Uncovering Problematic Designs Hindering Ubiquitous Cellular Emergency Services Access

Yiwen Hu*, Min-Yue Chen*, Haitian Yan*, Chuan-Yi Cheng‡, Guan-Hua Tu*, Chi-Yu Li‡, Tian Xie◇, Chunyi Peng△, Li Xiao*, Jiliang Tang*

*Michigan State University, ‡National Yang Ming Chiao Tung University,
◇ Utah State University, △Purdue University

ABSTRACT

Cellular networks provide the most accessible emergency services with ubiquitous coverage, yet their emergency-specific designs remain largely unexplored. To systematically explore potential design defects that lead to failures or delays in emergency services, we introduce M911-Verifier, an emergency-specific model checking tool. It reveals many counterintuitive findings regarding the ubiquitous access support for cellular emergency services. Our study shows that, despite sufficient wireless signal coverage, users may still experience prolonged emergency call setup times, call initiation failures, or call drops due to flaws in the design of cellular emergency services. These design defects arise from three major causes: problematic network selection for initiating emergency calls, emergency-unaware call operation, and network escalation forbidden during emergency calls. The impacts of these defects have been experimentally validated across three U.S. carriers and two Taiwan carriers using commodity smartphones. Finally, we propose solutions and evaluate their effectiveness.

CCS CONCEPTS

• **Networks → Mobile networks**; **Network management**.

KEYWORDS

Emergency Services, 911 (9-1-1), Mobility, Cellular Networks

ACM Reference Format:
Yiwen Hu*, Min-Yue Chen*, Haitian Yan*, Chuan-Yi Cheng‡, Guan-Hua Tu*,, Chi-Yu Li‡, Tian Xie◇, Chunyi Peng△, Li Xiao*, Jiliang Tang*. 2024. Uncovering Problematic Designs Hindering Ubiquitous Cellular Emergency Services Access. In *The 30th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '24), November 18–22, 2024, Washington D.C., DC, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3636534.3690704

ACM MobiCom '24, November 18–22, 2024, Washington D.C., DC, USA
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0489-5/24/11
https://doi.org/10.1145/3636534.3690704

1 INTRODUCTION

Emergency services are vital lifelines for individuals facing emergencies. The most accessible channels are through cellular networks due to their ubiquitous coverage. Both regulatory authorities like the FCC in the U.S. and standard organizations such as 3GPP have stipulated specifications to enhance the availability and effectiveness of these cellular emergency services. For example, the FCC [52] in the U.S. requires carriers to transmit all 911 calls to a Public Safety Answering Point (PSAP, e.g., 911 call center), regardless of whether the caller subscribes to them or not. 3GPP [8, 10, 17] allows User Equipment (UE) to access emergency services across heterogeneous networks, including all available 3GPP Radio Access Networks (RANs) such as 5G/4G Base Stations (BSs), non-3GPP RANs like Wi-Fi BS, as well as cellular systems from different generations (e.g., 5G/4G) and Public Land Mobile Networks (PLMNs) like AT&T and Verizon.

However, the comprehensive support of cellular emergency services is a double-edged sword. While it allows for ubiquitous access, the corresponding network functions across cellular networks/systems are numerous and complex in their interactions, rendering cellular emergency services prone to errors. Despite many studies [36, 47, 48, 59, 60] examining the performance and effectiveness of ubiquitous mobile services, emergency services have not yet been fully studied. These services rely on emergency-specific mechanisms, differing from non-emergency ones, which encompass network selection for initiating emergency calls to handover among RANs, systems, and networks during mobility.

In this study, we develop M911-Verifier, an emergency-specific model checking tool, to assess support for ubiquitous access to cellular emergency services and identify potential defects in 3GPP standard designs. While most emergency-specific designs function properly, we uncover several counterintuitive findings where users, despite sufficient wireless coverage, experience long emergency call setup times, call initiation failures, or call drops due to design flaws in cellular emergency services. We identify 11 such defects, summarized

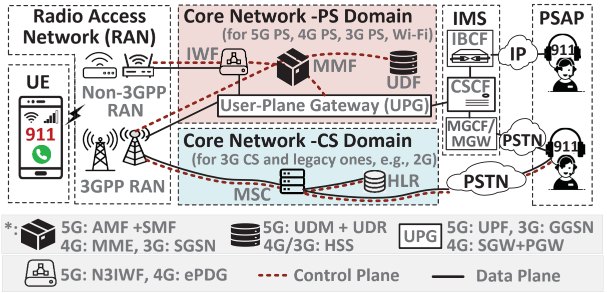


Figure 1: Cellular emergency service architecture.

in Table 2 (§5), categorized into problematic network selection for initiating emergency calls (§6), emergency-unaware 9-1-1 call operation (§7), and network escalation forbidden during emergency calls (§8). Experimental validation reveals that these design defects can significantly impact emergency services, leading to failures and delays.

Specifically, 3GPP allows cellular emergency calls via both cellular and Wi-Fi networks, but its problematic network selection can prevent 90% of indoor emergency calls from reaching PSAPs within 2 minutes, compared to just 5.85 seconds for non-emergency calls in the same locations. Moreover, emergency call failures and drops during mobility, even with sufficient coverage, are linked to other design defects, posing serious risks to emergency users. All validation experiments were conducted with three top-tier U.S. carriers, two major carriers in Taiwan, campus Wi-Fi, and four carrier-certified phone models. Importantly, we employed a responsible methodology with ethical consideration to avoid routing calls to PSAPs during these experiments. We also proposed solutions to address these issues.

This paper makes three key contributions: (1) it presents the first study using model checking techniques to explore design flaws that hinder access to cellular emergency services; (2) it uncovers 11 new design defects, 9 of which were validated experimentally, revealing that even with sufficient wireless coverage, emergency users may face prolonged call setup times, call initiation failures, or call drops, posing public safety risks; and (3) it proposes standard-compliant, low-infrastructure-support solutions, evaluated through a prototype. The lessons learned offer valuable insights for improving emergency services for billions of cellular users.

2 BACKGROUND

Heterogeneous Cellular Architecture Supporting Emergency Services. Figure 1 illustrates the heterogeneous cellular network architecture, enabling UE to access emergency services across various RANs and network domains. The former includes 3GPP RANs, such as 5G/4G/3G BSs, and non-3GPP RANs, such as Wi-Fi BS. The latter is classified into two domains, PS (Packet-Switched) and CS (Circuit-Switched). The PS domain contains 5G/4G/3G systems, whereas the CS domain supports legacy 3G systems. To reach the PSAP, emergency call requests can be delivered through two paths from RANs: (1) the PS domain, IP Multimedia Subsystem (IMS), and Public Switched Telephone Network (PSTN) or IP networks; and (2) the CS domain and PSTN.

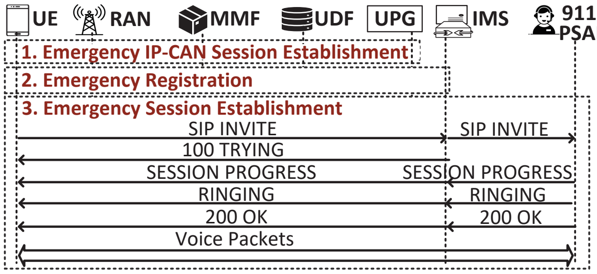


Figure 2: Emergency service flow.

We next introduce key network elements in the cellular network architecture. For simplicity, we intentionally avoid telecom jargon and use generic names for network entities that have similar network functions. In the PS core network, User-Plane Gateway (UPG) routes packets between the UE/RAN and IMS in the user plane. In the control plane, the Mobility Management Function (MMF) [13, 14] manages user mobility, authentication, and session connectivity, including emergency IP connectivity. The User Data Function (UDF) [4, 20] stores user and service subscription information to assist the MMF in user authentication. The Inter-working Function (IWF) [9, 11] serves as a gateway for the UE to access the PS core network over non-3GPP RANs by establishing IPsec connections. In the CS core network, there are two key elements: the Mobile Switching Center (MSC) [12] and the Home Location Register (HLR). The MSC manages voice/text/emergency services, user mobility, and authentication, while the HLR functions similarly to the UDF.

The IMS facilitates emergency voice and text services over IP. It comprises three primary network entities: the Call Session Control Function (CSCF, hereafter referred to as the IMS server), the Media Gateway Control Function/Media Gateway (MGCF/MGW), and the Interconnect Border Control Function (IBCF). The IMS server manages IMS service signaling, utilizing the Session Initiation Protocol (SIP) [55]. The MGCF/MGW connects to the traditional PSTN, while the IBCF serves as a session border controller interconnected with other IP/IMS networks.

Emergency Service Flow. Emergency UEs can initiate cellular emergency services over 5G/4G/3G networks [8, 10, 12] from both home and visited PLMNs [8, 10], and Wi-Fi networks from the home PLMN. Figure 2 illustrates the initialization procedure for PS-based emergency services over 5G/4G networks. To establish an emergency session with the PSAP, an emergency UE needs to perform the following three actions: (1) *establishing an emergency IP-CAN session connectivity* with the UPG; (2) doing *emergency registration*

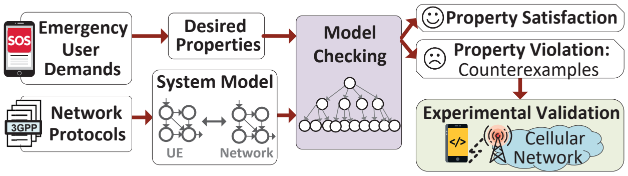


Figure 3: The overview of M911-Verifier.

and authentication with the IMS server [6, 17]; (3) *establishing an IMS emergency session* with the PSAP [6, 17, 32, 33]. Afterwards, the UE sends a SIP INVITE message to the IMS server to set up an emergency call session. Notably, anonymous UEs are still allowed to access the IMS emergency service without being registered, in accordance with local regulatory requirements [19].

3 M911-VERIFIER

In this section, we propose M911-Verifier, an emergency-specific model checking framework, to systematically explore the issues arising from ubiquitous access to cellular emergency services. It aims to identify design flaws stemming from the 3GPP standard that could result in emergency service failures or delays. Below, we present an overview of M911-Verifier, technical challenges in its development, and the corresponding designed approaches, along with details on its implementation and evaluation.

3.1 Overview of M911-Verifier

Figure 3 shows the framework of M911-Verifier. It begins by identifying emergency user demands from emergency use scenarios and their corresponding user expectations. Subsequently, desired properties are defined based on these demands. The protocol interactions for providing emergency services and managing user mobility, as per the 3GPP standard, are then modeled. The model checker utilizes these desired properties and modeled systems for protocol screening. Any counterexamples that violate the desired properties could be identified, revealing potential design defects. Finally, these design defects are validated through experiments.

We next present the modeling of network protocols and emergency use scenarios, along with the desired properties and the method for checking these properties.

Modeling of Network Protocols. We implement protocols related to radio access [16, 22, 25], PS/CS services [12–14], mobility [8–11, 13, 14], and emergency services [12, 17], in adherence to the 3GPP standard. Specifically, each protocol (e.g., EPS Mobility Management (EMM)/EPS Session Management (ESM) [13]) is modeled as two finite state machines (FSMs): one operating at the UE and the other within the network architecture, or across two networks. The interaction between each protocol’s two FSMs is facilitated by cellular messages transmitted over two unidirectional uplink and downlink channels. To reduce the complexity of protocol modeling, we focus on critical states and messages pertinent to emergency services, while omitting less relevant elements, such as charging mechanisms for these services.

Cellular message transmission loss is simulated to mirror real-world wireless conditions. Unlike conventional model-checking tools like SPIN [37, 51], which typically use a constant loss rate (e.g., 50%), our approach correlates transmission loss with signal strength, establishing an inverse proportional relationship. As simulated signal strength fluctuates between 0 and 10, the transmission loss rate varies from 100% to 0%, respectively.

We explore all possible outcomes for an FSM when receiving a request, including acceptance or rejection due to various standard-defined error causes. For example, the 4G attach procedure [13] specifies over 30 potential error causes, each triggering a unique UE or network response. In our model, if a rejection occurs, an error cause is randomly assigned, allowing us to explore all potential error scenarios.

Modeling of Use Scenarios. We model the behaviors of an emergency service user accessing cellular networks, driving state transitions in the FSMs of cellular network protocols. The four major behavioral patterns include: (1) the UE connects to at most one cellular network system (e.g., 4G and 5G); (2) the user may power their UE on or off at any time, initiating the attach or detach procedures; (3) the user may request access to cellular emergency services at any time; and (4) the user may move from one RAN to another, triggering inter/intra-RAT or inter-system handovers (e.g., 4G→5G).

Each use scenario, composed of different behavior patterns, is transformed into a series of time events (e.g., powering on the UE at t_0, dialing a voice call at t_1, and triggering an inter-RAT handover at t_{i-1}). These events are then fed into the M911-Verifier during property checking, driving all potential state transitions for the modeled scenarios.

Desired Properties. The desired properties address user needs and regulatory requirements for emergency services.

- (φ_1) Availablity_Guaranteed: The cellular network shall accept any emergency service request whenever any of its connected RANs is available to the requesting UE, regardless of the UE’s subscription status.
- (φ_2) Continuity_Guaranteed: An established emergency session over the cellular network shall not be interrupted under any circumstances, especially during UE mobility. Handovers among RANs and systems shall ensure that emergency services remain uninterrupted.
- (φ_3) Applicable_Access_Guaranteed: To establish an emergency session with the PSAP before reaching the failure limit, a RAN, whether 3GPP or non-3GPP, must be selected with signals stronger than the weakest signal among the RANs that can maintain stable non-emergency services.
- (φ_4) Limited_Session_Establishment: The number of failed attempts to establish an emergency session with the PSAP shall not exceed a pre-defined threshold.

Property Checking. The model checker initiates the entire state space by intertwining all FSMs for individual protocols. In each scenario, the signal generator constructs a sequence of initial signaling messages, which determine the initial states of the model. Subsequently, the depth-first algorithm is employed to navigate through state transitions from the initial states across various use scenarios. Particularly, when encountering multiple output signaling messages for a state, a new branch is generated from this state for each message. For instance, upon receiving an RRC connection setup request, both acceptance and rejection messages are taken into account. This approach ensures testing of all possible cases for the responses. Furthermore, our implementation considers two potential outcomes for each message delivery: success and loss, contingent upon the signal strength of the serving cell. This methodology aids in comprehending the behavior of signaling protocols in the face of signaling loss or corruption. Consequently, we enumerate all potential message delivery scenarios in a dynamic network environment.

3.2 Challenges and Our Approaches

The model checking technique has gained popularity in recent years for systematically examining cellular network protocols [28, 38, 40, 41, 45, 58]. However, these prior studies usually focus on cellular network protocols within a single cellular network system (e.g., 3G or 4G). In contrast, modeling cellular emergency services introduces more heterogeneity and complexity, as some regulatory authorities (e.g., FCC) allow UEs to access emergency services without UE identity validation [52]. This involves not only system-wide protocols but also spans multiple cellular network systems, RANs, and PLMNs, creating new challenges. Below, we present two technical challenges and the corresponding approaches when developing M911-Verifier.

Challenge 1: Diverse Use Scenarios. Emergency services can be initiated from both home and visited PLMNs, differing from non-emergency services, which are usually accessed through home PLMNs. Furthermore, only emergency services can be accessed by anonymous UEs without UE identity validation. The cellular network supporting emergency services can be heterogeneous, involving different systems and RANs. For each UE, wireless RAN signals fluctuate over time due to wireless dynamics and UE mobility. These environmental factors may impede the UE from selecting an appropriate network, involving a system and a RAN, to initiate emergency services. While undergoing handovers among systems and RANs, the continuity of emergency services must still be maintained. Thus, it is challenging to model all possible use scenarios for emergency UEs.

⋄ **Adaptive Emergency Scenario Modeling.** We adopt an adaptive scenario modeling approach to cover diverse emergency user scenarios, including both stationary and mobile users. Varying cell signal strength is primarily executed for UEs accessing emergency services, aiming to trigger different network selections and handovers [16, 22, 25]. Changes in signal strength can impact network selection for initiating emergency services and cause various handovers during ongoing emergency sessions.

Specifically, M911-Verifier manages a list of cells from different RANs (e.g., 4G, 5G, and Wi-Fi). During property checking, it assigns a random signal strength value ranging from 0 (no signal) to 10 (strongest signal) to each cell. This random assignment occurs periodically after initiation. Although this may not perfectly mirror real-world conditions (e.g., sudden changes from 10 to 0), validation experiments will be conducted to verify if identified counterexamples occur in operational cellular networks.

Challenge 2: Inefficient Property Checking. Recent advancements in model-checking techniques have proven effective in identifying design defects within cellular network protocols and services. For example, Hussain et al. [40] developed *LTEInspector*, a model-checking tool designed to examine security and privacy issues in the 4G LTE Radio Resource Control (RRC) and EMM protocols. Basin et al. [28] and Cremers et al. [31] conducted a formal analysis of the 5G authentication and key agreement protocol. Additionally, Klischies et al. [45] proposed a model-checking-based approach to detect undefined behaviors in the 4G LTE standard.

However, these techniques share a fundamental limitation: they are vulnerable to state explosion, which restricts their applicability in analyzing complex communication systems, as opposed to focusing solely on specific protocols. Typically, when conducting property checking, a model checker generates a complete state space and then checks for violations of the desired properties under various scenarios. This approach becomes increasingly inefficient when applied to cellular emergency services, which require enabling emergency UEs to access all available 3GPP and non-3GPP RANs, cellular systems, and PLMNs. Such system-wide collaboration may result in an overwhelmingly large model, leading to severe state explosion during property checking.

Moreover, the common solutions adopted to resolve state explosion include abstraction and bounded checking (e.g., exploring only 250 steps). However, when full-path testing is not feasible but bounded checking is employed due to the state explosion problem, property violations may occur early or only in a limited set of procedures, which limits further exploration and leads to inefficient property checking.

⋄ **Dynamic Checker Loading.** We deliberately avoid implementing an extensive cellular network model that interconnects all potentially involved FSMs. Instead, we adopt a procedure-oriented approach to modeling the cellular network. For example, a 5G network supporting emergency services must accommodate various procedures, including registration, PDU session establishment, 5G/4G RAN handover, and emergency service fallback. These procedures are modeled individually and stored in a model storage center.

The procedure-oriented approach follows a hybrid method, utilizing full-path testing exclusively for emergency service procedures, while applying bounded checking to the systems that initiate emergency services. The models for emergency service procedures are overseen by the protocol screening controller, which operates based on specific use scenarios. The controller loads the modeled UE and infrastructure procedures corresponding to the use scenarios. The loaded models perform property checking using full-path testing. The outputs from each procedure model are then fed into the next loaded model. This dynamic checker loading approach allows property checking to focus on multiple small, procedure-oriented models, rather than a single extensive model. Moreover, each model undergoes thorough examination before being invoked by the controller to collaborate with other models, thereby enabling more efficient property checking.

3.3 Implementation and Evaluation

We implement two major components for M911-Verifier using Python and SPIN [37], a widely used model-checking tool for network protocol verification [54, 56, 58]: a protocol screening controller and a suite of models representing emergency service procedures. Based on received messages or user events (e.g., dialing emergency calls and powering off the UE), the controller either loads the corresponding UE and/or infrastructure procedures for property checking or updates network environment settings (e.g., adjusting cell signal strength). A property checking run ends either when a property violation is detected in any loaded procedure model or when the maximum number of steps is reached by the controller (e.g., 250 procedure loadings). Notably, SPIN performs full-path testing with a maximum of 10,000 steps and truncates the search if this limit is reached [57].

We then evaluate M911-Verifier in terms of its coverage and efficiency across emergency use scenarios, comparing it to traditional model checkers that implement all procedures in a single giant model [38]. We configure M911-Verifier to perform 100,000 property-checking runs. Each procedure model in M911-Verifier is subjected to full-path testing with a maximum of 10,000 steps, in line with the implementation limits of SPIN. Additionally, a 250-step bounded checking is applied to both the screening controller and the giant model.

Coverage of Emergency Use Scenarios. We assess coverage by analyzing the traces generated by M911-Verifier and the giant model. Our analysis yields two key findings. First, M911-Verifier successfully captures all emergency use scenarios permitted by the 3GPP standard. For stationary scenarios, four types of emergency call initiations from different networks are identified: 5G, 4G, 3G, and Wi-Fi. For non-stationary scenarios, we observe 20 types of inter-RAT handovers (e.g., from 5G to 4G) and 5 types of intra-RAT handovers (e.g., from 5G to 5G) during ongoing emergency calls, totaling 25, as summarized in Table 1. Second, M911-Verifier not only captures a greater number of use scenarios than the giant model but also demonstrates superior efficiency. As illustrated in Figure 4, after the first 10,000 runs, 23 out of 29 scenarios (4 stationary and 25 non-stationary) are observed with M911-Verifier, compared to only 11 scenarios observed with the giant model.

Source \ Dest.		5G	4G	3G		Wi-Fi
				PS	CS	
5G		○	○	○	○†	○
4G		○	○	○	○†	○
3G	PS	○	○	○	○†	○
	CS	○†	○†	○†	○	○‡
Wi-Fi		○	○	○	○‡	○

†: Refer to Single Radio Voice Call Continuity (SRVCC) design in [18].
‡: Refer to Dual Radio Voice Call Continuity (DRVCC) design in [7].

Table 1: Summary of non-stationary emergency service use scenarios observed on M911-Verifier.

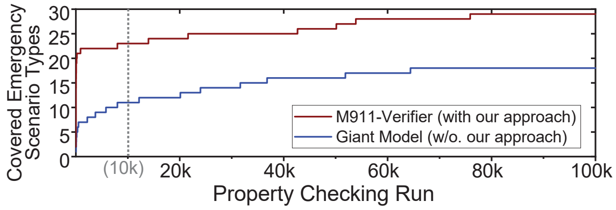


Figure 4: Number of emergency use scenarios increases with property checking runs.

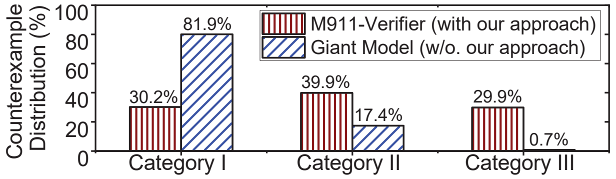


Figure 5: Counterexample distributions for each category of UE status at termination of property checking.

Property Checking Efficiency. We next evaluate the efficiency of property checking with M911-Verifier by analyzing the distribution of counterexamples, which indicates how efficiently counterexamples can be generated under different termination conditions. The property checking runs are classified into three categories based on the UE status at termination: (1) no emergency calls are successfully made; (2) at least one emergency call is successfully made; and (3) at least one handover is observed during an ongoing emergency call. Figure 5 illustrates the counterexample distributions from both M911-Verifier and the giant model. The results show that M911-Verifier identifies counterexamples more efficiently across all categories compared to the giant model. Specifically, M911-Verifier's counterexamples are distributed as follows: 30.2% in Category I, 39.9% in Category II, and 29.9% in Category III, compared to the giant model's 81.9%, 17.4%, and 0.7%, respectively. This suggests that the giant model may overlook counterexamples in the last two categories, which are crucial for emergency use scenarios.

With this efficient property checking, we identified several design defects that were previously undiscovered or unreported by other studies. Details will be provided in §5.

4 EXPERIMENTAL METHODOLOGY

To validate all potential design defects identified by M911-Verifier, we designed corresponding experiments conducted on two campuses. These experiments utilized both campus Wi-Fi and operational cellular networks: three operators from the U.S. (designated as US-I, US-II, and US-III) and two operators from Taiwan (TW-I and TW-II). Four carrier-certified phone models were employed: Samsung Galaxy S21, Google Pixel 5, LG G8X, and Motorola G Stylus 5G. Our validation experiments encompassed both 3GPP and non-3GPP networks, including 5G, 4G, 3G, and Wi-Fi networks.

Ethical Consideration and Responsible Methodology. We understand the potential risks validation experiments pose to cellular networks and users. To mitigate these, we conducted our preliminary study responsibly with three key approaches: (1) *No emergency calls were delivered to PSAPs at any point during our experiments*, ensuring that emergency services were not disrupted. To facilitate this, we developed a smartphone application named Emerg-Call-Blocker[1], which, with root privileges, effectively prevents 5G/4G/3G emergency calls from reaching PSAPs. (2) We subscribed to unlimited service plans for all experimental devices and minimized resource consumption. (3) Our experiments were small-scale, focused on validating design flaws without causing harm.

Specifically, Emerg-Call-Blocker intercepts and discards all SIP-based emergency call signaling messages by monitoring all network interfaces on each test phone. Each emergency call attempt fails when any SIP REGISTER/INVITE message sent by the IMS client application is blocked by Emerg-Call-Blocker. It is important to note that REGISTER and INVITE messages are used by subscribed and anonymous UEs, respectively, to initiate emergency calls, as anonymous UEs do not need SIP registration.

However, if the phone fails to initiate 4G/5G emergency calls via the IMS client application, it may attempt to dial 3G emergency calls through cellular modems using legacy 3G CS call signaling, such as CC Setup[12], thereby bypassing Emerg-Call-Blocker's SIP-based call signaling interception. To address this, we employ Cellular Pro[26], an application designed to collect cellular network signaling from cellular modems. We detect and terminate connection attempts (e.g., RRC connection establishment) by monitoring signaling messages displayed on the phone screen using Optical Character Recognition (OCR) [49], effectively blocking these 3G emergency calls as well. Thus, none of the emergency calls can complete initialization or be made.

Emerg-Call-Blocker allows us to responsibly measure the emergency call setup time for validation experiments. This time is measured from the moment a user presses the dial button on the phone to the interception of the SIP REGISTER/INVITE message that initiates the emergency call. Therefore, the measured emergency call setup times are a few seconds shorter than the actual times would be.

Accountable Disclosure[2]. We contacted the involved parties, including operators and 3GPP standardization organizations, to share our validated design defects along with proposed solutions. Additionally, we provided design defects that were uncovered but not validated, either due to ethical considerations or limited access to the necessary infrastructure and mobile devices, for their internal analysis.

5 OVERVIEW OF FINDINGS

Through the analysis of M911-Verifier's counterexamples, we identified 11 previously unreported defects that can be experimentally validated, as summarized in Table 2. Notably, Table 2 did not cover all potential defects for the following reasons. First, M911-Verifier did not implement full-path testing across all possible scenarios but instead used a hybrid approach to mitigate state explosion, meaning some defects may still be undetected, despite uncovering more issues than prior arts. Second, some identified defects cannot be experimentally validated without support from cellular infrastructure or device modification. This study, however, focuses mainly on those defects that can be practically validated. Moreover, it is worth noting that the traces of our counterexamples match the UE and network behaviors observed during experimental validation, which confirms the modeling accuracy of M911-Verifier.

We detail the three categories of identified defects below.

Problematic Network Selection for Initiating Emergency Calls. In this category, the UE's network selections among 3GPP and non-3GPP RANs within a PLMN for initiating emergency calls do not always function properly. These counterexamples can lead to prolonged setup times for emergency calls. They can be grouped into five instances. NS-1 and NS-2, violating the properties of Applicable_Access _Guaranteed or/and Limited_Session_Establishment, can skip the best or only use bearable RAN and select nonexistent 3G RANs, respectively. In NS-3, subscribed UEs have fewer options than anonymous UEs, violating the property of Limited_Session_Establishment. For NS-4 and NS-5, both violating the property of Availablity_Guaranteed, the initiation of emergency calls may be rejected due to the prior

[1] The applications developed in this paper, including Emerg-Call-Blocker and Emerg-Call-Dialer, can be downloaded from [27].

[2] Note that we presented our methodology to our institution's IRB office for review. The IRB granted a waiver, as the study did not involve any human subjects.

Category	ID	Description	Property Violation	Root causes	Vali-dated?
Problematic Network Selection for Initiating Emergency Calls (§6)	NS-1	UEs skip the best or only use bearable RAN, leading to long call setup times (e.g., 120 seconds) or failures.	φ_3, φ_4	The 3GPP standards [9, 10] prohibit UEs from making emergency calls through non-3GPP RANs when any 3GPP RAN is available.	○
	NS-2	UEs attempt to initiate emergency services from 3G RANs when there are no 3G RANs deployed nearby.	φ_3, φ_4	The 3GPP standard [17] uses the UE's registration status in the core network, rather than its RAN status, to determine the emergency service domain (PS/CS).	○
	NS-3	Subscribed UEs have fewer network/system selections than anonymous UEs when dialing emergency calls.	φ_4	Subscribed UEs must prioritize their home PLMN for accessing emergency services [5], whereas anonymous UEs can use all available PLMNs.	○
	NS-4	The initiation of emergency calls may be rejected due to the prior improper session termination.	φ_1	The 3GPP standard [10] only allows a UE to establish a single emergency session with PSAPs, either over 3GPP or non-3GPP RAN.	×
	NS-5	Anonymous UEs cannot initiate emergency service through non-3GPP RAN (e.g., Wi-Fi).	φ_1	Due to security concerns, 3GPP standard [17] prohibits UEs without a security context from accessing emergency services via non-3GPP RAN.	○
Emergency-unaware 9-1-1 Call Operation (§7)	EU-1	Emergency requests may be rejected by the network.	φ_1	Not all NAS (Non-Access-Stratum) signalings between the emergency UE and the cellular infrastructure indicate the emergency usage.	○
	EU-2	Emergency UEs are not always permitted to initiate emergency attach procedure to the network.	φ_1	The emergency attach is only permitted when the UE is in certain states, such as EMM-DEREGISTERED.LIMITED-SERVICE.	○
	EU-3	The emergency UE's requests may be rejected by non-3GPP RAN (e.g., Wi-Fi).	φ_1	According to Wi-Fi standards [43], not all Wi-Fi signalings can indicate the emergency usage, leaving service providers unaware of emergency services.	○
Network Escalation Forbidden During Emergency Calls (§8)	NF-1	An emergency call drops when the emergency UE moves from a 4G cell to 5G a cell.	φ_2	The 3GPP standard [11] prohibits the occurrence of 4G to 5G inter-system handover during emergency calls.	×
	NF-2	An emergency call may drop when the emergency UE moves from a 3G cell to a 4G/5G cell.	φ_2	The 3GPP standard [17] prohibits the occurrence of 3G CS to 4G/5G PS inter-domain handover during emergency calls.	○†
	NF-3	An emergency call drops when the emergency UE moves from one PLMN to another.	φ_2	Seamless inter-PLMN handover for emergency call continuity is not supported.	○†

Property φ_1: Availablity_Guaranteed, Property φ_2: Continuity_Guaranteed, Property φ_3: Applicable_Access_Guaranteed, Property φ_4: Limited_Session_Establishment
○: Validated using emergency service initiation. ○†: Validated using non-emergency services since they share the same standards with non-emergency ones.
×: No validation results due to ethical issues.

Table 2: Summary of findings identified by M911-Verifier.

improper session termination, and anonymous UEs cannot initiate emergency services through non-3GPP RANs due to the absence of their security context, respectively.

Emergency-unaware 9-1-1 Call Operation. This category contains counterexamples from three design defects violating the property of Availability_Guaranteed, which can be attributed to some emergency-unaware operations for initiating emergency services in some cases. These counterexamples can cause emergency service requests to be rejected by the network, leading to unnecessary delays up to several minutes. Specifically, in EU-1 and EU-3, not all the signaling messages sent by emergency UEs indicate emergency usage. EU-2 presents that an emergency attach is not always permitted but only in certain states.

Network Escalation Forbidden During Emergency Calls. Counterexamples here violate the Continuity_Guaranteed property, attributed to the forbidden network escalation during emergency calls. Certain handovers for emergency services are prohibited, resulting in the potential dropping of ongoing emergency sessions during mobility. Three prohibited handovers include: (1) 4G to 5G inter-system handover in NF-1; (2) 3G CS to 4G/5G PS inter-system handover in NF-2; (3) inter-PLMN handover in NF-3.

We next present seven representative design defects and analyze their root causes: NS-1, NS-2, and NS-3 in §6; EU-1 and EU-2 in §7; and NF-1 and NF-2 in §8.

6 PROBLEMATIC NETWORK SELECTION FOR INITIATING EMERGENCY CALLS

Cellular networks ensure ubiquitous coverage by allowing UEs to access mobile services via 3GPP (e.g., 4G, 5G) and non-3GPP (e.g., Wi-Fi) radio technologies. The 3GPP standard [2, 5, 9–11, 15, 18, 21, 24] stipulates network selection and handover mechanisms across these technologies, ensuring carrier-grade service quality. However, M911-Verifier discovers that some network selection mechanisms perform problematically when initiating emergency calls.

In the following, we present the identified issues from two major network selection scenarios: (1) problematic UE restriction on network selection among 3GPP and non-3GPP radio access networks within the same PLMN; and (2) unfair UE limitation on network selection across home PLMN and visited PLMN. The issues are then experimentally validated and analyzed for their root causes.

6.1 Inferior to Non-Emergency Calls - Restrictions within PLMN

Cellular emergency calls can be made through both 3GPP and non-3GPP RANs. Logically, even when a UE has poor connectivity to 3GPP RANs, emergency call setup times may not be prolonged if there is strong connectivity from non-3GPP RANs (e.g., Wi-Fi). However, 3GPP standards [9, 10] prohibit UEs from making emergency calls through non-3GPP RANs when any 3GPP RAN is available. This restriction applies specifically to emergency services. It appears reasonable, since 3GPP RANs are generally considered more reliable, and non-3GPP RANs can still be accessed if 3GPP RANs fail to provide emergency service.

However, this restriction poses practical problems. It prioritizes any available 3GPP RAN over non-3GPP RANs, regardless of the 3GPP RAN's connection quality, even if it provides a poor signal to the UE. This can lead to prolonged emergency call setup times, exacerbating certain emergency situations. For example, when a UE attempts to access a 4G RAN with weak signals, it may experience up to 8 RRC connection establishment failures, with up to 64 seconds [22] spent before switching to another RAN.

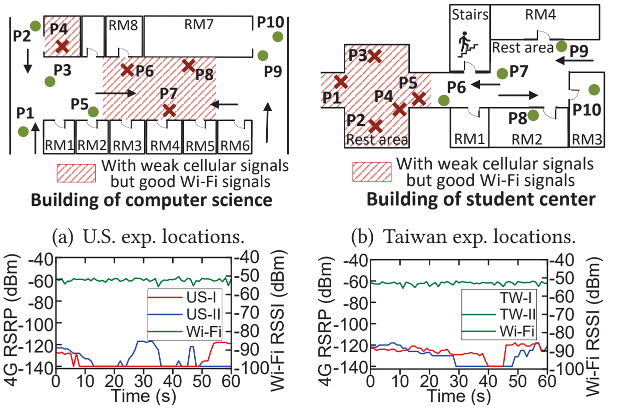
This problematic restriction, "3GPP-always-preferred", leads M911-Verifier to discover counterexamples that violate two major properties, namely Applicable_Access_Guaranteed and Limited_Session_Establishment. All the violations occur when UEs connect to 3GPP RANs with poor or near-deadzone signal strength. We next present two observed frequent cases illustrating the property violation.

◇ **Skipping the Best or Only Using Bearable RAN.** It is observed that UEs usually skip the best RAN or only use a bearable RAN when initiating emergency services. This behavior can lead to the violation of those two properties, causing long call setup times and poor service quality for emergency services. There are two key observations. First, in most of the counterexamples, UEs encounter the maximum number of attempt failures for accessing 3GPP RANs, even though they observe stronger signals from non-3GPP RANs. Second, even when considering only 3GPP RANs, UEs may still skip the best, since the 3GPP standard leaves the decision of 3GPP RAN connectivity to UE implementation.

Moreover, to initiate an inter-system switch for accessing emergency services over 3GPP RANs with better signal strength, a UE has only two options: (1) fallback from 5G to 4G , and (2) fallback from 4G to 3G. These limited switch options impede considering all available 3GPP RANs.

◇ **Selecting Nonexistent RANs.** Another observation is that UEs may attempt to initiate emergency services from the 3G CS domain even when there are no 3G RANs deployed nearby. This also violates the aforementioned two properties. This issue stems from a problematic domain selection rule in the 3GPP standard [17]. The rule specifies that, given the PS/CS network registration statuses and the availability of VoIMS and emergency services—namely "CS is Attached," "PS is Attached," "VoIMS is Supported," and "EMS (Emergency Service) is Supported"—for a UE, the first emergency call attempt shall be launched through the same domain as the UE's non-emergency call service, and the second attempt shall be made through a different domain. For example, in one of the counterexamples, after the first emergency call attempt uses the PS domain from a 4G network and fails, the second attempt shall use the CS domain, which is only available in 3G networks.

The rule conflict may arise from the support of backward compatibility. Specifically, for attaching to a 4G network, the UE usually performs a combined EPS/IMSI attach procedure [2, 13], where the combination indicates that the network shall attach the UE to both a 3G network and a 4G network. This approach ensures that the UE does not need to undergo separate attach procedures with different networks, reducing attachment overhead. During the combined attach procedure, the 4G network initiates a CS attach procedure to attach the UE to the 3G network, allowing the UE to register with both 4G PS and 3G CS networks. Even though most 3G networks are phased out, for backward compatibility, the 4G network still provides a positive answer to the combined attach request; otherwise, UEs with old modem implementations may encounter issues. However, there may not be any 3G RANs available to the attached UE.



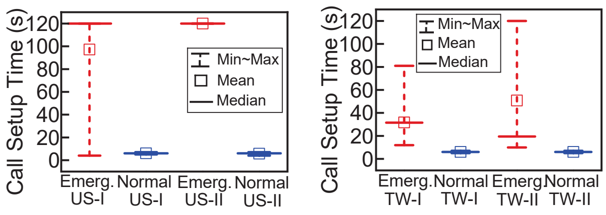
(a) U.S. exp. locations. (b) Taiwan exp. locations.

(c) RSRP/RSSI at location P7 (U.S.). (d) RSRP/RSSI at location P4 (TW).

Figure 6: Experiments were conducted for restrictions within PLMN in the U.S. and Taiwan.

Experimental Validation. We conducted experiments to validate the two problematic cases mentioned earlier. We selected 10 locations each from our U.S. and Taiwan campuses, as illustrated in Figures 6(a) and 6(b), respectively. At each location, we made 10 non-emergency calls and 10 emergency calls for each carrier while measuring the call setup times. All phone models used were carrier-certified, except for the Motorola G Stylus 5G. All tested phones supported VoWiFi (Voice over Wi-Fi) and were configured to connect to both cellular networks and campus Wi-Fi, with the "VoWiFi preferred" setting enabled for making calls.

Those two cases were indeed observed in practice. First, at locations with poor cellular signals (not stronger than -120 dBm from the 4G RAN) but with moderate to good Wi-Fi signals (not weaker than -55 dBm from the Wi-Fi RAN), as indicated by the red zones in Figures 6(a) and 6(b), the emergency call setup times for UEs were significantly longer than those for non-emergency calls. For example, at location P7 in Figure 6(a), all non-emergency calls were made via VoWiFi, with setup times ranging from 4 to 7 seconds and an average of 5.85 seconds, as illustrated in Figure 7. However, for emergency services, the setup times for 18 calls reached the maximum duration of 120 seconds, which was the maximum waiting time set by our experiment. This indicates that 90% of emergency calls could not connect to PSAPs within 2 minutes, due to the "3GPP-Always-Preferred" design. Note



(a) Under US-I/US-II

(b) Under TW-I/TW-II

Figure 7: 3GPP-Always-Preferred design results in minutes of emergency call setup delay in US-I, US-II, TW-I, and TW-II.

that only the results for US-I and US-II are considered at this location, as good cellular signals were observed from US-III.

Similar results were observed with Taiwan carrier networks. At location P4, the average emergency call setup times for TW-I and TW-II RANs were 31.7 and 50.8 seconds, respectively, while non-emergency calls for both carriers averaged only 6 seconds, as shown in Figure 7(b). Notably, the situations observed at the above two locations are not rare in practice. The reason is that cellular RAN signals are often weak in indoor environments, where Wi-Fi RANs can provide stronger signal strength.

Second, UEs attempted to initiate emergency calls through nonexistent 3G networks at certain locations. This abnormal case, if available, can be observed only with carriers US-I and US-III, as US-II did not support the combined EPS/IMSI attach procedure. In the validation experiment, we observed this issue occurring in US-I. During the initial attachment, the UE received an acceptance message from the 4G network, which also indicated attachment to a 3G network. After the UE's first emergency call attempt failed on the 4G network using the PS domain, it triggered an inter-system switch from the 4G to the 3G network, attempting a CS-based emergency call. However, no response was received because US-I shut down its 3G networks in 2022.

Attempting an emergency call through a nonexistent 3G network can lead to unexpected failures. According to the 3GPP standard [13], if the UE does not receive a response to the inter-system switch request after the timer expires (set to 10 seconds), it will begin searching for a 2G or 3G network to initiate the emergency call. However, not all phone models can handle this failure properly. It was observed that the Samsung Galaxy S21 became stuck during this process and could not recover until the outgoing emergency call was manually terminated.

Root Cause and Lessons Learned. The design principle of 3GPP-always-preferred for emergency services is not made without rationale. According to the 3GPP standard [1, 8, 10], 3GPP RANs and networks not only guarantee transmission bitrates for the delivery of emergency services but also prioritize them over non-emergency ones. This ensures emergency service quality, especially in case of network congestion. However, this design principle may unexpectedly cause negative real-world impacts, as demonstrated in our validation experiments. Thus, it calls for a coherent, flexible network selection mechanism oriented towards service quality to support emergency services.

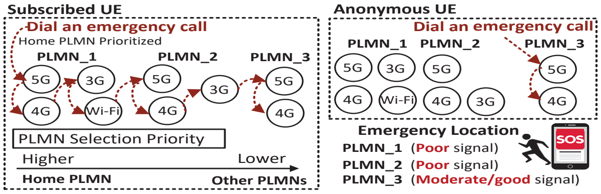


Figure 8: Subscribed UE prioritizes its home PLMN for dialing an emergency call, whereas anonymous UE does not.

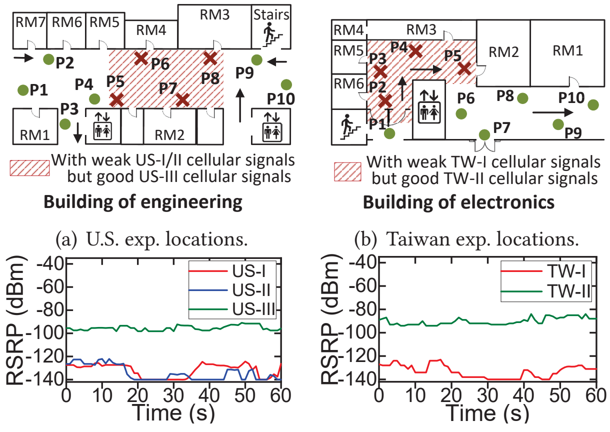
6.2 Fewer Options than Anonymous UEs - Limitation across PLMNs

Anonymous UEs, mobile equipment without valid SIMs, are permitted to access emergency services through nearby 3GPP RANs from all available PLMNs. However, UEs with valid subscriptions must prioritize their home PLMN [5], while also being allowed to access emergency services from all available PLMNs. This may incur a large overhead for UEs, as illustrated in Figure 8. The subscribed UE prioritizes its home PLMN for RAN selection when dialing an emergency call, while the anonymous UE selects the PLMN with the RAN offering the strongest signal.

With the limitation placed on subscribed UEs, M911-Verifier identifies corresponding counterexamples that violate one property of emergency services: Limited_Session_Establishment. The most commonly observed counterexample is when, for an emergency UE, the maximum number of failures to establish an emergency session with PSAPs is reached before attempting other available visited PLMNs. This occurrence implies that subscribed UEs have fewer options for accessing emergency services compared to anonymous UEs in practice, potentially leading to increased emergency call setup times and a downgrade in service quality.

Experimental Validation. We conducted experiments to validate the limitation across PLMNs in practice. The experimental setting was similar to that in §6.1. To identify the limitation, we considered locations with unbalanced signals, in which the carriers/PLMNs available in an area have 3GPP RANs with significant signal differences. Figure 9 shows two example locations, P6 and P3, for the U.S. and Taiwan, respectively. Such locations were not rarely observed in practice due to carriers' diverse deployment of RANs. At each location, we made 10 emergency calls from both subscribed UEs and anonymous UEs while measuring their call setup times.

As shown in Figure 10, subscribed UEs experienced significantly longer emergency call setup times compared to anonymous UEs. Specifically, setup times were 61.3, 70.2,



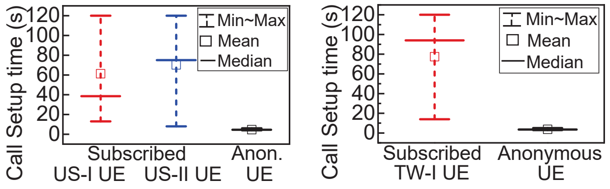
(a) U.S. exp. locations.

(b) Taiwan exp. locations.

(c) RSRP at location P6 (U.S.).

(d) RSRP at location P3 (TW).

Figure 9: Experiments were conducted for limitation across PLMNs in the U.S. and Taiwan.



(a) Users of US-I and US-II

(b) Users of TW-I

Figure 10: Subscribed UEs suffer longer emergency call setup times compared to anonymous UEs.

and 77.4 seconds for US-I, US-II, and TW-I, respectively. In contrast, anonymous UEs at the same locations had much shorter call setup times, averaging 4.6 seconds at location P6 in the U.S. and 3.7 seconds at location P3 in Taiwan. This discrepancy is due to the fact that subscribed UEs from US-I, US-II, and TW-I encountered many failures due to weaker signals, whereas anonymous UEs were able to access 3GPP RANs with much stronger signals from US-III and TW-II.

Root Cause and Lessons Learned. It is reasonable for subscribed UEs to prioritize their home PLMNs for accessing mobile services since connecting to visited PLMNs can incur roaming service fees. However, this reasoning does not apply to emergency services, as they are critical and provided free-of-charge according to the GSMA standard [34]. Therefore, subscribed UEs should not be restricted but should be allowed, like anonymous UEs, to select the best PLMN to guarantee the quality of emergency services.

7 EMERGENCY-UNAWARE 9-1-1 CALL OPERATION

All cellular operations need to be aware of signaling messages from emergency services so that they can be prioritized and handled differently from non-emergency services (e.g., call validation is skipped for emergency services [52]). When some operations are imprudently designed to be unaware of emergency services, the service initialization may face rejection from the infrastructure due to various potential reasons, such as congestion, roaming, and disallowed PLMN.

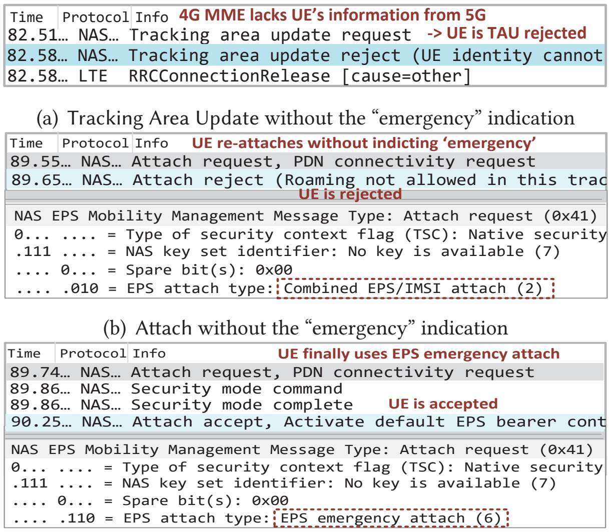
Some counterexamples of emergency services fallback were discovered by M911-Verifier corresponding to the problem of emergency unawareness. A commonly observed scenario among them is when the procedure of emergency service fallback [11] from 5G to 4G is invoked by a subscribed UE, but it fails, leading the UE to connect to the 4G network for its emergency request but potentially facing rejection for the UE's initial message. With the potential for failure and message rejection, this scenario could significantly delay the UE's access to emergency services, thereby violating the property of Availability_Guaranteed.

The failure of UE-initiated fallback for emergency services can occur due to the loss of the Handover Command message from the 5G MMF to the UE, typically caused by weak signals or the expiration of inter-system coordination [25]. If the UE does not receive the handover message, it proceeds with a mobility procedure without coordination between the 4G and 5G networks. The UE connects to an available 4G RAN and sends a Tracking Area Update (TAU) Request message to the 4G MMF. However, because this message lacks an indication of emergency service initialization, the request may be rejected, with the error cause: "*UE identity cannot be derived by the network*." Thus, the UE initiates a non-emergency attach procedure, as required by the 3GPP standard [13], which is not prioritized, to the 4G network for emergency services.

Experimental Validation. We experimentally validated the issue considering only the US-I network, as it was the only carrier that had a 5G SA (Standalone) network deployed on our campus. Additionally, it supported the emergency service fallback. The experiment was conducted at locations where 4G signals were stronger than 5G signals, with values greater than -110 dBm and below -120 dBm, respectively. At these locations, an emergency call was dialed from a tested phone while measuring call setup times and collecting control-plane signaling messages using Cellular Pro.

Figure 11 shows a sequence of three messages sent by the UE during an emergency service fallback from 5G to 4G without network coordination. The first, a TAU Request, was rejected due to the previously mentioned error cause. The UE then initiated a non-emergency Attach procedure, but this was rejected with the error cause "*Roaming not allowed in this tracking area*." Finally, the UE successfully initiated an Emergency Attach procedure to the 4G network. The total call setup time, from sending the TAU Request to the Emergency Attach Request, was 7.23 seconds.

We made two key observations. First, prior failed TAU requests and combined EPS/IMSI attachment, which lacked any indication of emergency, were rejected due to identity



```
Time   Protocol Info  4G MME lacks UE’s information from 5G
82.51… NAS…  Tracking area update request  -> UE is TAU rejected
82.58… NAS…  Tracking area update reject (UE identity cannot
82.58… LTE   RRCConnectionRelease [cause=other]
```

(a) Tracking Area Update without the “emergency” indication

```
Time   Protocol Info    UE re-attaches without indicting ‘emergency’
89.55… NAS…  Attach request, PDN connectivity request
89.65… NAS…  Attach reject (Roaming not allowed in this trac
                              UE is rejected
NAS EPS Mobility Management Message Type: Attach request (0x41)
0... .... = Type of security context flag (TSC): Native security
.111 .... = NAS key set identifier: No key is available (7)
.... 0... = Spare bit(s): 0x00
.... .010 = EPS attach type: Combined EPS/IMSI attach (2)
```

(b) Attach without the “emergency” indication

```
Time   Protocol Info                UE finally uses EPS emergency attach
89.74… NAS…  Attach request, PDN connectivity request
89.86… NAS…  Security mode command
89.86… NAS…  Security mode complete    UE is accepted
90.25… NAS…  Attach accept, Activate default EPS bearer cont
NAS EPS Mobility Management Message Type: Attach request (0x41)
0... .... = Type of security context flag (TSC): Native security
.111 .... = NAS key set identifier: No key is available (7)
.... 0... = Spare bit(s): 0x00
.... .110 = EPS attach type: EPS emergency attach (6)
```

(c) Re-Attach with the “emergency” indication

Figure 11: Emergency service fallback from 5G to 4G without network coordination includes three messages, where only the last Re-Attach message has the “emergency” indication.

validation errors and service restrictions, respectively. However, identity and subscription checks are not required for emergency services, as anonymous UEs are allowed. Second, while the average prolonged call setup time was only 7.23 seconds, it could extend to several minutes. For example, after a second rejection due to a roaming service restriction error, the UE could immediately initiate the emergency attach procedure. However, if the rejection is due to network congestion [13], the network may specify a timer, T3346, in the rejection message, which prevents the UE from restarting the attach procedure until the timer expires. This timer, ranging from 0 to 186 minutes (e.g., Cisco’s default is 25 minutes [30]), can significantly delay emergency call setup.

Root Cause and Lessons Learned. Ideally, for the failed TAU and non-emergency attachment requests, the 4G MMF can identify their emergency service intent by examining the headers of the underlying protocol, S1AP (S1 Application Protocol)[23]. Specifically, these requests are transmitted via the NAS (Non-Access-Stratum) protocol between the UE and 4G MMF, while the underlying protocols between the UE and 4G RAN, and between 4G RAN and 4G MMF, are RRC [22] and S1AP [23], respectively. The RRC and S1AP headers include a field indicating the RRC establishment cause, such as emergency or mobile-originated signaling. However, the NAS protocol [13] does not consider the RRC establishment cause in S1AP messages [13] for prioritizing emergency-related requests. Thus, there is a need for an explicit emergency indication in all emergency-related requests to make the corresponding procedures emergency-aware.

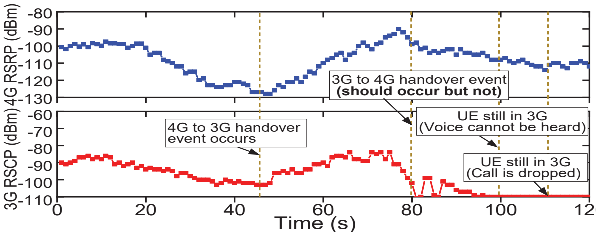


Figure 12: A call dropped due to forbidden 3G→4G handover.

8 NETWORK-ESCALATION FORBIDDEN DURING EMERGENCY CALLS

Emergency UEs may experience mobility while engaged in emergency calls. Like non-emergency UEs, the 3GPP standard [8, 11, 18] stipulates several voice call continuity mechanisms to maintain voice calls during handovers between networks or systems. However, two kinds of inter-system handovers are prohibited during an emergency call: (1) from 4G to 5G [11]; and (2) from 2G/3G with CS-based call service to 4G/5G with PS-based call service [18]. This restriction on network escalation can result in dropped emergency calls if such handovers are necessary.

Several counterexamples were observed where this prohibition on network escalation during an emergency call led to violations of the Continuity_Guaranteed property. In these cases, emergency calls were dropped when poor signals were detected from legacy systems (e.g., 3G), despite strong signals being available from newer systems (e.g., 4G/5G), causing a failure in the in-call network escalation handover.

Experimental Validation. We validated the forbidden network escalation using non-emergency calls due to ethical considerations. Specifically, we tested the handover from 3G CS to 4G PS, as this restriction also applies to non-emergency calls. These tests were conducted in Taiwan using the TW-I and TW-II networks, which still support 3G, as U.S. carriers discontinued 3G in 2022. The experiment involves a walking route containing three key locations, namely P0, P1, and P2, where P0 and P2 had a strong signal from a 4G network but a poor signal from a 3G network, and P1 had the opposite scenario. For each test, a non-emergency call was initiated by a tested UE from a 4G network at P0. Subsequently, the UE moved from P0 to P1 and P2 at a speed of 3 mph, while Cellular Pro was used to collect cellular network traces.

We plot the collected trace from TW-II alone to demonstrate the result, as shown in Figure 12. It depicts signal strengths over time in the 3G and 4G networks from a 2-minute walk on campus. Three important timings are noteworthy. First, when the 4G to 3G handover occurred at the 45th second (near location P1), the voice call remained uninterrupted. Second, at the 79th second, as the UE passed location P2, the expected 3G to 4G handover based on signal strengths did not occur. Third, despite a good signal of around -112 dBm from the 4G network, the voice call was dropped at the 112th second. This experiment confirms that network escalation from 3G CS to 4G PS during an ongoing voice call is forbidden, leading to unexpected call drops.

Root Cause and Lessons Learned. The prohibition on network escalation for emergency calls may stem from the common carrier practice of supporting multiple generations of cellular networks, where older network generations typically have broader coverage than their successors due to incremental deployment and cost consideration.

However, the real situation is more complex. Carriers' deployment policies, business considerations, and local regulations vary, leading to different deployment strategies across multiple network generations and situations where network escalation becomes necessary. For example, carriers like TW-I and TW-II, which concurrently support 3G, 4G, and 5G networks, may have reduced 3G coverage compared to 4G, due to replacing 3G RANs with 4G/5G ones, while still maintaining 3G RANs in urban areas. Therefore, a more flexible voice continuity mechanism, independent of network deployment assumptions, is needed for emergency UEs.

9 SOLUTION

We propose three approaches that require minimal infrastructure support while ensuring compliance with standards to address problematic network selection, emergency-unaware 9-1-1 call operation, and forbidden network escalation, respectively. We finally prototype and evaluate them.

Non-prioritized Network Selection. We propose disabling prioritized network selection for emergency services, enabling UEs to choose the best RAN from all available nearby 3GPP and non-3GPP networks.

Emergency-aware NAS Protocol. We indicate the status as "emergency" in all NAS messages for emergency UEs, making the NAS protocol emergency-aware and enabling the infrastructure to prioritize them. In case of network congestion, an appropriate error is returned, allowing emergency UEs to quickly access alternative RANs and PLMNs.

Unrestricted Handover for Call Continuity. We propose removing network escalation restrictions for emergency call continuity, enabling emergency UEs to use all available networks for improved voice continuity during mobility.

9.1 Prototype and Evaluation

We prototype and evaluate two solution methods that can mitigate unnecessary delays in the setup of emergency calls.

Non-prioritized Network Selection. We developed an application named Emerg-Call-Dialer [27] to select the best available RAN for emergency calls. It addresses two scenarios: (I) If the home PLMN signals are weak but visited PLMNs offer stronger signals, it disables the SIM/eSIM, switching the UE to anonymous mode to access nearby RANs; and (II) If all PLMN signals are weak but Wi-Fi is available, it initiates emergency calls via VoWiFi by translating the emergency number to a local dispatch center's number (e.g., 248-796-5500 for Oakland County, MI, U.S.).

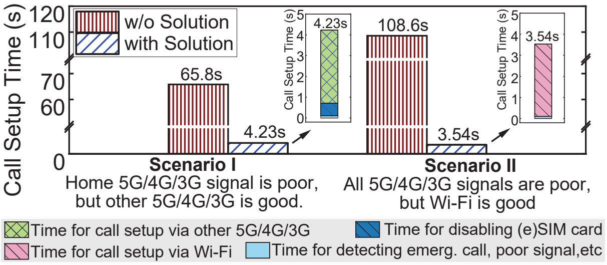


Figure 13: Call setup time vary with/w.o. solutions.

We conducted experiments with Emerg-Call-Dialer on the Google Pixel 5 and Samsung S21 at locations corresponding to the two network selection scenarios presented in §6. The emergency call setup time was measured with and without our solution, with 10 runs per device. The results are illustrated in Figure 13.

There are two key findings. First, the average emergency call setup times with our solution were significantly shorter than those without for both scenarios, 4.23 seconds versus 65.8 seconds (scenario I) and 3.54 seconds versus 108.6 seconds (scenario II). Second, the call setup times in scenario I with our solution were slightly longer than those in scenario II, with an average difference of only 0.61 seconds. The slight delay was due to the operation of disabling the eSIM/SIM to switch the UE to anonymous mode, allowing it to freely access non-home RANs. After the call is finished, it takes an average of 2.63 seconds to enable (e)SIM. Moreover, the resource usage required by this application was negligible. For example, on the Samsung 21, the application consumed only 1.95% CPU usage and 1.99% memory usage on average.

Emergency-aware NAS Protocol. This solution was implemented on an open-source 4G LTE SDR platform using srsRAN v23.11, comprising a 4G base station and a 4G core network. Since the phone modems cannot be modified, the prototype identified emergency-related NAS messages by referencing the RRC establishment cause header in S1AP messages. Two key changes were made to srsRAN. First, NAS messages from emergency UEs were marked as "emergency" in S1AP messages sent to the 4G MMF. Second, the MMF was modified to prioritize these NAS messages. Specifically, when the MMF receives a TAU Request for emergency services without network coordination, it rejects the request with a "Tracking area not allowed" error, placing the emergency UE in a limited service state, which enables immediate emergency attachment.

To assess the prototype's effectiveness, we measured how quickly a COTS phone (Google Pixel 5) re-initiates an emergency attachment after receiving either "Tracking area not allowed" or "UE identity cannot be derived by the network" errors (see §7). We conducted 10 tests for each error. Results show that after receiving the"Tracking area not allowed," the UE entered a limited service state and began an emergency attachment in about 0.17 seconds. Conversely, with another error, the UE continued a normal attachment without entering the limited state.

9.2 Potential Limitation

The proposed non-prioritized network selection might pose a potential security issue by allowing a UE to anonymously access non-home 3GPP RANs. Without a shared security context between the UE and roaming networks, emergency communications with PSAPs may lack encryption and integrity protection. To mitigate this issue, operators can enable TLS protection for IMS services, a security measure stipulated by 3GPP [3]. This approach allows anonymous UEs to establish a secure TLS session with the IMS infrastructure using only the server's certificate for IMS emergency services.

10 DISCUSSION

We discuss some potential challenges and limitations of applying this study's measurements to different operators, countries, or phone models. First, Emerg-Call-Blocker works only with Android phones and has not been tested on all models (see [27] for tested ones). A preliminary experiment (e.g., dialing non-emergency calls) is needed to verify functionality with your specific phone models and operators. Second, to avoid possible ethical issues, it is important to consult your IRB (Institutional Review Board) to obtain approval or a waiver, as policies may vary among institutions.

11 RELATED WORK

Ubiquitous Cellular Services Access. Some studies have examined cellular network accessibility and performance. For instance, Hassan et al. [36] analyzed 5G handover performance during a cross-country trip, while Xu et al. [59] studied TCP disconnections over LTE on high-speed rail systems. Pan et al. [53] investigated extreme mobility effects on throughput and signal quality on high-speed railways. In contrast, this study focuses on cellular emergency services, which operate differently from non-emergency services.

Cellular Emergency Services. Studies on cellular emergency services typically focus on security and fall into two categories: infrastructure-oriented and service-oriented.

Infrastructure-oriented studies [29, 40, 45, 46] explore attacks on public warning systems, while service-oriented works [35, 38, 39, 50] examine vulnerabilities in emergency voice and text services, including free data service attacks, DDoS attacks, emergency call blocking, and making calls through emergency panels. This study is service-oriented, aiming to identify design flaws that hinder emergency service access, rather than attacking emergency UEs.

Model Checking on Cellular Networks. Model checking has been widely used to scrutinize cellular protocol interactions [31, 38, 40–42, 44, 58]. However, limited studies used model checking for cellular emergency services. Klischies et al.[45] modeled 4G public warning systems and uncovered a message reassembly sequence with two undefined behaviors that can cause the phone modem to crash. Hou et al.[38] modeled the UE attach and call control procedures and identified four security vulnerabilities allowing attackers to bypass the phone's emergency checking panel to dial calls. Unlike prior studies, ours focuses on emergency service accessibility and continuity across heterogeneous cellular networks, including both stationary and mobile scenarios. This introduces greater challenges and reduces efficiency in modeling and checking. The modeled systems must encompass various aspects such as PLMN search, inter-system handovers, cell redirection, and emergency service fallback across multiple generations and RAN types. Interconnected protocols present unique challenges, prompting us to propose adaptive emergency scenario modeling and dynamic checker loading for efficient property checking.

12 CONCLUSION

Cellular networks provide mobile users with ubiquitous access to emergency services. However, not all emergency-specific designs have undergone rigorous examination. We developed M911-Verifier, a tool using model checking techniques with cellular-specific heuristics to formally investigate design defects from the 3GPP standard regarding ubiquitous access to emergency services. Our study showed that with the design issues discovered by M911-Verifier, emergency users may experience prolonged call setup times up to two minutes, unexpected service rejections, and call drops, even occurring in locations with good wireless signals. We experimentally validated these negative impacts with three major U.S. carriers and two Taiwan carriers. Such issues may commonly occur in practice, necessitating increased attention from emergency users, the standard community, carriers, and device vendors.

13 ACKNOWLEDGMENTS

We appreciate the insightful and constructive comments from our shepherd and the anonymous reviewers. This work is supported in part by the National Science Foundation (NSF) under Grants No. CNS-2226888, CNS-2246050, CNS-2246051, and CNS-2321416, and by the National Science and Technology Council (NSTC) under Grants No. 112-2628-E-A49-016-MY3, 113-2634-F-A49-001-MBK, 113-2218-E-A49-027, and 113-2218-E-A49-025. 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 NSTC.

REFERENCES

[1] 3GPP. 2021. TS 23.203: Policy and charging control architecture (Release 17). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=810.

[2] 3GPP. 2021. TS 23.272: Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2 (Release 17). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=835.

[3] 3GPP. 2021. TS 33.203: Access security for IP-based services (Release 17). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2277.

[4] 3GPP. 2021. TS 33.401: 3GPP System Architecture Evolution (SAE); Security architecture (Release 17). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296.

[5] 3GPP. 2022. TS 23.122: Universal Mobile Telecommunications System (UMTS); LTE; 5G; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=789.

[6] 3GPP. 2022. TS 23.228: IP Multimedia Subsystem (IMS); Stage 2 (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=821.

[7] 3GPP. 2022. TS 23.237: IP Multimedia Subsystem (IMS) Service Continuity; Stage 2 (Release 17). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=826.

[8] 3GPP. 2022. TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=849.

[9] 3GPP. 2022. TS 23.402: Architecture enhancements for non-3GPP accesses (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=850.

[10] 3GPP. 2022. TS 23.501: System architecture for the 5G System (5GS) (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144.

[11] 3GPP. 2022. TS 23.502: 5G; Procedures for the 5G System (5GS) (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145.

[12] 3GPP. 2022. TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1015.

[13] 3GPP. 2022. TS 24.301: Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1072.

[14] 3GPP. 2022. TS 24.501: Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3370.

[15] 3GPP. 2022. TS 25.304: User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode (Release 17). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1167.

[16] 3GPP. 2022. TS 25.331: Radio Resource Control (RRC); Protocol specification (Release 17). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1180.

[17] 3GPP. 2023. TS 23.167: IP Multimedia Subsystem (IMS) emergency sessions (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=799.

[18] 3GPP. 2023. TS 23.216: Single Radio Voice Call Continuity (SRVCC); Stage 2 (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=816.

[19] 3GPP. 2023. TS 24.229: IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1055.

[20] 3GPP. 2023. TS 33.501: Security architecture and procedures for 5G System (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169.

[21] 3GPP. 2024. TS 36.304: Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2432.

[22] 3GPP. 2024. TS 36.331: Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2440.

[23] 3GPP. 2024. TS 36.413: Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP) (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2446.

[24] 3GPP. 2024. TS 38.304: NR; User Equipment (UE) procedures in Idle mode and in RRC Inactive state (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3192.

[25] 3GPP. 2024. TS 38.331: NR; Radio Resource Control (RRC) protocol specification (Release 18). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3197.

[26] alibaba1126. 2022. Cellular Pro - a practical network optimization software. https://play.google.com/store/apps/details?id=make.more.r2d2.google.cellular_pro&hl=en_US&gl=US.

[27] Anonymous. 2024. Emergency Call Blocker/Dialer Tools. https://github.com/EmergencyAccess/Emergency-Blocker-Dialer-Tools.

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

[29] Evangelos Bitsikas and Christina Pöpper. 2022. You have been warned: Abusing 5G's Warning and Emergency Systems. In *Proceedings of the 38th Annual Computer Security Applications Conference* (, Austin, TX, USA,) *(ACSAC '22)*. Association for Computing Machinery, New York, NY, USA, 561–575. https://doi.org/10.1145/3564625.3568000

[30] CISCO. 2021. Cisco Mobility Management Entity Overview. https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-26/mme-admin/21-26-mme-admin/21-17-MME-Admin_chapter_01.html.

[31] Cas Cremers and Martin Dehnel-Wild. 2019. Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion. In *Network and Distributed System Security Symposium (NDSS)*. Internet Society.

[32] GSMA. 2020. Official Document IR.92 -IMS Profile for Voice and SMS (Version 15.0). https://www.gsma.com/newsroom/gsma_resources/ir-92-ims-profile-for-voice-and-sms-19-0/.

[33] GSMA. 2020. Official Document NG.111 -SMS Evolution (Version 2.0). https://www.gsma.com/newsroom/gsma_resources/ng-111-v-2-0/.

[34] GSMA. 2023. Official Document NG.119 -Emergency Communication (Version 1.0). https://gsma.com/newsroom/wp-content/uploads//NG.119-V2.1-2.pdf.

[35] Mordechai Guri, Yisroel Mirsky, and Yuval Elovici. 2017. 9-1-1 DDoS: Attacks, Analysis and Mitigation. In *2017 IEEE European Symposium*

on Security and Privacy (EuroS&P). 218–232. https://doi.org/10.1109/EuroSP.2017.23

[36] Ahmad Hassan, Arvind Narayanan, Anlan Zhang, Wei Ye, Ruiyang Zhu, Shuowei Jin, Jason Carpenter, Z. Morley Mao, Feng Qian, and Zhi-Li Zhang. 2022. Vivisecting mobility management in 5G cellular networks. In *Proceedings of the ACM SIGCOMM 2022 Conference* (Amsterdam, Netherlands) *(SIGCOMM '22)*. Association for Computing Machinery, New York, NY, USA, 86–100. https://doi.org/10.1145/3544216.3544217

[37] G.J. Holzmann. 1997. The model checker SPIN. *IEEE Transactions on Software Engineering* 23, 5 (1997), 279–295. https://doi.org/10.1109/32.588521

[38] Kaiyu Hou, You Li, Yinbo Yu, Yan Chen, and Hai Zhou. 2021. Discovering emergency call pitfalls for cellular networks with formal methods. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services* (Virtual Event, Wisconsin) *(MobiSys '21)*. Association for Computing Machinery, New York, NY, USA, 296–309. https://doi.org/10.1145/3458864.3466625

[39] Yiwen Hu, Min-Yue Chen, Guan-Hua Tu, Chi-Yu Li, Sihan Wang, Jingwen Shi, Tian Xie, Li Xiao, Chunyi Peng, Zhaowei Tan, and Songwu Lu. 2022. Uncovering insecure designs of cellular emergency services (911). In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking* (Sydney, NSW, Australia) *(MobiCom '22)*. Association for Computing Machinery, New York, NY, USA, 703–715. https://doi.org/10.1145/3495243.3560534

[40] S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. *Network and Distributed Systems Security (NDSS) Symposium 2018* (2018). https://par.nsf.gov/biblio/10055689

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

[42] Syed Rafiul Hussain, Imtiaz Karim, Abdullah Al Ishtiaq, Omar Chowdhury, and Elisa Bertino. 2021. Noncompliance as Deviant Behavior: An Automated Black-box Noncompliance Checker for 4G LTE Cellular Devices. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, Republic of Korea) *(CCS '21)*. Association for Computing Machinery, New York, NY, USA, 1082–1099. https://doi.org/10.1145/3460120.3485388

[43] IEEE. 2016. IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)* (2016), 1–3534. https://doi.org/10.1109/IEEESTD.2016.7786995

[44] Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim. 2019. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. In *2019 IEEE Symposium on Security and Privacy (SP)*. 1153–1168. https://doi.org/10.1109/SP.2019.00038

[45] Daniel Klischies, Moritz Schloegel, Tobias Scharnowski, Mikhail Bogodukhov, David Rupprecht, and Veelasha Moonsamy. 2023. Instructions unclear: undefined behaviour in cellular network specifications. In *32nd USENIX Security Symposium (USENIX Security 23)*. 3475–3492.

[46] Gyuhong Lee, Jihoon Lee, Jinsung Lee, Youngbin Im, Max Hollingsworth, Eric Wustrow, Dirk Grunwald, and Sangtae Ha. 2019. This is Your President Speaking: Spoofing Alerts in 4G LTE Networks. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services* (Seoul, Republic of Korea) *(MobiSys '19)*. Association for Computing Machinery, New York, NY, USA, 404–416. https://doi.org/10.1145/3307334.3326082

[47] Yuanjie Li, Haotian Deng, Jiayao Li, Chunyi Peng, and Songwu Lu. 2016. Instability in Distributed Mobility Management: Revisiting Configuration Management in 3G/4G Mobile Networks. *SIGMETRICS Perform. Eval. Rev.* 44, 1 (jun 2016), 261–272. https://doi.org/10.1145/2964791.2901457

[48] Yuanjie Li, Qianru Li, Zhehui Zhang, Ghufran Baig, Lili Qiu, and Songwu Lu. 2020. Beyond 5G: Reliable Extreme Mobility Management. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication* (Virtual Event, USA) *(SIGCOMM '20)*. Association for Computing Machinery, New York, NY, USA, 344–358. https://doi.org/10.1145/3387514.3405873

[49] Jamshed Memon, Maira Sami, Rizwan Ahmed Khan, and Mueen Uddin. 2020. Handwritten optical character recognition (OCR): A comprehensive systematic literature review (SLR). *IEEE access* 8 (2020), 142642–142668.

[50] Yisroel Mirsky and Mordechai Guri. 2021. DDoS Attacks on 9-1-1 Emergency Services. *IEEE Transactions on Dependable and Secure Computing* 18, 6 (2021), 2767–2786. https://doi.org/10.1109/TDSC.2019.2963856

[51] Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker, and Michael Deardeuff. 2015. How Amazon web services uses formal methods. *Commun. ACM* 58, 4 (2015), 66–73.

[52] Code of Federal Regulations. 2021. FCC 911 Regulations: 47 CFR Part 9: 911 Requirements. https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-9?toc=1.

[53] Yueyang Pan, Ruihan Li, and Chenren Xu. 2022. The First 5G-LTE Comparative Study in Extreme Mobility. *Proc. ACM Meas. Anal. Comput. Syst.* 6, 1, Article 20 (feb 2022), 22 pages. https://doi.org/10.1145/3508040

[54] Santhosh Prabhu, Kuan Yen Chou, Ali Kheradmand, Brighten Godfrey, and Matthew Caesar. 2020. Plankton: Scalable network configuration verification through model checking. In *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*. 953–967.

[55] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. 2002. SIP: Session Initiation Protocol. https://www.ietf.org/rfc/rfc3261.txt.

[56] Ahmed Roumane, Bouabdellah Kechar, and Belkacem Kouninef. 2017. Formal verification of a radio network random access protocol. *International Journal of Communication Systems* 30, 18 (2017), e3447.

[57] SPIN. 2024. SPIN-Option. https://spinroot.com/spin/Man/Manual.html.

[58] Guan-Hua Tu, Yuanjie Li, Chunyi Peng, Chi-Yu Li, Hongyi Wang, and Songwu Lu. 2014. Control-plane protocol interactions in cellular networks. In *Proceedings of the 2014 ACM Conference on SIGCOMM* (Chicago, Illinois, USA) *(SIGCOMM '14)*. Association for Computing Machinery, New York, NY, USA, 223–234. https://doi.org/10.1145/2619239.2626302

[59] Chenren Xu, Jing Wang, Zhiyao Ma, Yihua Cheng, Yunzhe Ni, Wangyang Li, Feng Qian, and Yuanjie Li. 2020. A First Look at Disconnection-Centric TCP Performance on High-Speed Railways. *IEEE Journal on Selected Areas in Communications* 38, 12 (2020), 2723–2733. https://doi.org/10.1109/JSAC.2020.3005486

[60] Zhehui Zhang, Yuanjie Li, Qianru Li, Jinghao Zhao, Ghufran Baig, Lili Qiu, and Songwu Lu. 2023. Movement-Based Reliable Mobility Management for Beyond 5G Cellular Networks. *IEEE/ACM Transactions on Networking* 31, 1 (2023), 192–207. https://doi.org/10.1109/TNET.2022.3190788