145/3317549.3324927>.
83. Basheer, S.; Kumar, G.; Nalband, A.H.; Raveendran, C. Securing 5G Networks: Strategies for Prevention, Detection, and Mitigation of Rogue Base Stations. In Proceedings of the 2023 Fourth International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 8–9 December 2023. <https://doi.org/10.1109/icstcee60504.2023.10585168>.

84. Purification, S.; Wuthier, S.; Kim, J.; Kim, J.; Chang, S.-Y. Fake Base Station Detection and Blacklisting. In Proceedings of the 2024 33rd International Conference on Computer Communications and Networks (ICCCN), Kailua-Kona, HI, USA, 29–31 July 2024. <https://doi.org/10.1109/icccn61486.2024.10637542>.
85. Paci, A.; Chiacchia, M.; Bianchi, G. 5GMap: Enabling external audits of access security and attach procedures in real-world cellular deployments. *Comput. Commun.* **2025**, *234*, 108091. <https://doi.org/10.1016/j.comcom.2025.108091>.
86. Samuthira Pandi, V.; Albert, A.J.; Thapa, K.N.K.; Krishnaprasanna, R. A Novel Enhanced Security Architecture for Sixth Generation (6G) Cellular Networks Using Authentication and Acknowledgement (AA) Approach. *Results Eng.* **2024**, *21*, 101669. <https://doi.org/10.1016/j.rineng.2023.101669>.
87. Rao, C.V.; Vandana, C.; Reddy, M.K.V.S.; Raju, K.S.; Sirisha, R.V.P.; Killamsetti, H. Advanced forest fire alert system with real-time GPS location tracking. In Proceedings of the 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 11–13 December 2023; pp. 95–99. <https://doi.org/10.1109/ICACRS58579.2023.10404409>.
88. Alam, D.E.R.; Amelia, F.; Ogi, D.; Marlana, D. Design and development of a woman safety device prototype with fingerprint authentication. In Proceedings of the 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Bali, Indonesia, 17–19 December 2024; pp. 790–795. <https://doi.org/10.1109/ICICYTA64807.2024.10912872>.
89. Hassain, M.M. IoT based smart walking stick for enhanced mobility of the visually impaired. In Proceedings of the 2024 International Conference on Innovations in Science, Engineering and Technology (ICISSET), Chittagong, Bangladesh, 26–27 October 2024; pp. 1–6. <https://doi.org/10.1109/ICISSET62123.2024.10939797>.
90. Aung, N.W.; Thein, T.L.L. Location tracking of accident detection on expressway for informing nearest rescue service. In Proceedings of the 2023 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 27–28 February 2023; pp. 369–374. <https://doi.org/10.1109/ICCA51723.2023.10181700>.
91. Jansi, S.; Sanjeevaiah, K.; Aruna, S.; Reddy, P.V.; Ganesh, D.; Suresh, J. Real-time distress detection and location tracking using a voice-activated system. In Proceedings of the 2025 10th International Conference on Communication and Electronics Systems (ICES), Coimbatore, India, 28–30 October 2025; pp. 716–721. <https://doi.org/10.1109/ICES67310.2025.11336253>.
92. Sarker, S.; Rahman, M.S.; Sakib, M.N. An approach towards intelligent accident detection, location tracking and notification system. In Proceedings of the 2019 IEEE International Conference on Telecommunications and Photonics (ICTP), Dhaka, Bangladesh, 28–30 December 2019; pp. 1–4. <https://doi.org/10.1109/ICTP48844.2019.9041759>.
93. Fung, N.M.; Wong Sing Ann, J.; Tung, Y.H.; Seng Kheau, C.; Chekima, A. Elderly fall detection and location tracking system using heterogeneous wireless networks. In Proceedings of the 2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE), Kota Kinabalu, Malaysia, 27–28 April 2019; pp. 44–49. <https://doi.org/10.1109/ISCAIE.2019.8743664>.
94. Ebenezer, P.R.; Priya, V.M.; Nivetha, B. GPS navigation with voice assistance and live tracking for visually impaired travelers. In Proceedings of the 2019 International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 14–15 March 2019; pp. 1–4. <https://doi.org/10.1109/ICSSS.2019.8882833>.
95. Fauziah, R.J.; Mutiara, G.A.; Periyadi. Smart tracking and fall detection for golden age's citizen. *Procedia Comput. Sci.* **2019**, *161*, 1233–1240. <https://doi.org/10.1016/j.procs.2019.11.237>.
96. Heuer, C.; Jung, V.; Brell-Cokcan, S. A hardware-based RFID identification and tracking system for components in digitalised construction logistics. *Dev. Built Environ.* **2025**, *23*, 100726. <https://doi.org/10.1016/j.dibe.2025.100726>.
97. Park, S.H.; Shin, S.; Hong, S.; Kim, B.; Kim, T. Towards a control and optimization intelligence for 6G mobile networks. In Proceedings of the 2025 IEEE International Conference on Big Data (BigData); IEEE: New York, NY, USA, 2025; pp. 8312–8314. <https://doi.org/10.1109/BigData66926.2025.11402251>.
98. Soualhia, M.; Ullah, M.A.; Yu, P. A hybrid quantum-classical computing for tracking area management for future networks. In Proceedings of the 2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2026; pp. 1–7. <https://doi.org/10.1109/CCNC65079.2026.11366577>.
99. Roensch, W.; Kwon, H.M.; Bhattarai, S.; Banavath, M.N. NextG positioning at user equipment against amplify-and-forward relay jamming. In Proceedings of MILCOM 2025—2025 IEEE Military Communications Conference, Los Angeles, CA, USA, 6–10 October 2025; pp. 1–6. <https://doi.org/10.1109/MILCOM64451.2025.11310331>.
100. Asim, M.; Wu, J.; Li, W.; Lin, Z.; Zhang, P.; He, H.; Wei, D.; Mohi-ud-Din, G. Quantum-resistant blockchain architecture for secure vehicular networks: An ML-KEM-enabled approach with PoA and PoP consensus. *Future Gener. Comput. Syst.* **2026**, *180*, 108391. <https://doi.org/10.1016/j.future.2026.108391>.
101. SLACOZE: Secure LoRa ad-hoc communication network over the dead zone. In Proceedings of the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 6–8 July 2023; pp. 1–7. <https://doi.org/10.1109/ICCCNT56998.2023.10307672>.
102. Lai, Y.; Xu, Y.; Yang, F.; Lu, W.; Yu, Q. Privacy-aware query processing in vehicular ad hoc networks. *Ad Hoc Netw.* **2019**, *91*, 101876. <https://doi.org/10.1016/j.adhoc.2019.101876>.

103. Sanwal, A.; Singh, S.P.; Pradhan, P.M. Development of an algorithm for reducing signalling overhead cost in 5G networks. In Proceedings of the 2021 Advanced Communication Technologies and Signal Processing (ACTS), Virtual, 15–17 December 2021; pp. 1–5. <https://doi.org/10.1109/ACTS53447.2021.9708301>.
104. Alsaedy, A.A.R.; Chong, E.K.P. Mobility management for 5G IoT devices: Improving power consumption with lightweight signaling overhead. *IEEE Internet Things J.* **2019**, *6*, 8237–8247. <https://doi.org/10.1109/JIOT.2019.2920628>.
105. Makai, L.B.; Varga, P. Predicting mobility management demands of cellular networks based on user behavior. In Proceedings of NOMS 2023—2023 IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, 8–12 May 2023; pp. 1–6. <https://doi.org/10.1109/NOMS56928.2023.10154215>.
106. Wen, R.; Feng, G.; Zhou, J.; Qin, S. Mobility management for network slicing based 5G networks. In Proceedings of the 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, China, 8–11 October 2018; pp. 291–296. <https://doi.org/10.1109/ICCT.2018.8600026>.
107. Purification, S.; Chang, S.-Y. Verifiable alerts for 4G/5G public warning system. In Proceedings of the 2025 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 8–11 September 2025; pp. 1–9. <https://doi.org/10.1109/CNS66487.2025.11195018>.
108. Zaidi, S.M.A.; Manalastas, M.; Farooq, H.; Imran, A. Mobility management in emerging ultra-dense cellular networks: A survey, outlook, and future research directions. *IEEE Access* **2020**, *8*, 183505–183533. <https://doi.org/10.1109/ACCESS.2020.3027258>.
109. Sarah, A.; Nencioni, G.; Olimid, R.F. Multi-objective 5G-MEC service relocation: A joint view on performance, availability, and privacy. *Future Gener. Comput. Syst.* **2026**, *176*, 108211. <https://doi.org/10.1016/j.future.2025.108211>.
110. Dimou, S.; Noubir, G. ARGOS: Anomaly recognition and guarding through O-RAN sensing. In Proceedings of the 2025 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 8–11 September 2025; pp. 1–11. <https://doi.org/10.1109/CNS66487.2025.11194171>.
111. Talvitie, J.; Säily, M.; Valkama, M. Orientation and location tracking of XR devices: 5G carrier phase-based methods. *IEEE J. Sel. Top. Signal Process.* **2023**, *17*, 919–934. <https://doi.org/10.1109/JSTSP.2023.3309463>.
112. Sumathi, D.; Prakasam, P.; Nandakumar, S.; Balaji, S. Efficient seamless handover mechanism and mobility management for D2D communication in 5G cellular networks. *Wirel. Pers. Commun.* **2022**, *125*, 2253–2275. <https://doi.org/10.1007/s11277-022-09655-5>.
113. Kato, T.; Sasaki, C.; Tagami, A. Reducing signaling overhead in 5G mobile network for IoT device mobility. In *Advanced Information Networking and Applications*; Springer: Cham, Switzerland, 2024. https://doi.org/10.1007/978-3-031-57840-3_8.
114. Agiwal, M.; Agiwal, A.; Maheshwari, M.K.; Muralidharan, S. Split PO for paging in B5G networks. *J. Netw. Comput. Appl.* **2022**, *205*, 103430. <https://doi.org/10.1016/j.jnca.2022.103430>.
115. Thulasinathan, Y.; Carvalho, G.H.S.; Woungang, I. BERT-driven intrusion detection system for 5G core security. In Proceedings of the 2025 4th International Conference on Computing, Management and Telecommunications (ComManTel), Madrid, Spain, 14–17 December 2025; pp. 64–69. <https://doi.org/10.1109/ComManTel68363.2025.11368344>.
116. Scholler, R.; Alaoui-Ismaili, O.; Couchot, J.-F.; Ballot, E.; Renaud, D. Observing road freight traffic from mobile network signalling data while respecting privacy and business confidentiality. In *Privacy and Identity Management. Between Data Protection and Security*; Springer: Cham, Switzerland, 2022. https://doi.org/10.1007/978-3-030-99100-5_14.
117. Patruni, M.R.; Humayun, A.G. PPAM-mIoT: A privacy-preserving authentication with device verification for securing health-care systems in 5G networks. *Int. J. Inf. Secur.* **2024**, *23*, 679–698. <https://doi.org/10.1007/s10207-023-00762-3>.
118. Parne, B.L.; Gupta, S.; Chaudhari, N.S. PSE-AKA: Performance and security enhanced authentication key agreement protocol for IoT-enabled LTE/LTE-A networks. *Peer-to-Peer Netw. Appl.* **2019**, *12*, 1156–1177. <https://doi.org/10.1007/s12083-019-00785-5>.
119. Nyangaresi, V.O. Target tracking area selection and handover security in cellular networks: A machine learning approach. In *Proceedings of the Third International Conference on Sustainable Expert Systems*; Springer: Singapore, 2023. https://doi.org/10.1007/978-981-19-7874-6_59.
120. Mahmood, A.; Vu, T.X.; Khan, W.U.; Chatzinotas, S.; Ottersten, B. UAV-assisted 5G networks: Mobility-aware 3D trajectory optimization and resource allocation for dynamic environments. In Proceedings of the 2025 IEEE 102nd Vehicular Technology Conference (VTC2025-Fall), Chengdu, China, 19–22 October 2025; pp. 1–7. <https://doi.org/10.1109/VTC2025-Fall65116.2025.11309902>.
121. Wang, X.; Li, T.; Xiong, X.; Gao, Y.; Ning, Z. Federation chain for data privacy protection in industrial Internet of Things: The perspective from 5G core networks. *IEEE Internet Things J.* **2025**, *12*, 39260–39271. <https://doi.org/10.1109/JIOT.2024.3452179>.
122. Mir, A.; Zuhairi, M.F.; Musa, S.; Syed, T.A.; Alrehaili, A. POSTER: A survey of security challenges with 5G-IoT. In Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 3–5 November 2020; pp. 249–250. <https://doi.org/10.1109/SMART-TECH49988.2020.00063>.
123. Ibrahim, Y.; Abdel-Malek, M.A.; Azab, M.; Rizk, M.R. Towards in-depth trustworthy communications in NextG networks. In Proceedings of the 2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2025; pp. 977–982. <https://doi.org/10.1109/CCWC62904.2025.10903696>.

124. Masood, A.; Scazzoli, D.; Sharma, N.; Le Moullec, Y.; Ahmad, R.; Reggiani, L.; Magarini, M.; Alam, M.M. Surveying pervasive public safety communication technologies in the context of terrorist attacks. *Phys. Commun.* **2020**, *41*, 101109. <https://doi.org/10.1016/j.phycom.2020.101109>.
125. Ogulenko, A.; Benenson, I.; Toger, M.; Östh, J.; Siretskiy, A. The fallacy of the closest antenna: Towards an adequate view of device location in the mobile network. *Comput. Environ. Urban Syst.* **2022**, *95*, 101826. <https://doi.org/10.1016/j.compenvurbsys.2022.101826>.
126. Liu, Y.; Tian, J.; Du, Y.; Li, S. A random sensitive area based privacy preservation algorithm for location-based service. *Wirel. Pers. Commun.* **2021**, *119*, 1179–1192. <https://doi.org/10.1007/s11277-021-08256-y>.
127. Zhang, S.; Kang, H.; Yu, D. An enhanced location-data differential privacy protection method based on filter. In *Smart Grid and Internet of Things*; Springer: Cham, Switzerland, 2022. https://doi.org/10.1007/978-3-031-20398-5_10.
128. Qu, Y.; Zhang, J.; Li, R.; Zhang, X.; Zhai, X.; Yu, S. Generative adversarial networks enhanced location privacy in 5G networks. *Sci. China Inf. Sci.* **2020**, *63*, 220303. <https://doi.org/10.1007/s11432-019-2834-x>.
129. Li, M.; Yang, Q.; Zheng, X.; Nawaf, L. Spatiotemporal location privacy preservation in 5G-enabled sparse mobile crowdsensing. In *Proceedings of the International Conference on Computing and Communication Networks*; Springer: Singapore, 2022; pp. 277–295. https://doi.org/10.1007/978-981-19-0604-6_24.
130. Zhang, C.; Xu, C.; Sharif, K.; Zhu, L. Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications. *Comput. Stand. Interfaces* **2021**, *77*, 103520. <https://doi.org/10.1016/j.csi.2021.103520>.
131. Yao, A.; Pal, S.; Li, X.; Zhang, Z.; Dong, C.; Jiang, F.; Liu, X. A privacy-preserving location data collection framework for intelligent systems in edge computing. *Ad Hoc Netw.* **2024**, *161*, 103532. <https://doi.org/10.1016/j.adhoc.2024.103532>.
132. Liao, D.; Li, H.; Sun, G.; Zhang, M.; Chang, V. Location and trajectory privacy preservation in 5G-enabled vehicle social network services. *J. Netw. Comput. Appl.* **2018**, *110*, 108–118. <https://doi.org/10.1016/j.jnca.2018.02.002>.
133. Ashok, P.; Prabhu, S. Attack-Resistant Cybersecurity Measures for Next-Generation Connected Electric Vehicles. *Recent Adv. Electr. Electron. Eng.* **2026**, *19*, 1–16. <https://doi.org/10.2174/0123520965388722250429051322>.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.