Dissecting Privacy-Exposing Identifiers in 5G/4G Networks

Munshi Saifuzzaman
School of Computing
Utah State University
Logan, UT 84321 USA
munshi.saifuzzaman@usu.edu

Ke Xie
School of Computing
Utah State University
Logan, UT 84321 USA
ke.xie@usu.edu

Tian Xie
School of Computing
Utah State University
Logan, UT 84321 USA
tian.xie@usu.edu

Xiao Zhang
Department of Computer and Information Science
University of Michigan-Dearborn
Dearborn, MI 48128 USA
zhanxiao@umich.edu

Xinyu Lei
Department of Computer Science
Michigan Technological University
Houghton, MI 49931
xinyulei@mtu.edu

***Abstract*—Modern cellular networks rely on a variety of signaling identifiers to support core operations like authentication, mobility, and capability negotiation. While these identifiers are functionally essential, they can inadvertently leak privacy-sensitive information, even under standard-compliant procedures. Prior studies have focused on isolated attack cases or specific identifiers such as IMSI and GUTI. However, the broader identifier ecosystem, including less-known fields, remains insufficiently examined. In this paper, we present the first systematized and specification-grounded analysis of privacy-exposing identifiers in 5G and 4G networks, spanning NAS, RRC, MAC layers, and PC5 interface. We evaluate their exposure conditions and highlight persistent privacy risks arising from default protocol behavior. Notably, we uncover and analyze three underexplored identifiers: UE Radio Capability ID, Remote UE ID, and ProSe UE ID, that reveal critical privacy vulnerabilities through mechanisms such as fingerprintability, reuse across sessions, and exposure across protocol layers. Our analysis is fully grounded in 3GPP standards and validated using an operational U.S. mobile network. The findings expose critical gaps in identifier protection logic and motivate rethinking cellular privacy beyond adversarial threat models.**

***Index Terms*—Cellular network privacy, 5G/4G security**

I. Introduction

Modern cellular networks are critical societal infrastructure, enabling ubiquitous mobile communication, IoT connectivity, and real-time services across sectors such as healthcare, transportation, finance, and agriculture. To support these functionalities, cellular networks employ a variety of signaling identifiers, such as IMSI, SUPI, GUTI, and C-RNTI, that facilitate authentication, session and mobility management, radio access and scheduling. While identifiers are essential for operational correctness and efficiency in cellular networks, they have also raised increasing privacy concerns within the research community. Despite standardization efforts by 3GPP, these identifiers can inadvertently expose sensitive information, such as user location, long-term identity linkage, and behavioral patterns, when intercepted by adversaries. This concern is especially critical as mobile devices become increasingly embedded in individuals' personal lives.

To mitigate such privacy risks, 3GPP has introduced mechanisms such as temporary identifiers (e.g., TMSI, SUCI) to reduce the exposure of long-term identities. However, numerous studies have demonstrated that privacy leakage persists even with these mechanisms in place [1]–[3]. Unsurprisingly, the research community has invested substantial efforts in attempting to detect, dissect, and mitigate privacy risks posed by identifiers [1]–[24]. For instance, a recent work from Tucker et al. studies the IMSI-Catcher detection [23], highlighting the importance of message-level analysis to identify privacy-exposing flows. The problem with these works is that existing research remains fragmented, largely limited to isolated case studies (e.g., IMSI catchers or paging sniffing) or focused on a narrow subset of procedures. Unfortunately, no published work has been able to present a principled, systematized, and specification-grounded analysis to dissect privacy-exposing identifiers in cellular networks. Thus, many identifiers in cellular networks have yet to be thoroughly examined for whether they can compromise user privacy.

In this paper, we address this gap by proposing a principled and systematized methodology for analyzing privacy-exposing identifiers in 5G and 4G networks. Our two-step approach identifies identifiers across multiple network layers and interfaces, examines their operational behaviors, and assesses their exposure conditions based on standard-compliant procedures. This framework not only enables a structured understanding of known identifiers but also uncovers and analyzes three previously underexplored identifiers: UE (User Equipment) Radio Capability ID, Remote UE ID, and ProSe UE ID.

This paper makes three key contributions:

- To the best of our knowledge, we propose the first principled and systematized methodology to discover privacy-

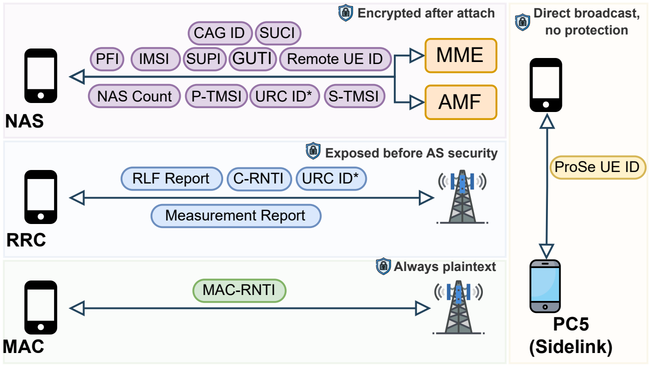


Fig. 1: Identifier placement across NAS, RRC, MAC layers and PC5 interface, along with their security protection mechanisms.

exposing identifiers in cellular networks. Our approach offers a comprehensive framework and leads to the identification of three underexplored identifiers with privacy implications.

- We conduct a specification-driven, message-level analysis of privacy-exposing identifiers. By tracing their usage across signaling procedures, we assess privacy exposure risks without requiring time-consuming empirical experimentation.
- The insights derived from our analysis can inform improvements in cellular standards and implementations, ultimately enhancing the privacy protection for both mobile users and network operators.

II. Background

5G/4G Cellular Network Layers and Security Mechanisms. Modern cellular networks are built on a layered protocol architecture that includes the physical (PHY), Medium Access Control (MAC), Radio Resource Control (RRC), Non-Access Stratum (NAS), and application layers, resembling the layered models used in general computing systems. These layers collectively manage signaling, control, and data exchange between the UE, base stations, and the core network. Particularly, MAC, RRC, and NAS layers, as shown in Figure 1, form the core signaling plane. They handle numerous identifiers that are of significant interest in privacy research due to their exposure and uniqueness within the mobile ecosystem.

◇ *NAS* operates between the UE and the core network and is responsible for critical control functions such as mobility management, session management, and authentication procedures. This layer carries various identifiers, including IMSI, SUPI, GUTI, and Remote UE ID [25]. NAS layer messages are protected by encryption and integrity mechanisms only after successful mutual authentication and the establishment of a NAS security context [26], [27]. Prior to this, NAS messages such as `Attach Request` and `Registration Request` are transmitted without confidentiality, leaving sensitive identifiers exposed.

◇ *RRC* manages the radio configuration, UE state transitions, and mobility procedures between the UE and the base station [28], [29]. The RRC layer utilizes identifiers such as C-RNTI, Measurement Reports and RLF (Radio Link Failure) Reports. Access Stratum (AS) security ensures the RRC-level traffic is confidential, authenticated, and integrity protected. It is distinct from NAS security, which secures communication between the UE and the core network. AS security is activated after NAS security is completed. Until then, RRC layer traffic is transmitted in plaintext, which can lead to the location inference, device fingerprinting, and passive tracking [26].

◇ *MAC* handles low-level scheduling and resource allocation between the UEs and base stations. Identifiers such as MAC-RNTI are defined at this layer for control signaling and resource assignment [30]. They are transmitted unencrypted without integrity protection, making them trivially observable to adversaries.

PC5 Interface. The PC5 interface supports direct device-to-device communication using Proximity Services (ProSe) [31], [32]. Unlike conventional communication paths, PC5 traffic typically bypasses the core network and is implemented using the dedicated sidelink MAC layer as shown in Figure 1. Identifiers such as the ProSe UE ID with PC5 interface are broadcast between UEs without encryption or authentication. Since NAS and AS security mechanisms do not apply to PC5, any identifier included in a ProSe discovery or communication message is openly broadcast and can be collected by any nearby device [31].

III. Related Work

Long-term identifiers. Several prior studies in cellular privacy have predominantly focused on persistent long-term identifiers. Hussain et al. [6] and Kotuliak et al. [3] demonstrated that the use of predictable or improperly randomized IMSIs before the completion of authentication can enable long-term user tracking. These studies primarily aimed to detect exposure of permanent identifiers during initial attach procedures. Tucker et al. [23] leveraged IMSI-Catchers to identify downlink messages that reveal the IMSI. However, their analysis remained constrained to IMSI-specific exposures within the EPS NAS layer, omitting broader identifier categories or their cross-layer use. Bartock et al. [24] extended the analysis to 5G by evaluating the SUPI, revealing that it may be exposed in plaintext in NAS Registration Request messages when the SUCI mechanism is disabled or uses null encryption, especially in scenarios like emergency services or incomplete operator support. Kohls et al. [21] and Rupprecht et al. [22] demonstrated how even encrypted LTE layer-two traffic can reveal user identities through side-channel inference using metadata, timing, and identifier linkage (e.g., C-RNTI to TMSI mapping), enabling indirect but persistent IMSI-level tracking under passive observation.

Short-term identifiers. While 3GPP introduces temporary identifiers to mitigate persistent tracking risks, users may still experience privacy leakage due to identifier reuse or lack of update. Several works showed that temporary identifiers, including GUTI, S-TMSI, P-TMSI, C-RNTI, MAC-RNTI,

TABLE I: Abbreviations and full forms of privacy-exposing identifiers and their related works.

Privacy-exposing Identifiers	**Full Form**	**Related Works**
IMSI	International Mobile Subscriber Identity	[4]–[23]
SUPI	Subscription Permanent Identifier	[24]
SUCI	Subscription Concealed Identifier	[6], [10]
GUTI	Globally Unique Temporary Identifier	[1], [5], [7], [10], [15]
P-TMSI	Packet Temporary Mobile Subscriber Identity	[2]
CAG ID	Closed access group Identifier	[10]
PFI	Paging Frame Index	[6]
NAS Count	Non-Access Stratum Sequence Counter	[10]
C-RNTI	Cell Radio Network Temporary Identifier	[17]
S-TMSI	SAE Temporary Mobile Subscriber Identity	[3]
RLF Report	Radio Link Failure Report	[7]
Measurement Report	RRC Measurement Report	[7]
MAC-RNTI	Medium Access Control Radio Network Temporary Identifier	[3]
URC ID	User Equipment Radio Capability Identifier	Our work
REMOTE UE ID	REMOTE User Equipment Identifier	Our work
ProSe UE ID	Proximity Services User Equipment Identifier	Our work

can remain linkable across sessions or procedures if they are not refreshed adequately [1]–[3], [7], [17]. Hermes [10] and LTEInspector [5] extended the analysis to authentication-related short-term identifiers (i.e., SUCI and GUTI), revealing vulnerabilities stemming from control-plane behavior.

Moreover, the PFI, a deterministic field derived from the IMSI, can cause privacy exposure by leaking the UE's paging schedule. This timing correlation forms the basis of the ToRPEDO attack, allowing attackers to infer user presence and mount denial-of-service or location-tracking attacks [6]. Shaik et al. [7] showed that unprotected RLF and Measurement Reports can be exploited to obtain signal metrics or GPS location data under active MitM setups. These reports are often accepted before AS security is established, enabling location tracking under standard-compliant procedures.

Our work differs from the above state-of-the-art works in two **key** regards. **First**, prior works mostly focus on one or a few privacy-exposing identifiers on a specific network layer. Our work studies the privacy-exposing identifiers across multiple network layers in 5G/4G networks, allowing us to identify and investigate the hidden ones that were not explored before. **Second**, state-of-the-art studies primarily target implementation flaws, isolated procedures, or adversarial exploitations rather than privacy risks in standard-compliant service flows. In contrast, our work uses 3GPP specifications as the base to analyze privacy-exposing identifiers in 5G/4G networks in six dimensions. By tracing their propagation through routine network procedures, we demonstrate that privacy leakage can occur even in normal message flows.

IV. Threat Model and Ethical Consideration

Threat Model: In this work, adversaries are people or organizations that attack the cellular networks. We consider adversaries with the following capabilities: (1) they can intercept, modify, or inject any messages in the public cellular network channels; (2) they adhere to all cryptographic assumptions, e.g., adversaries cannot decrypt an encrypted message without the decryption key.

Ethical Consideration: We understand that some feasibility tests and evaluations might be harmful to the operators and/or users. Accordingly, we conducted this study responsibly by running all experiments in fully controlled environments. Particularly, to validate the discovered privacy vulnerabilities, we collected traces with our lab members. Our goal is to disclose new security vulnerabilities instead of aggravating the damage.

V. Methodology

Cellular networks utilize various identifiers across multiple protocol layers to support key functionalities such as authentication, mobility, paging, and resource scheduling. These identifiers span the NAS, RRC, MAC network layers, and PC5 interface, differing in design objectives, scopes, and lifetimes. Although designed to be short-term or long-term, their real-world behavior often deviates from specification. Because of the sensitive information (e.g., UE location, device model) in those identifiers, their exposures raise privacy concerns. To systematically investigate the privacy issues, we propose a two-step methodology to analyze privacy-exposing identifiers in 5G and 4G networks as below.

Network-layer-based identifier extraction. To systematically analyze the identifiers in cellular networks, we first use a network-layer-based methodology to identify and organize privacy-exposing identifiers. Specifically, we define the *privacy-exposing identifiers* as signaling fields that either uniquely represent a user, device, subscription, or session, or can be used to infer or correlate user activity under standard-compliant procedures. Our analysis encompasses both permanent identifiers (e.g., IMSI, SUPI) and temporary ones (e.g., GUTI, S-TMSI, C-RNTI). An identifier is classified as privacy-exposing if it meets one or more of the following criteria: (i) it is assigned to a specific UE or subscription; (ii) it enables persistent linkage across sessions or procedures; or (iii) it reveals behavioral or location information attributable to a UE. While many identifiers are explicitly user-unique, others, such as counters or measurement reports, can leak sensitive

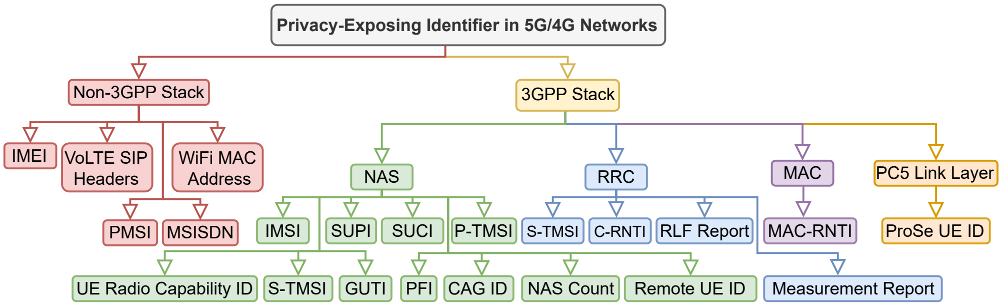


Fig. 2: Privacy-exposing identifiers in 5G/4G Networks organized by network layers.

information through their signaling characteristics even if they are not uniquely assigned.

We leverage the network stack layer to categorize the identifiers in signaling messages, including 3GPP stack and non-3GPP stack (e.g., Wi-Fi). Our focus is limited to standardized identifiers defined in 3GPP specifications. As shown in Figure 2, we extract privacy-exposing identifiers from network layers such as NAS, RRC, and MAC, and PC5 interface. Note that we classify the identifiers, such as SIP headers used in VoLTE services that are not specifically defined in 3GPP standards, as non-3GPP identifiers. They are excluded from further analysis.

Specification-driven message-level analysis. For each identifier discovered in the prior step, we trace its appearance across signaling procedures (e.g., registration, paging, relay) using 3GPP standards. We systematically analyze the signaling messages that carry these identifiers and examine both uplink and downlink message flows to assess the presence or absence of integrity and confidentiality protections. Importantly, it **does not** require empirical fuzzing adversarial testing, which is often time-consuming and dependent on physical testbeds. Instead, our analysis leverages the normative content of 3GPP standards, adhered to by mobile device manufacturers and network operators worldwide, to evaluate privacy risks in a scalable and reliable manner.

Novelty of Method: Our approach makes two key innovations compared to prior works. First, we adopt a network-layer-based analysis method that organizes the privacy-exposing identifiers in cellular networks, spanning NAS, RRC, MAC layers, and PC5 interface. This structural foundation enables broader identifier coverage compared to prior works [5], [6], which typically focus on isolated identifiers (e.g., IMSI, GUTI) or specific procedures (e.g., paging, attach). Second, we conduct a specification-driven, message-level analysis. Based on 3GPP specifications, by tracing the identifier usage, exposure points, and associated protection conditions based on 3GPP standards, our findings showcase that even within standard-compliant message flows, privacy-exposing identifiers in 5G/4G networks can facilitate user tracking or linkage.

VI. Results

In this section, we present the discovered privacy-exposing identifiers in 5G/4G mobile networks across multiple network layers and the damages they can cause.

A. *Privacy-exposing Identifiers in 5G/4G Cellular Networks*

Table II provides an overview of the privacy-exposing identifiers in 5G and 4G networks that can expose mobile user privacy even under the standard-compliant operations. Each identifier is evaluated in six dimensions. **Purpose** column outlines the primary role of the identifier in the network, such as authentication, mobility management, and network capability reporting. **Lifecycle** describes how long the identifier is expected to persist, ranging from permanent values used for long-term to session-based or event-triggered values used for short-term. If an identifier persists longer, it can bring a greater risk of tracking and linkability. **Security Protection** column summarizes security protection mechanisms applied to the identifiers in terms of confidentiality and integrity. Based on 3GPP specifications, the identifiers can be encrypted, conditionally encrypted, or always plaintext for transmission. **Tracking Risk** estimates the likelihood that an adversary can use the identifier for linking or tracking, based on its Lifecycle and Security Protection. We classify an identifier as high-risk if it is globally unique, long-lived, or reused across procedures (e.g., IMSI, SUPI, Remote UE ID). Identifiers that are session-based but reused, unprotected, or predictable (e.g., GUTI, MAC-RNTI, S-TMSI, RLF Report) are assigned medium risk. Identifiers that are always encrypted or not observable in practice are excluded from our scope. Thus, there is no identifier with no or low tracking risk in this table. **Cellular Generation** indicates whether the identifier is used in 4G, 5G, or both. **Message Layer** specifies the network layer where the identifier appears, such as NAS, RRC, MAC, or PC5. It highlights its exposure scope in the protocol stack. Together, these attributes provide a foundation for the message-level analysis and risk categorization.

1) Privacy Leakage in Various Network Layers: Privacy-exposing identifiers appear at various network layers, most notably NAS, RRC, MAC, and PC5.

TABLE II: Summary of privacy-exposing identifiers in 5G/4G networks, organized by purpose, message layer, lifecycle, protection status, and privacy risk.

Identifier	Purpose	Message Layer	Gen.	Lifecycle	Protection Status	Privacy Risk	3GPP Spec
IMSI	Authentication	NAS	5G/4G	Permanent	No (unless SUCI used)	High	TS 23.003
SUPI	Permanent user identity	NAS	5G	Permanent	No (unless SUCI is used)	High	TS 23.003
SUCI	Concealed form of SUPI	NAS	5G	Session-based	Yes (except null scheme)	Medium	TS 23.003
GUTI	Temporary identity for EPS	NAS	5G/4G	Session-based	No (plaintext in NAS)	Medium	TS 23.003
P-TMSI	Temporary ID for SGSN access	NAS	4G	Session-based	No	Medium	TS 23.003
CAG ID	Access Control Group Identifier	NAS	5G	Session-based	No	Medium	TS 23.003
PFI	EPS bearer filter ID	NAS	4G	Session-based	No	Medium	TS 24.301
NAS Count	Message replay protection counter	NAS	5G/4G	Ephemeral	Partial (integrity protected only)	Medium	TS 24.301
C-RNTI	RRC Connection Identifier	RRC	4G	Session-based	No	Medium	TS 36.331
S-TMSI	Shortened GUTI for paging	NAS	4G	Temporary	No	Medium	TS 23.003
RLF Report	Link failure diagnostics	RRC	4G	Event-triggered	No	Medium	TS 36.331
Measurement Report	Feedback on signal quality	RRC	4G	Event-triggered	No	Medium	TS 36.331
MAC-RNTI	Physical layer UE scheduling	MAC	4G	Ephemeral	No	Medium	TS 36.331
UE Radio Capability ID	UE capability profile reference	NAS/RRC	5G/4G	N/D†	Depends¶	Medium	TS 23.003
Remote UE ID	Identity of relayed UE	NAS	5G/4G	Session-based‡	Depends¶	High	TS 24.301
ProSe UE ID	Identifier for public safety UE discovery	PC5 Interface	4G	N/D†	Depends¶	Medium	TS 23.003

† Identifiers marked as ‘N/D’ do not have lifecycle defined in 3GPP specifications.
‡ The Remote UE ID itself is session-scoped, though it may embed persistent identifiers like IMEI
¶ “Depends” reflect conditional protection based on NAS, AS, or ProSe security activation.

NAS. Long-term identifiers such as IMSI and SUPI are assigned and used during initial authentication procedures. They have been known to have a critical privacy vulnerability that can make mobile users trackable. While the short-term identifiers such as GUTI and SUCI can mitigate the privacy concern, they can still leak sensitive information. For example, SUCI may be linkable if operators deploy static public keys or null-encryption schemes [24], and GUTIs may remain unchanged for extended periods, enabling session correlation [1], [7]. In addition to these known privacy-exposing identifiers, several identifiers that are not traditionally considered privacy-exposing are investigated and warrant further attention. For instance, the UE Radio Capability ID is a compact representation of the UE’s supported radio features, which can be used to infer the device model and vendor information. They can contribute to persistent fingerprinting to track UEs. Similarly, the Remote UE ID, used in ProSe relay scenarios, allows the UE to report its identity to others. While this field is session-scoped for a short term, the Remote UE ID can embed permanent identifiers like IMEI or IMEISV, which thereby create indirect privacy leakage risks.

RRC. Identifiers in the RRC layer are primarily used for the UE’s radio connection and mobility. C-RNTI is the identifier scoped to individual cells but has been shown to persist across idle-to-active transitions and resumption procedures [3]. Measurement-related fields like RLF Reports can further expose signal histories or GPS-related information if accepted before AS security activation [7].

MAC. MAC-RNTI is transmitted without encryption and can be exploited for stealthy device tracking via side-channel timing analysis [3]. Note that we exclude the non-3GPP identifiers, such as Wi-Fi MAC address, in MAC layer.

PC5. PC5 is an interface used for direct device-to-device (D2D) communication, bypassing the cellular infrastructure like base stations or core network components. The ProSe UE ID operates outside NAS protection and is used for device discovery in public safety scenarios. Since no rotation or renewal scheme is mandated by TS 23.003, this identifier can remain stable across sessions, enabling long-term local tracking.

2) Observations: We next discuss four key observations.

Identifiers Can Be Spec-Compliant but Privacy-Compromising. Our analysis reveals a set of identifiers whose exposure arises not from implementation flaws, but from specification-level weaknesses in protocol design. For example, the Closed Access Group (CAG) ID is processed by the UE before the enforcement of integrity protection. Thus, it permits unauthenticated `Registration Reject` messages from man-in-the-middle (MiTM) adversaries to launch the persistent denial-of-service (DoS) attack in non-public network deployments [10]. Similarly, according to 3GPP standards, Remote UE ID can appear in the signaling messages before NAS security is activated. The exposure of these identifiers, despite adherence to 3GPP standard-defined procedures, highlights a critical insight: the specification compliance does not guarantee privacy preservation. There is a critical need to review the 3GPP standards from the privacy perspective.

Identifiers Can Enable Side-channel Privacy Attacks. Some identifiers in our study are not explicitly designed as user identifiers by 3GPP standards. However, they can still leak behavioral or location information under passive interception. For instance, Measurement Reports and RLF Reports are transmitted before AS security is activated, which is used to ensure radio-level communication between the UE and the base station is confidential, authenticated, and integrity protected [26], [27]. Thus, without confidential protection, they can expose the serving cell IDs, signal quality, and GPS location data. While they are not unique per UE, they still pose privacy risks by enabling side-channel inference or mobility profiling [7]. Likewise, NAS Count is used to defend against message replay attacks. However, it can be abused to recognize the sequence patterns to infer session conditions. As a result, the exposure of these identifiers violates user anonymity and can enable further side-channel attacks.

Identifier Reuse Can Lead to Linkability. Our analysis shows that many identifiers are intended to be short-lived to mitigate the privacy exposure vulnerability. However, they can also make the mobile users trackable if they are not consistently updated per session or procedure. For instance, GUTIs and S-TMSIs have been shown to persist across TAU and paging cycles [1], [7]. The UE Radio Capability ID, while not designed as a pseudonym, can nonetheless function as a stable fingerprint when reused across registration procedures. These reuse patterns indicate a lack of unlinkability guarantees and allow adversaries to correlate distinct sessions to the same UE.

Privacy Exposure Occurs in Various Layers. One of the key findings of our study is that the privacy exposure caused by identifiers is not limited to a specific network layer. Our study highlights that the threat surface spans the various network layers across the mobile networks, not just a single network layer typically focused by prior works.

B. Specification-driven Message-level Analysis

We next present a detailed specification-driven message-level analysis with a focus on three underexplored privacy-exposing identifiers: UE Radio Capability ID, Remote UE ID, and ProSe UE ID. Our analysis spans both uplink and downlink flows and deliberately focuses on standard-compliant procedures, excluding adversarial manipulation or protocol violations. It ensures that the observed exposures stem from 3GPP standards. In the end, we explain how and when privacy exposure can occur even during standard-compliant procedures and what privacy behaviors can be introduced with the specification-backed analysis and empirical experiment results. The analysis results, including the vulnerable messages, usage scope, and security protection mechanisms, are summarized in Table III.

1) UE Radio Capability ID (URC ID): The URC ID is a compact identifier representing a UE's supported radio configuration. It may persist across sessions and includes fields such as the Vendor ID and the Radio Configuration Index (RCI). TS 23.003 §29.3 [33] defines that the mobile network can use the URC ID to refer to a predefined radio capability profile without the need to retransmit the full UE radio capability list. The URC ID can be manufacturer assigned (via IANA enterprise numbers [34]) or network assigned and indexed via the UCMF (UE Capability Management Function). In either case, the URC ID reveals both the device's radio configuration and manufacturer-specific information, making it a potentially long-term identifier that could be used to correlate a UE across multiple sessions and network connections.

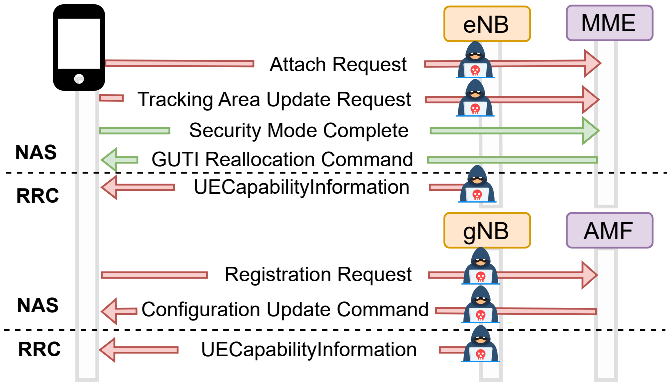


Fig. 3: Signaling messages carrying the URC ID could be transmitted in 4G and 5G networks.

The URC ID can be transmitted in both NAS and RRC signaling flows illustrated in Figure 3, emphasizing how URC IDs can be exposed during early stages of the protocol before cryptographic protections are applied. At the NAS layer, several messages can carry the URC ID, including `Registration Request` and `Configuration Update Command` (TS24.501 §4.16) in 5G [35], `Security Mode Complete` (TS24.301 §8.2.21.4), `Attach Request`, `Tracking Area Update request` (TS24.301 §8.2.21.4), and `GUTI Relocation Command` TS24.301 §5.4.1.3 in 4G [36]. The URC ID is encrypted only if a NAS security context has already been established. For instance, it is encrypted when included in the `Security Mode Complete` message after completing NAS security establishment. Otherwise, it can be exposed in plaintext in messages such as the initial `Registration Request`, which occurs before any security context is in place. In addition to NAS messages, the URC ID may also be included in the `UECapabilityInformation` message at the RRC layer. The security of this message depends on whether RRC ciphering has been activated. If `UECapabilityInformation` is transmitted prior to the `Security Mode Command`, its contents, including the URC ID, are sent in plaintext and can be intercepted by the adversary.

Validation. To empirically validate our findings, we analyzed real-world traces to confirm the presence and exposure of URC IDs. We used a Samsung S21 device with MobileInsight [37] installed to collect NAS and RRC messages on the T-Mobile network in 4G. Our analysis of the captured traces confirms

TABLE III: Specification-driven exposure mapping[¶] for three underexplored identifiers across NAS, RRC, and PC5 message layers in 4G and 5G.

Identifier	Generation	Message Layer	Uplink Message	Downlink Message	Usage Scope[†]	Protection Status[‡]
URC ID	4G	NAS	SECURITY MODE COMPLETE	SECURITY MODE COMMAND	SP	Yes
		NAS	ATTACH REQUEST	ATTACH ACCEPT	SP	Both
		NAS	TRACKING AREA UPDATE REQUEST	TRACKING AREA UPDATE ACCEPT	SP	Both
		NAS	N/A	GUTI REALLOCATION COMMAND	FC	Yes
		RRC	UECapabilityInformation	UECapabilityEnquiry	SP	Depends
	5G	NAS	REGISTRATION REQUEST	REGISTRATION ACCEPT	SP	Depends
		NAS	REGISTRATION REQUEST	CONFIGURATION UPDATE COMMAND	SP	Depends
		RRC	UECapabilityInformation	UECapabilityEnquiry	SP	Depends
Remote UE ID	4G	NAS	REMOTE UE REPORT	REMOTE UE REPORT RESPONSE	SP	No
	5G	NAS	REMOTE UE REPORT	REMOTE UE REPORT RESPONSE	SP	No
ProSe UE ID	4G	PC5 Link Layer	ProSe Discovery Broadcast	N/A	SP	No

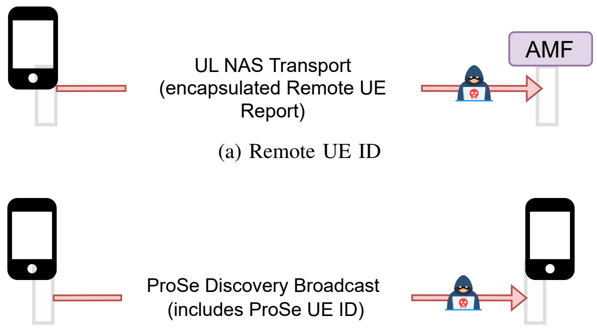
[†] Usage Scope: SP = Standard Procedure, FC = Fallback Case.
[‡] Protection Status: Yes = Encrypted, No = Plaintext, Depends = Conditional on security context, Both = Encrypted in one direction and plaintext in the other.
[¶] Exposure conditions are extracted from 3GPP TS 24.301 v18.9.0, TS 24.501 v18.10.0, TS 36.331 v18.5.0, TS 38.331 v18.5.1 and 23.303 v18.0.0.

that URC IDs are indeed present in the identified signaling messages and are exposed in plaintext when transmitted without an established security context, aligning with the behavior specified in 3GPP standards. Note that URC IDs are optional and may be configured on an operator-specific basis. In addition, the UE's radio capabilities can alternatively be conveyed through fields such as ueCapabilityInformation [36], UE-CapabilityRAT-Container [28], and UE-NR-Capability [29].

On Open-source Platform Open5GS. On Open5GS, when the UE carries the URC ID in the identified signaling messages, the AMF can respond with messages carrying the URC ID. To trigger the UE and AMF to embed the URC ID in messages, on Open5GS, it can be easily configured by setting the presence mask bit UE_RADIO_CAPABILITY_ID_PRESENT to 1. Since the URC ID is configured according to the UE's hardware and firmware, which rarely change over time, it remains consistent across sessions and thus functions as an effectively static identifier.

2) Remote UE ID: The Remote UE ID is an identifier used to report the identity of another UE to the network during ProSe (Proximity Services) relay operations. It is defined with a 3-bit type field that allows it to serve as a container for various identifiers, including the IMEI, IMEISV, and PRUK ID [38]. While the Remote UE ID field itself is scoped for the relay session only, the identifiers it carries, such as IMEI or IMEISV of the relayed device, are globally unique and long-lived. The persistent content introduces critical privacy risks despite the short signaling lifetime of the Remote UE ID.

As illustrated in Figure 4a, according to TS 24.501 §9.11.4.29.2 for 5G [35] and TS 24.301 §6.6.3.2 for 4G [36], the Remote UE ID is carried in the `Remote UE Report`, encapsulated within a `UL NAS Transport` to AMF during ProSe relay or discovery procedures when one UE assists in establishing context for another device. Notably, the Remote UE ID is also used for 4G public safety scenarios according to TS 24.301 §6.6.3.2.



(a) Remote UE ID

(b) ProSe UE ID

Fig. 4: Illustration of identifier transmission under standard-compliant signaling. (a) Remote UE ID is transmitted via UL NAS TRANSPORT and may carry third-party identifiers (e.g., IMEI) without encryption. (b) ProSe UE ID is broadcast between devices during sidelink discovery, exposed in plaintext over the PC5 interface.

While the `Remote UE Report` message shall be encrypted by NAS security when available, our study shows that the encryption of `Remote UE Report` is not strictly enforced by 3GPP specifications and it can be sent before NAS security is activated. Specifically, during initial attach procedures and emergency services for public safety in 4G, the `Remote UE Report` message is transmitted without NAS security protection; if the NEA0 algorithm (null encryption) is misconfigured, the message can be transmitted without confidentiality. Consequently, the REMOTE UE ID containing the persistent identifier IMEI or IMEISV can be exposed in plaintext during ProSe relay or discovery. It presents a unique third-party exposure vector, compliant with standards, that could leak nearby device identities and raise serious privacy concerns in mobile networks.

Validation. Due to the limited deployment of ProSe relay and discovery procedures in U.S. commercial mobile networks, we were unable to collect real-world traces to empirically validate these behaviors. Nonetheless, our analysis, grounded in 3GPP-compliant procedures, shows that if operators implement the infrastructure as specified, the inclusion of long-term identifiers within Remote UE ID poses tangible privacy risks.

On Open-source Platform Open5GS. Open5GS does not offer ProSe replay support. Remote UE ID is absent in its NAS signaling.

3) ProSe UE ID:

The *ProSe UE ID* is a 24-bit identifier for direct D2D communication over the PC5 interface [31], [33]. It is primarily used in proximity services such as V2X and public safety, where two UEs communicate directly without involving the core network. Different from the aforementioned NAS and RRC identifiers, the ProSe UE ID is scoped to the sidelink (PC5), outside of the common security domains in cellular networks.

As shown in Figure 4b, the ProSe UE ID is included in the MAC header of the discovery broadcast message. As described in TS 23.303, this message enables nearby UEs to detect and respond to each other without core network assistance [31]. Since this identifier is transmitted in unicast and broadcast messages at the MAC layer, it bypasses all NAS and RRC protections. Moreover, there is no mandated per-session rotation, obfuscation, or expiration of the identifier in 3GPP standards. This omission permits the long-term identifier reuse, which enables device tracking across discovery sessions. As a result, the same ProSe UE ID may persist across discovery cycles, sessions, or device reboots. The absence of encryption in MAC layer and the reuse of this static identifier pose significant privacy risks. Any MiTM adversary within radio range can associate the ProSe UE ID with a specific device and track its presence across time and space.

Validation. Due to the limited support for ProSe discovery and relay in commercial U.S. networks at this moment, we were unable to collect real-world traces to empirically validate the privacy exposure. Nonetheless, our analysis, grounded in 3GPP specifications, confirms that the ProSe UE ID is included in MAC layer discovery broadcasts over the PC5 interface, is not subject to any security mechanisms. Once ProSe is deployed as specified, this identifier can be reused across discovery sessions and presents a tangible privacy risk.

On Open-source Platform Open5GS. Open5GS does not implement ProSe relay functionality. Therefore, ProSe UE ID cannot be empirically observed in its traces.

VII. Conclusion

This paper presents the first systematic and specification-grounded study of privacy-exposing identifiers in 5G and 4G networks. Unlike prior works focused on a few known identifiers, our framework uncovers a broader ecosystem spanning NAS, RRC, MAC layers, and PC5 interface. Our analysis reveals that even standard-compliant signaling procedures can expose sensitive identifiers, especially when protections like NAS and AS security are not yet activated. Among the 16 identifiers analyzed, we spotlight three underexplored fields, UE Radio Capability ID, Remote UE ID, and ProSe UE ID, that introduce serious privacy risks due to long-term persistence, cross-layer exposure, or lack of encryption. These identifiers can enable user fingerprinting, third-party tracking, and persistent local monitoring, even without violating 3GPP specifications. Our analysis and experimental results confirm that leakage can occur in practical scenarios. We hope our study motivates future improvements in identifier design, adoption of stricter protection mechanisms, and standard revisions to minimize privacy exposure in cellular networks.

VIII. Acknowledgments

This work is supported in part by the National Science Foundation under Grant No. CNS-2153393 and by the National Artificial Intelligence Research Resource (NAIRR) Pilot under Grant No. NAIRR240456. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors only and do not necessarily reflect those of the NSF and NAIRR.

References

[1] B. Hong, S. Bae, and Y. Kim, "Guti reallocation demystified: Cellular location tracking with changing temporary identifier." in *NDSS*, 2018.

[2] A. Singla, S. R. Hussain, O. Chowdhury, E. Bertino, and N. Li, "Protecting the 4g and 5g cellular paging protocols against security and privacy attacks," *Proceedings on Privacy Enhancing Technologies*, 2020.

[3] M. Kotuliak, S. Erni, P. Leu, M. Röschlin, and S. Čapkun, "{LTrack}: Stealthy tracking of mobile phones in {LTE}," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1291–1306.

[4] P. O'hanlon, R. Borgaonkar, and L. Hirschi, "Mobile subscriber wifi privacy," in *2017 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2017, pp. 169–178.

[5] S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "Lteinspector: A systematic approach for adversarial testing of 4g lte," in *Network and Distributed Systems Security (NDSS) Symposium 2018*, 2018.

[6] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4g and 5g cellular paging protocols using side channel information," *Network and distributed systems security (NDSS) symposium2019*, 2019.

[7] A. Shaik, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," *arXiv preprint arXiv:1510.07563*, 2015.

[8] G.-H. Tu, C.-Y. Li, C. Peng, Y. Li, and S. Lu, "New security threats caused by ims-based sms service in 4g lte networks," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 1118–1130.

[9] S. Chalakkal, H. Schmidt, and S. Park, "Practical attacks on volte and vowifi," *ERNW Enno Rey Netzwerke, Tech. Rep*, 2017.

[10] A. Al Ishtiaq, S. S. S. Das, S. M. M. Rashid, A. Ranjbar, K. Tu, T. Wu, Z. Song, W. Wang, M. Akon, R. Zhang *et al.*, "Hermes: unlocking security analysis of cellular network protocols by synthesizing finite state machines from natural language specifications," in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024, pp. 4445–4462.

[11] S. F. Mjølsnes and R. F. Olimid, "Easy 4g/lte imsi catchers for non-programmers," in *Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings 7*. Springer, 2017, pp. 235–246.

[12] S. P. Rao, B. T. Kotte, and S. Holtmanns, “Privacy in lte networks,” in *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, 2016, pp. 176–183.

[13] S. P. Rao, I. Oliver, S. Holtmanns, and T. Aura, “We know where you are!” in *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE, 2016, pp. 277–293.

[14] F. Van Den Broek, R. Verdult, and J. De Ruiter, “Defeating imsi catchers,” in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 340–351.

[15] Y. Chen, D. Tang, Y. Yao, M. Zha, X. Wang, X. Liu, H. Tang, and B. Liu, “Sherlock on specs: Building {LTE} conformance tests through automated reasoning,” in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 3529–3545.

[16] A. Dabrowski, G. Petzl, and E. R. Weippl, “The messenger shoots back: Network operator based imsi catcher detection,” in *Research in Attacks, Intrusions, and Defenses: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings 19*. Springer, 2016, pp. 279–302.

[17] R. P. Jover, “Lte security, protocol exploits and location tracking experimentation with low-cost software radio,” *arXiv preprint arXiv:1607.05171*, 2016.

[18] M. S. A. Khan and C. J. Mitchell, “Trashing imsi catchers in mobile networks,” in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017, pp. 207–218.

[19] K. Norrman, M. N¨”””aslund, and E. Dubrova, “Protecting imsi and user privacy in 5g networks,” in *Proceedings of the 9th EAI international conference on mobile multimedia communications*, 2016, pp. 159–166.

[20] S. Holtmanns, S. P. Rao, and I. Oliver, “User location tracking attacks for lte networks using the interworking functionality,” in *2016 IFIP Networking conference (IFIP Networking) and workshops*. IEEE, 2016, pp. 315–322.

[21] K. Kohls, D. Rupprecht, T. Holz, and C. P¨”””opper, “Lost traffic encryption: fingerprinting lte/4g traffic on layer two,” in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 249–260.

[22] D. Rupprecht, K. Kohls, T. Holz, and C. P¨”””opper, “Breaking lte on layer two,” in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 1121–1136.

[23] T. Tucker, N. Bennett, M. Kotuliak, S. Erni, S. Capkun, K. Butler, and P. Traynor, “Detecting imsi-catchers by characterizing identity exposing messages in cellular traffic,” in *Network and Distributed System Security (NDSS) Symposium 2025*. Internet Society, 2025, p. 1115.

[24] M. Bartock, J. Cichonski, M. Souppaya, K. Scarfone, P. Grayeli, S. Sharma, and C. Teague, “Protecting subscriber identifiers with subscription concealed identifier (suci): Applying 5g cybersecurity and privacy capabilities (draft),” US Department of Commerce, Tech. Rep., 2024.

[25] 3GPP, “Ts23.501: System architecture for the 5g system (5gs),” Mar. 2025.

[26] ——, “TS33.401: 3GPP System Architecture Evolution (SAE); Security architecture,” Sep. 2024.

[27] ——, “Ts33.501: Security architecture and procedures for 5g system,” Sep. 2024.

[28] ——, “Ts36.331: Evolved universal terrestrial radio access (e-utra); radio resource control (rrc); protocol specification,” Mar. 2025.

[29] ——, “Ts38.331: Nr; radio resource control (rrc); protocol specification,” Mar. 2025.

[30] ——, “Ts36.321: E-utra medium access control (mac) protocol specification,” Jan. 2024.

[31] ——, “Ts23.303: Proximity-based services (prose); stage 2,” Apr. 2024.

[32] ——, “Ts36.300: E-utra and e-utran; overall description,” Dec. 2024.

[33] ——, “TS23.003: Numbering, addressing and identification,” Sep. 2024.

[34] IANA, “Private enterprise numbers,” May 2025.

[35] 3GPP, “TS24.501: Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3,” Sep. 2024.

[36] ——, “TS24.301: Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3,” Sep. 2024.

[37] Y. Li, C. Peng, Z. Yuan, J. Li, H. Deng, and T. Wang, “Mobileinsight: Extracting and analyzing cellular network information on smartphones,” in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, 2016, pp. 202–215.

[38] 3GPP, “Ts33.503: Security aspects of proximity based services (prose) in the 5g system (5gs),” Sep. 2024.