POWERING THE INFRASTRUCTURE FOR CRITICAL SERVICES: ENSURING SECURE AND RELIABLE EMERGENCY COMMUNICATIONS OVER CELLULAR NETWORKS

By

Yiwen Hu

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Computer Science—Doctor of Philosophy

2025

ABSTRACT

Cellular networks (4G, 5G, and beyond), the only large-scale wireless network infrastructure on par with the Internet, play an indispensable role in supporting not only daily voice, text, and data services but also critical services such as emergency services. Emergency communication over cellular networks is a vital part of our nation's emergency response and disaster preparedness system. To maximize emergency service availability, there are some special requirements from standard organizations and administrative authorities. For example, in the U.S., the Federal Communications Commission (FCC) stipulates that cellular carriers must transmit all wireless 911 calls without call validation to Public Safety Answering Points (PSAPs). The 3GPP standard provides emergency services with higher priority than non-emergency services and enables them across all available radio access technologies, generations, and operators. Therefore, ideally, by design, users are supposed to access emergency services anytime and anywhere, as long as wireless coverage is available.

However, it is very challenging to support such emergency communications. An operational cellular infrastructure usually comprises multiple generations of cellular networks, such as 5G Standalone, 5G Non-Standalone, 4G, and 3G, using different radio access technologies, including 5G NR (New Radio), 4G E-UTRA (Evolved Universal Terrestrial Radio Access), or even public/private Wi-Fi networks. However, the security mechanisms and supported services of different generations are not equally reliable. Moreover, to maximize emergency service support, networks must permit some insecure operations, such as allowing anonymous emergency access for roaming users or users without mobile subscriptions. These special operations, while essential, similar to backdoors, introducing potential attack surfaces. Even more threatening, emergency and non-emergency services share the same underlying infrastructure. Therefore, any design flaw in emergency services can compromise the security and reliability of the entire mobile ecosystem. Despite their importance, emergency services remain underexplored, as prior work mainly targets user equipment or simulated DoS attacks, lacking systematic study of such critical infrastructure.

This dissertation presents our research on powering the infrastructure for critical services to

ensure secure and reliable emergency communications over cellular networks. We highlight our research insights and findings on: (1) identifying design defects in cellular emergency service standards, and (2) investigating the security and reliability of operational emergency services in the U.S. and other countries/areas, along with the technical challenges we encountered and our approaches to addressing them. Our results show that, from a security perspective, operational cellular emergency services are not only abusable but also deniable. For example, an adversary can block a victim's emergency calls by sending just a single message to the carrier network. Adversaries without purchasing any mobile subscription can obtain free data, voice, and text services through the high-priority emergency communication channel. Even more threatening, our study also reveals that, in some situations, with sufficient wireless coverage, emergency calls cannot be made within 2 minutes, whereas non-emergency calls at the same locations can be made within 3-6 seconds. Finally, we conclude our existing research on studying critical emergency services, discuss new challenges and opportunities for safeguarding next-generation emergency services, and outline future research directions.

The significance of this dissertation is threefold: (1) It presents a systematic methodology that integrates model checking and empirical experiments to uncover design flaws in cellular networking standards; (2) It explores and addresses real-world critical emergency service problems, with the discovered defects experimentally validated across three U.S. and two Taiwan carriers; and (3) We have reported the discovered issues and flaws to operators and standards organizations with the proposed solutions. Our research work has been recognized in several ways from both academia and industry, such as MobiCom Best Community Paper Award Runner Up (2022), ACM GetMobile research highlights (2023), SIGMOBILE research highlights (2024), and AT&T Security Award. The lessons learned offer valuable insights for improving systems and services for billions of mobile users.

To my parents, whose unwavering love and support have been my foundation, and to my husband Yang, who stands by me in hard times and shares in my happiness.

ACKNOWLEDGMENTS

I would like to begin by expressing my sincere gratitude to my advisor, Dr. Li Xiao, for giving me a research opportunity during my undergraduate years at Zhejiang University and offering me the chance to begin my PhD journey in her lab. She has been patient with me in academics, guiding the direction of my work, listening to my ideas, and encouraging me to explore the research areas I am truly passionate about. As an active female professor in computer science and engineering, she has not only excelled in her research and teaching but also served as an inspiring role model for young researchers like me. I express my deep respect and appreciation to her.

I would like to especially extend my heartfelt thanks to my advisor, Dr. Guan-Hua Tu. I will always remember that whenever I doubted myself or felt discouraged by research setbacks, he remained professional and served as a guiding light, teaching me to stay grounded, persevere, and continue exploring new ideas. His guidance ultimately led to my significant work in cellular emergency services. Time has flown by, and it is his seven years of dedicated support and guidance that have shaped who I am today. Whenever I look back at the standards I've studied, the papers I've published, and the slides I've presented, I can still feel the imprint of his patient mentorship behind it all.

I am sincerely thankful to Dr. Matt W. Mutka, Dr. Qiben Yan, and Dr. Yuying Xie for serving on my PhD guidance committee. Dr. Mutka's expertise in wireless communication systems, Dr. Yan's guidance on system security, and Dr. Xie's proficiency in data analysis have all been pivotal in shaping my work. Their thoughtful advice and constructive feedback have not only advanced my research but also helped me grow as an academic. I am truly grateful for their time, support, and mentorship throughout this journey.

I would like to thank my past and present colleagues in the SNMS Lab and eLans Lab: Dr. Xinyu Lei, Dr. Tian Xie, Sihan Wang, Min-Yue Chen, Jingwen Shi, Dr. Chin-Jung Liu, James Mariani, Kanishka Wijewardena, Griffin Klevering, Dr. Xiao Zhang, and Dr. Hanqing Guo. We collaborated on research problems, set up experiments, and also celebrated sports events together.

I would like to express my appreciation to my research collaborators at MSU and from external

institutions: Dr. Songwu Lu (UCLA), Dr. Jiliang Tang (MSU), Dr. Chunyi Peng (Purdue), Dr. Chi-Yu Li (National Yang Ming Chiao Tung University), Dr. Zhaowei Tan (UC Riverside), and researchers at AT&T, 3GPP, and GSMA. It has been an honor working with them, and together we have made many impactful contributions.

I am also grateful to many faculty and staff members at Michigan State University for their support in teaching, research, and student services throughout my PhD program: Dr. Abdol-Hossein Esfahanian, Dr. Sandeep Kulkarni, Dr. Philip McKinley, Dr. Charles B. Owen, Dr. Xiaoming Liu, Dr. Hui Liu, Brenda Hodge, and Vincent Mattison.

Most importantly, I am deeply grateful to my parents for their unwavering support and love. I want to thank my husband, who always stays with me and supports me and thank my grandparents, whom I haven't seen in six years and truly miss. I would like to thank my dear dog, Xiao Hua, a warm French Bulldog who has been by my side for five years. Though she cannot speak, I know she understands me.

Lastly, I would like to thank myself for staying positive, being brave, and demonstrating intelligence and determination throughout this journey.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

Cellular networks such as 4G and 5G are the only large-scale wireless network infrastructure on par with the Internet. According to data from global mobile organizations such as GSMA [55] and Ericsson [48], cellular networks have been deployed in 226 countries and territories worldwide. In 5G, downlink and uplink throughput can reach up to 20 gigabits per second with latency as low as 10 milliseconds. With such ubiquitous coverage, ultra-fast speed, and extremely low latency, cellular networks serve as a powerful infrastructure that is vital to modern life. They support essential services such as voice, text, data, and life-saving emergency communications. In addition, they power a wide range of mobile applications in financial management and social engagement, and drive innovations in mobile health, industrial Internet of Things, and autonomous vehicular systems.

1.1: Research Motivation

Among the diverse services supported by cellular networks, emergency services are the most vital, closely tied to our nation's emergency response and disaster preparedness system. The globally-deployed cellular networks with ubiquitous coverage have been the most accessible channel to emergency users. To maximize the emergency services availability, there are some specialized requirements from regulation authorities and standard organizations. In the U.S., the Federal Communications Commission (FCC) stipulates that cellular carriers must transmit all wireless 911 calls without call validation to Public Safety Answering Points (PSAPs) [84]. The GSM Association (GSMA) standard requires emergency services must be supported by all mobile phones even without SIM cards and be free of charge [54]. The 3GPP standard provides emergency services with higher priority than non-emergency services and enables them across all available radio access technologies, generations, and operators [28]. Therefore, ideally, users are supposed to access emergency service anytime and anywhere, as long as there is wireless coverage, as illustrated in Figure 1.1.

Supporting such emergency communications is highly challenging from both design and prac-

tical perspectives. This is because an operational cellular infrastructure always consists of multiple generations of networks. It is impossible for a nationwide operator to shut down 4G overnight and fully deploy 5G within a day. For example, nowadays, some locations still rely on 4G, others can access 5G, some remote areas like national parks may only have 3G, and indoor scenarios often depend on Wi-Fi. These 3G, 4G, and 5G generations are interconnected through various network interfaces. While the security mechanisms and services across different generations are not equally reliable. Legacy systems often contain security vulnerabilities that newer systems aim to address. Yet, as newer generations support more features, they also introduce new attack surfaces, making the system increasingly complex to secure.

However, within such a complex infrastructure, to fulfill the special requirement of emergency services, network infrastructure has to permit certain insecure operations. For example, anonymous access must be allowed in situations where users cannot connect to their home carriers—such as in national parks, where some carrier signals are strong while others are weak. In these cases, user authentication is bypassed. Additionally, emergency calls must be free of charge for all users. These special operations function like security backdoors within the system, creating potential attack surfaces. More concerning is that both emergency and non-emergency services share the same underlying infrastructure, where all mobile generations are interconnected. It is extremely challenging to allow certain insecure operations to maximize emergency service accessibility while ensuring these operations do not negatively impact other services. Any design defects in emergency services could threaten the security and reliability of the entire mobile ecosystem, and we are thus motivated to study them.

Despite the vital role of emergency services, prior research has largely focused on the security and functionality of services for normal mobile users and applications [47,66,72,73,75,76,88,102], leaving emergency services relatively underexplored. This research gap stems partly from the inherent complexity of supporting emergency services within cellular architectures, and partly from the practical and ethical concerns of conducting real-world experiments on operational networks, where testing may disrupt actual emergency operations. As a result, most existing work in this

area has focused either on the user equipment (UE) perspective [60,64], or on simulating denial-of-service scenarios targeting 911 call centers through message flooding [40,81,82,100], with corresponding mitigation strategies proposed [49,71,85,98,99]. In contrast, our work not only explores the security and reliability of emergency services from the UE side, but also from the network infrastructure perspective. We develop a systematic framework to evaluate the design of emergency service standards and uncover several new counterintuitive findings, which are further validated in a responsible manner using our developed applications over operational carrier networks.

Figure 1.1: The globally-deployed cellular networks with ubiquitous coverage have been the most accessible channel to emergency users.

1.2: Research Contribution

In this section, we introduce our research contribution to enhancing the security and reliability of cellular emergency services over mobile networked systems. I categorize my four research papers [44, 61–63] presented in this dissertation into two main areas with a discussion of their impact and recognition.

1.2.1: Enhancing the Security of Emergency Services (9-1-1)

Given the critical nature of emergency services, ensuring their availability is definitely the most important. Standard organizations (e.g., GSMA. 3GPP) and regulatory authorities (e.g., FCC) mandate emergency services support for both subscribed and non-subscribed users, offering free, high-priority access without call validation. Although these provisions maximize emergency service availability, they can also introduce new attack surfaces, increasing the risk of system security compromise. Moreover, in most scenarios, emergency services share the same network architec-

ture as commodity non-emergency services, attacks in critical infrastructure might affect not only emergency users and network elements but also propagate to other commodity services or users, causing severe negative impacts across the mobile ecosystem.

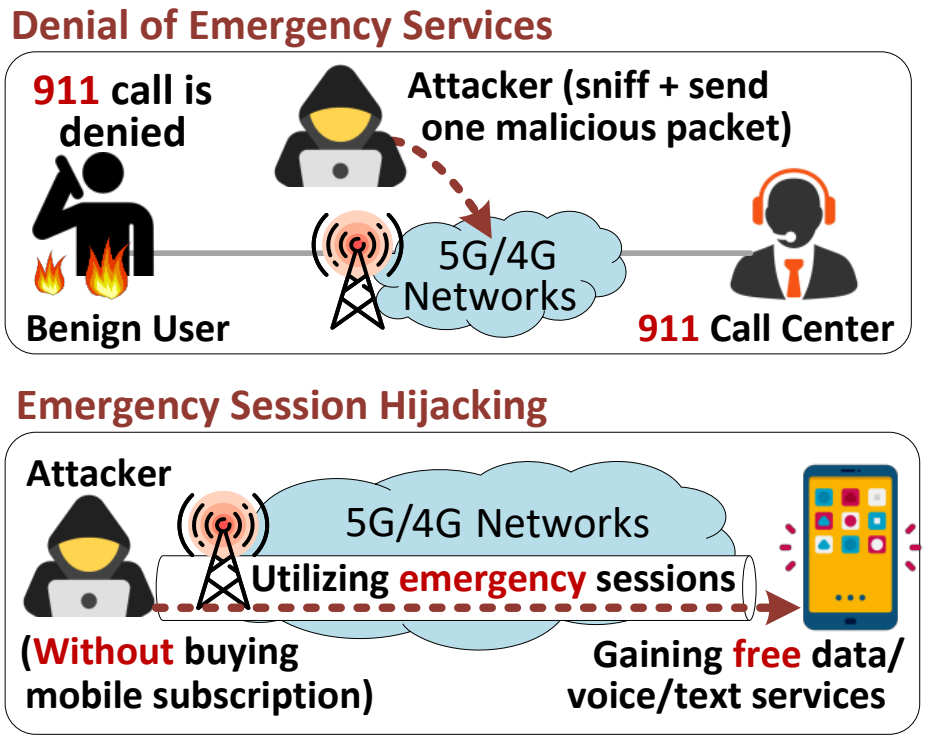


Figure 1.2: Proposed DoS and Hijacking Attacks towards 9-1-1 Services.

We identified six security vulnerabilities in emergency services across the three top-tier U.S. 5G/4G mobile networks: (V1) unverifiable emergency IP-CAN (IP Connectivity Access Network) session requests, (V2) Inconsistent Emergency IP-CAN Session Support, (V3) improper cross-layer security binding, (V4) non-atomic cellular emergency service initialization, (V5) improper access control on emergency IP-CAN sessions, and (V6) One-size-fits-all Prioritization for Emergency IP-CAN Sessions. We developed two proof-of-concept attacks based on them, as shown in Figure 1.2. The first attack, denial of cellular emergency service (DoCES), allows the adversary to prevent mobile users from accessing emergency services, using only two SDR (Software-defined Radio) platforms serving as an attack UE and a sniffer. This attack includes four variants, namely UE blocking, UE detaching, call cancel, and call drop, targeting different emergency call phases of users. The second attack exploits vulnerabilities to hijack emergency sessions. The attackers

can not only obtain free data/voice/text access from critical emergency network resources but also launch data overcharging and remote service scanning attacks towards non-emergency services mobile users, as shown in Figure 1.2. Moreover, in addition to the top three U.S. carriers, we also validated our findings on two major Taiwanese carriers, demonstrating the wide-reaching impact of our emergency findings.

The significance of this research is two-fold: (1) It improved the security of U.S. emergency services. We not only reported our findings to carriers but also proposed standard-compliant solutions, which were evaluated through a prototype. This work earned multiple awards, including the Best Community Paper Award Runner-Up at ACM MobiCom (2022), GetMobile Research Highlights (2023), the AT&T Security Award (2023), and SigMobile Research Highlights (2024). (2). Our research was also featured by media outlets such as MSU Today, Wood TV, and Wilx TV, to have a broad impact on national public safety. We believe that our projects are projected to extend the research to safeguard emergency services for not only ordinary users but also people with disabilities, and across more applications, such as vehicles and IoTs in the near future.

1.2.2: Improving the Reliability of Emergency Services (9-1-1)

Emergency services are vital lifelines for people in emergency conditions. Both regulation authorities and standard organizations have stipulated requirements to enhance the accessibility and resilience of emergency services. For example, 3GPP allows mobile users to access emergency services across heterogeneous mobile networks, including all available radio access networks (RANs) such as 5G/4G/Wi-Fi base stations, as well as different mobile generations (e.g., 5G/4G/3G) and public land mobile networks (PLMNs) like AT&T and Verizon. However, this comprehensive support significantly complicates the standard design of network functions and protocol interactions, rendering emergency services more prone to errors. Moreover, given its critical nature, the emergency service infrastructure usually cannot be fully accessed and tested by researchers, leaving emergency services largely unexplored.

We developed M911-Verifier, an emergency-specific framework that integrates model checking to conduct an automated diagnosis of complex emergency service protocols, as illustrated in

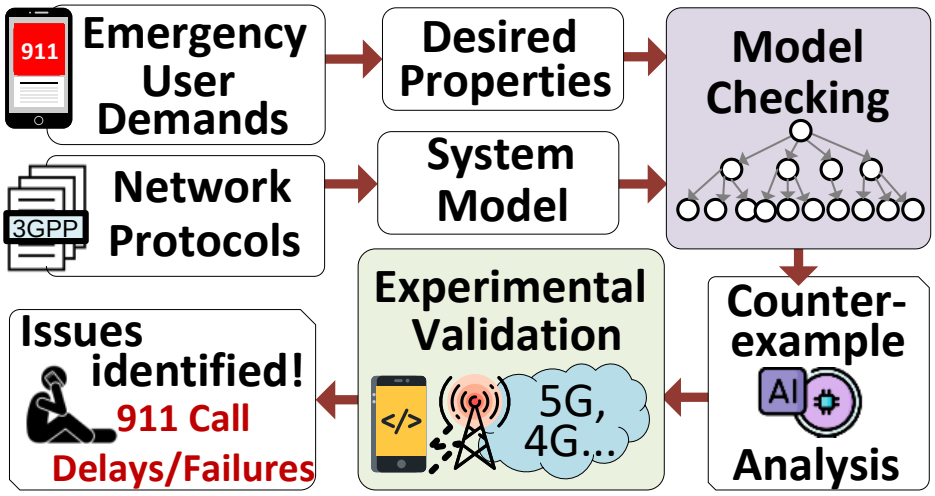


Figure 1.3: Uncovering Designs Flaws Hindering 9-1-1 Services Access.

Figure 1.3. Model checking is a formal method that explores all modeled system states to discover counterexamples that violate desired properties. However, it can face severe state exploration problems when applied to large, complex systems like emergency services, which require system-wide support and span multiple mobile generations. To address these problems, we proposed M911-Verifier that models emergency services as procedure-oriented ones and dynamically loads the modeled procedures for model checking. This dynamic framework allows M911-Verifier to systematically and effectively discover potential issues on emergency services. We utilized the developed M911-Verifier to uncover eleven counterintuitive findings. Our study shows that despite sufficient wireless coverage, users may still experience prolonged emergency call setup times (e.g., two minutes), emergency call initiation failures, or call drops due to improper designs in the 3GPP standards. For instance, while 3GPP allows emergency calls over both cellular and Wi-Fi networks, its problematic network selection mechanism results in 90% of indoor emergency calls cannot being dialed out within two minutes, whereas non-emergency calls at the same locations succeed in around five seconds. In some cases, the phones even attempt to initiate emergency calls via 3G networks, even when no 3G RANs are available nearby, instead of using available strong Wi-Fi signals. Moreover, we discovered that emergency service initiation requests can be rejected by the network due to emergency-unaware protocol designs. Emergency call communication may still drop even 5G/4G network signal coverage is sufficient due to network escalation restrictions.

The impacts of the discovered defects have been experimentally validated across three top-tier U.S. carriers and two major Taiwan carriers. To prevent disruptions to emergency service operations, we developed Emerg-Call-Blocker tools on smartphones that ensure no emergency calls reach PSAPs during our experiments.

The significance of this work is twofold: (1) The developed M911-Verifier framework and Emerg-Call-Blocker tools introduce a new systematic methodology that combines model checking and empirical experiments to discover and verify issues in critical emergency services within operational networks, without disruption of emergency operations; (2) We have reported the identified design flaws that cause emergency service delay or failure to operators and standards organizations, proposing solutions, and are collaborating with them to enhance the emergency services.

1.2.3: Research Impact

Our research has made two key impacts: (1) I pioneered new research methodologies for studying critical mobile network services. For problem discovery, I developed an emergency-specific model-checking framework to systematically identify design flaws across standards; For problem verification, I developed tools for conducting experiments within operational carrier networks without disrupting emergency services, evolving from simulation analysis used in prior research to ethically responsible real-world verification. The tools are open-sourced to encourage broader research involvement and lasting impact in this critical area. (2) I have contributed to addressing real-world security problems for critical emergency services and corresponding network infrastructures (e.g., denial of emergency services, hijacking emergency sessions for free data services). The identified vulnerabilities, along with proposed solutions, have been reported to operators (e.g., AT&T, Verizon, T-Mobile), mobile vendors (e.g., Samsung, Google, Motorola), and global standards organizations(e.g., 3GPP, GSMA), protecting network infrastructure and mobile users.

1.2.4: Research Recognition

My research work on cellular emergency services has been recognized in several ways from both academic and industry: (1) Several research papers have been published in the most prestigious

conferences and journals in the fields of networking, mobile systems, and security, including ACM MobiCom [62, 63], IEEE/ACM ToN [44], and ACM GetMobile [61], with the collaboration of my advisors and colleagues. (2) The emergency service (9-1-1) security paper received MobiCom Best Community Paper Award-Runner Up (2022), and was selected as research highlights by both SIGMOBILE and GetMobile communities. This work also obtained industrial awards, including AT&T Security Award and GSMA Thank-you Letters for our security vulnerability disclosure, which contributed to the updates of GSMA standards. (3). My research work has been disseminated to the public through several prestigious public media outlets, including Wilx TV, Wood TV, WILS Morning Wake-Up, ISSSource, EurekAlert, and Homeland Security News.

1.3: Dissertation Organization

This dissertation is organized as follows. Chapter 1 outlines the research motivation, contributions, and overall structure. Chapter 2 introduces background and related work. Chapter 3 presents our work on enhancing the security of emergency services (9-1-1), where we identify six critical vulnerabilities and introduce two new attack sets: Denial of Cellular Emergency Services (DoCES) and Emergency IP-CAN Session Hijacking. Chapter 4 focuses on improving the reliability of emergency services. We reveal that despite adequate wireless signal coverage, users may still face prolonged emergency call setup times, call failures, and dropped calls. Chapter 5 concludes the dissertation and outlines my future research plans on innovating and securing next-generation emergency services, cellular-V2X communications, and mobile health applications.

CHAPTER 2: BACKGROUND AND RELATED WORK

This chapter provides a concise overview of the background of cellular emergency services and presents the state of the art in emergency service research.

2.1: Research Background

To support diverse mobile services and applications with ubiquitous coverage, cellular networks have evolved into complex, interconnected infrastructures. These systems typically comprise the radio access network (RAN), such as 4G LTE (E-UTRAN) [15], 5G New Radio (NR) [17], and Wi-Fi [22], alongside a core network responsible for user authentication, mobility, and session management. The core network further connects to the IP Multimedia Subsystem (IMS) [5], which supports voice, text, as well as emergency services or connects to the broader Internet to enable various mobile applications. Operational mobile networks often integrate multiple generations (e.g., 4G and 5G) and support user mobility across generations and carriers (e.g., transitioning from 4G to 5G or from a home carrier like AT&T to a roaming carrier like Verizon) [41]. Due to these interconnected standards and numerous network components, mobile networked systems are inherently complex.

Figure 2.1 depicts a 5G/4G network architecture with the service flow for emergency voice/text services. An emergency service request from the UE traverses radio access network (RAN), core network, IP Multimedia Subsystem (IMS), and the 911 PSAP. Specifically, the RAN uses the base station (BS) to offer radio access. In the core network, the user-plane gateway (UPG) routes user traffic packets from the UE to the IMS network. Mobility Management Function (MMF) manages user mobility, authentication, and resource reservation. User Data Function (UDF) stores user and service subscription information. Policy Control Function (PCF) generates billing policies, QoS parameters, routing control rules, etc. In the IMS, Call Session Control Function (CSCF, referred to as IMS server hereafter) is responsible for IMS service signaling, which runs Session Initiation

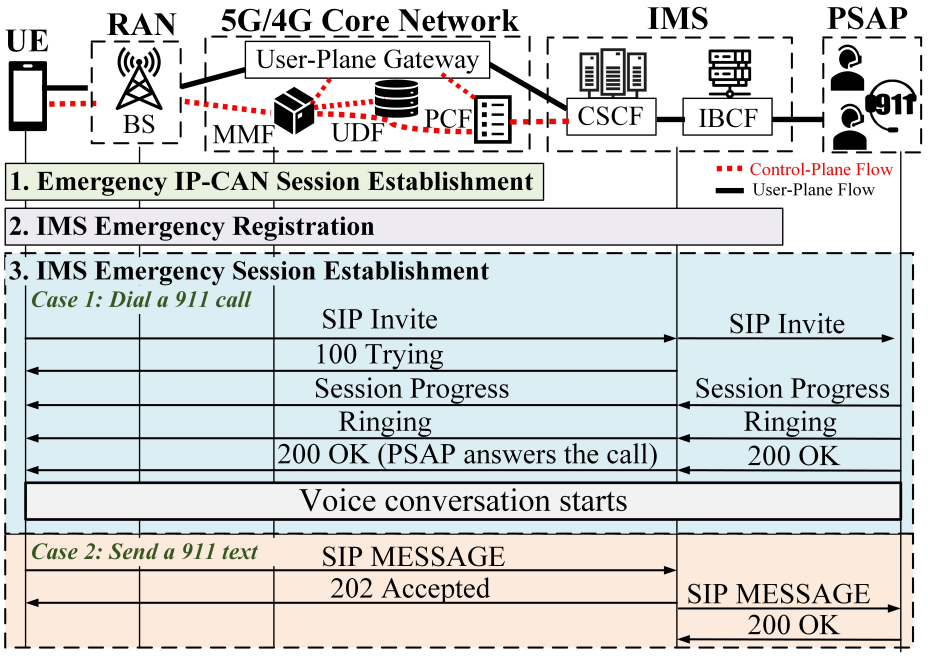


Figure 2.1: 5G/4G network architecture and the service flow for emergency voice/text services.

Protocol (SIP). Interconnect Border Control Function (IBCF) is a session border controller which is interconnected to other IP/IMS networks. To establish an emergency session with the PSAP, the emergency UE needs to perform three actions: (1) Emergency IP-CAN Session Establishment allows the UE to obtain the emergency IP connectivity to communicate with the IMS server; (2) IMS Emergency Registration has the IMS server and the UE authenticate with each other and enables the UE to register the emergency service; and (3) IMS Emergency Session Establishment allows the UE to establish an IMS emergency call/text session with the PSAP.

2.2: Related Work on Emergency Services Security

Research on mobile networked systems has become a highly active and rapidly evolving area, attracting significant attention in recent years. While prior research has largely focused on the security of services for normal mobile services and users [47, 66, 72, 73, 75, 76, 88, 102]. However, the security of emergency services remain underexplored despite their critical importance. In the following, we classify the related work of the emergency service security into non-cellular and cellular categories.

Non-cellular Emergency Service Security. Several studies have been proposed to examine the

security of non-cellular emergency services. Specifically, Goebel *et al.* [50] presented the vulnerabilities of the 9-1-1 call system from the perspectives of confidentiality, integrity, and availability. Fuchs *et al.* [49] developed an adapted intrusion detection architecture against the DoS attacks where a large number of faked VoIP-based emergency calls are generated. Seth *et al.* [95] designed a Wi-Fi based emergency service framework that enables mobile devices to contact the PSAP securely.

Cellular Emergency Services Security. The security issues of the cellular emergency service have attracted much attention in recent years. They can be classified into three categories. The first category of the studies is to launch or defend against the DDoS attack on the PSAP or the IMS emergency service server. Specifically, Mirsky *et al.* [82] showed that the adversary can jeopardize the statewide and nationwide PSAPs by generating random UE identities (e.g., IMEIs). Jung *et al.* [71] presented a CAPTCHA-based DDoS defense system that can protect the PSAP from DDoS attacks generated by compromised UEs (bots). Onofrei *et al.* [85] developed an adaptive firewall pinholing mechanism that can mitigate DDoS attacks against the server of the IMS emergency service. The second category is to examine the security issue that fabricated emergency/presidential alerts can be sent to UEs. Lee *et al.* [74] demonstrated that fabricated emergency alerts can be sent to UEs successfully. Hussain *et al.* [64] discovered that the adversary can hijack legitimate paging channels to send fabricated paging messages with emergency alerts to victim UEs successfully.

The last category is to exploit the cellular emergency service or resources to attack UEs or carriers. Hou *et al.* [60] developed two attacks based on the emergency service: UE screen lock bypassing and call service DoS. The first attack allows the adversary to dial any number on the emergency panel of the victim's UE and the call can be routed to the number owner, whereas the second attack can block phone calls made to a set of any numbers in a specific area. Our work belongs to this category; however, it differs from the above study from two major aspects as follows. First, the explored vulnerabilities and attacks are different; this study mainly presents the free data service, data DoS/overcharge, and DoCES attacks. Second, the adversary in the above study requires deploying a malicious eNB and let victim UEs connect to the eNB, whereas only

SDR-based UE without SIMs is needed in this work.

2.3: Related Work on Cellular Services and Model Checking

Some studies have examined cellular network accessibility and resilience for normal services, with model checking being a popular methodology to evaluate the design of cellular network protocols. However, such accessibility and resilience assessments focused on emergency services remain largely unexplored. This is partly due to the complexity of cellular network designs supporting emergency services and the significant challenges in conducting real-world experiments on operational networks, which could disrupt emergency services and raise ethical concerns. In the following, we review prior work on accessibility and resilience for cellular services, as well as the application of model checking to study cellular networks.

Ubiquitous Cellular Services Access. Some studies have examined cellular network accessibility and performance. For instance, Hassan et al. [58] analyzed 5G handover performance during a cross-country trip, while Xu et al. [106] studied TCP disconnections over LTE on high-speed rail systems. Pan et al. [87] investigated extreme mobility effects on throughput and signal quality on high-speed railways. In contrast, our work focuses on cellular emergency services, which operate differently from non-emergency services.

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

Infrastructure-oriented studies [43, 64, 73, 74] explore attacks on public warning systems, while service-oriented studies [56, 60, 62, 81] examine vulnerabilities in emergency voice and text services, including free data service attacks, DDoS attacks, emergency call blocking, and making calls through emergency panels. our 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 [47, 60, 64–66, 72, 102]. However, limited studies used model checking for cellular emergency services. Klischies et al. [73] 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. [60] 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.

CHAPTER 3: ENHANCING THE SECURITY OF EMERGENCY SERVICE (9-1-1) OVER MOBILE NETWORKS

3.1: Overview

This chapter presents our research on enhancing the security of emergency services (9-1-1) over mobile networks[1]. Emergency services are a vital lifeline to people in emergency conditions. The globally-deployed cellular networks with ubiquitous coverage have been the most accessible channel to emergency users. To ensure the availability for emergency uses, cellular standards and regulatory authorities have stipulated requirements for the offering of cellular emergency services. Specifically, from the GSM Association (GSMA) standard [54], emergency services must be supported by mobile phones without SIM (Subscriber Identity Module) cards, which are indicated as anonymous user equipments (UEs), and be free of charge for mobile users. The 3GPP standard [28] requires emergency services to be provided with higher priority than other services. In the U.S., Federal Communications Commission (FCC) [84] stipulates that cellular carriers have to deliver all wireless 911 calls to the public safety answering point (PSAP), which deals with emergency service requests, without respect to call validation results. Thus, cellular emergency services have become highly available and reliable for emergency uses.

The security research of emergency services has attracted much attention recently. Several attacks have been proposed to threaten emergency services, but they mainly focus on distributed denial-of-service (DDoS) attacks [40, 82, 100] against PSAPs (e.g., 911 call centers) rather than the

[1]This chapter is based on three previously published papers by Yiwen Hu, Min-Yue Chen, Guan-Hua Tu, Chi-Yu Li, Sihan Wang, Jingwen Shi, Tian Xie, Li Xiao, and others: (1) "Uncovering Insecure Designs of Cellular Emergency Services (9-1-1)," published in the Proceedings of the 28th Annual International Conference on Mobile Computing and Networking (MobiCom 2022), DOI: 10.1145/3495243.3560534 [62]; (2) "Unveiling the Insecurity of Operational Cellular Emergency Services (9-1-1): Vulnerabilities, Attacks, and Countermeasures," published in GetMobile: Mobile Computing and Communications, Volume 27, Issue 1, DOI: 10.1145/3599184.3599195 [61]; and (3) "Taming the Insecurity of Cellular Emergency Services (9-1-1): From Vulnerabilities to Secure Designs," published in IEEE/ACM Transactions on Networking, Volume 32, Issue 4, August 2024, DOI: 10.1109/TNET.2024.3379292 [44].

Category	Type	Vulnerability / Attack ID	Description
Vulnerabilities	Design defects	V1: Unverifiable emergency IP-CAN session requests (§3.4.1)	The establishment procedure of the emergency IP-CAN session cannot be protected and its initial request is naturally unverifiable.
		V2: Inconsistent emergency IP-CAN session support (§3.4.2)	The inconsistent support of the emergency IP-CAN session between the 3GPP and GSMA standards may fail the establishment.
		V3: Improper cross-layer security binding (§3.4.3)	The network-layer security (i.e., IPSec) is bound to the application-layer security (i.e., SIP registration).
		V4: Non-atomic emergency service initialization (§3.5.1)	UE can only establish an emergency IP-CAN session without doing IMS emergency registration and establishing an emergency session with PSAPs.
		V5: Improper access control on emergency IP-CAN sessions (§3.5.2)	The emergency IP-CAN session is not restricted to deliver traffic to the IMS server based on given PCC rules.
	Operational slips	V6: One-size-fits-all prioritization for emergency IP-CAN sessions (§3.5.3)	The emergency sessions requested by invalid UE IDs (i.e., IMEIs), which can escape from tracking, are not handled differently from those with valid IDs.
Proof-of-concept Attacks	Denial of cellular emergency services	A1: UE blocking (§3.5.4)	Adversary prevents victims from establishing emergency IP-CAN sessions by tampering their requests with UE capabilities unsupported by carriers.
		A2: UE detaching (§3.5.4)	Adversary detaches the victim's emergency IP-CAN session, preventing access to all emergency services.
		A3: Call cancel (§3.5.4)	Adversary cancels the victim's emergency call attempt.
		A4: Call drop (§3.5.4)	Adversary terminates the victim's ongoing emergency call conversation with a PSAP.
	Emergency IP-CAN session hijacking	A5: Free services (§3.5.4)	Adversary gains free data/voice/text services.
		A6: Data DoS/overcharge (§3.5.4)	Adversary bypasses carrier firewalls and injects spam to cause denial of service or excessive data billing to the victim.
		A7: Remote scanning (§3.5.4)	Adversary can remotely scan network services/applications on the victim's device and launch attacks based on discovered vulnerabilities.

Table 3.1: A summary of the identified vulnerabilities and attacks of operational cellular emergency services.

Vulnerability / Attack ID	Related Vulner.	Applicabilities								Victims' devices under attacks
		Carriers					Systems			
		US-I	US-II	US-III	TW-I	TW-II	4G	NSA	SA	
V1: Unverifiable emergency IP-CAN session requests (§3.4.1)	-	✓	✗†	✗†	✓	✓	✓	✓$^{\sigma}$	✗$^{\sigma}$	-
V2: Inconsistent emergency IP-CAN session support (§3.4.2)	-	✓	✗‡	✓	✗‡	✓	✓	✓$^{\sigma}$	✓$^{\sigma}$	-
V3: Improper cross-layer security binding (§3.4.3)	-	✓	✓	✓	✗♯	✗♯	✓	✓$^{\sigma}$	✓$^{\sigma}$	-
V4: Non-atomic emergency service initialization (§3.5.1)	-	✓	✓	✓	✓	✓	✓	✓$^{\sigma}$	✓$^{\sigma}$	-
V5: Improper emergency attach handling (§3.5.2)	-	✓	✓	✓	✓	✓	✓	✓$^{\sigma}$	✓$^{\sigma}$	-
V6: One-size-fits-all prioritization for emergency IP-CAN sessions (§3.5.3)	-	✓	✓	✓	✓	✓	✓	✗$^{\sigma}$	✗$^{\sigma}$	-
A1: UE blocking (§3.5.4)	V2	✓	✗‡	✓	✗‡	✓	✓	✓$^{\sigma}$	✓$^{\sigma}$	Verified on all tested smartphones, including Samsung Galaxy S8/S10/S21, Google Pixel 3/5, and iPhone 13; the vulnerabilities are on the infrastructure side, not device side.
A2: UE detaching (§3.5.4)	V1	✓	✗†	✗†	✓	✓	✓	✓σ	✗σ	
A3: Call cancel (§3.5.4)	V3	✓	✓	✓	✗♯	✗♯	✓	✓σ	✓σ	
A4: Call drop (§3.5.4)	V3	✓	✓	✓	✗♯	✗♯	✓	✓σ	✓σ	
A5: Free services (§3.5.4)	V4,V5,V6	✓	✓	✓	✓	✓	✓	✓σ	✓σ	
A6: Data DoS/overcharge (§3.5.4)	V4,V5,V6	✗∗	✓	✓	✗∗	✗∗	✓	✓σ	✓σ	
A7: Remote scanning (§3.5.4)	V4,V5,V6	✗∗	✓	✓	✗∗	✗∗	✓	✓σ	✓σ	

†: US-II and US-III do not follow what 3GPP stipulates but adhere to FCC regulations [84] by accepting duplicate requests to maximize the availability of emergency services.
‡: US-II and TW-I implement the GSMA's emergency service requirements by supporting both IPv4 and IPv6 for emergency IP-CAN sessions, whereas US-I, US-III, and TW-II follow the 3GPP's by supporting IPv4-only or IPv6-only.
♯: There are two requirements for tested COTS phones to validate V3 due to ethical issues, but we cannot find any for operator TW-I and TW-II: (1) they shall be carrier-certified; (2) they can be customized to intercept IMS signaling messages.
σ: All the vulnerabilities validated in 4G networks, except for V6, can be also applied to 5G NSA networks since they share the smae 4G core networks. More discussion is presented in §3.7.
∗: US-I, TW-I, and TW-II do not support the emergency-to-data-service (E2D) communication.

Table 3.2: A summary of the applicability of the identified vulnerabilities and attacks.

cellular emergency services. Many solutions [49,71,85,98,99] have been thus introduced to address them. For the cellular emergency services, there have been also some proposed attacks [60,64,74] from the literature. Specifically, Lee *et al.* [74] and Hussain *et al.* [64] uncover that fabricated emergency alerts can be sent to victim UEs based on the abuse of cellular alert protocols and the hijacking of paging channels, respectively. Hou *et al.* [60] allow the adversary to not only bypass the victim UE's screen lock to dial any numbers on the emergency panel, but also block phone calls made to a set of numbers in a specific area, by providing the victim UE with a list of fake local emergency numbers via control-plane signaling messages.

The above attacks corresponding to the cellular emergency services mainly target the vulnerabilities on the UE side, but the security of the cellular infrastructure supporting emergency services still remains unexplored. Moreover, the cellular emergency services operate differently from conventional cellular services. Once any conventional designs are applied to the emergency services without careful reviews from a security perspective, security vulnerabilities may arise. Furthermore, allowing anonymous UEs to access the emergency services can increase attack surface of the cellular infrastructure. We are thus motivated to study whether the emergency services in the cellular infrastructure introduce any new security threats to mobile ecosystem or not.

Surprisingly, we discover six security vulnerabilities from operational cellular emergency services in the cellular networks of three major U.S. carriers and two Taiwan carriers: (V1) unverifiable emergency IP-CAN (IP Connectivity Access Network) session requests, (V2) inconsistent emergency IP-CAN session support, (V3) improper cross-layer security binding, (V4) non-atomic emergency service initialization, (V5) improper access control on emergency IP-CAN sessions, and (V6) one-size-fits-all prioritization for emergency IP-CAN sessions.

We then develop two proof-of-concept attacks based on them. The first attack is the denial of cellular emergency service (DoCES) developed based on V1, V2, and V3; it allows the adversary to prevent mobile users from accessing cellular emergency services, and only two SDR (Software-defined Radio) platforms servicing as an attack UE and a sniffer are needed. This attack includes four variants, namely UE blocking, UE detaching, call cancel, and call drop. Our study reveals that

all the five tested cellular networks are vulnerable to at least one of those four attack variants. The second attack developed based on V4, V5, and V6 includes three variants, namely free data/voice/-text service, data DoS/overcharge, and remote scanning. Table 3.1 and Table 3.2 summarize the discovered vulnerabilities, their corresponding proof-of-concept attacks, and the applicability of those identified vulnerabilities and attacks. All of them are experimentally confirmed in those five tested carriers, unless explicitly stated otherwise.

In all the experiments, we take a responsible manner that always prevents emergency calls or texts from being sent to PSAPs. To have a fine-grained control over the UE, we use the SDR platform for all the validation and evaluation experiments, except for the validation of V3, which requires Commercial Off-The-Shelf (COTS) phones. However, it is important to note that the vulnerabilities and attacks are not only limited to SDR-based UEs but also COTS UEs. The major reason is that they exist on the infrastructure side instead of the device.

There have been many studies exploring DoS, free service, and data overcharge attacks in cellular networks [43, 64, 72, 77, 89, 90, 101, 107], but the present study differs from them in the major aspect that it targets cellular emergency services, the operation and requirement of which are different from those of non-emergency services examined by those studies. For example, if an emergency device cannot successfully connect to the current serving network, it shall attempt to exploring all the other available cellular networks; detaching an emergency device is based on not only the DETACH REQUEST, but also other criteria (e.g., no tracking area update is observed) [15], so it does not suffer from the DoS attacks based on forged DETACH REQUEST messages [43,72,107]. Moreover, the proposed free service and data overcharge attacks are launched by exploiting anonymous devices and free emergency services, and can be stealthier than the prior art. Table 3.3 presents a more detailed comparison.

Although we discover vulnerabilities on the infrastructure side, it does not mean that carriers should take the blame. After a careful analysis, we find that all identified vulnerabilities, except for V6, root in design defects of the cellular emergency standards, whereas V6 is an operational slip but exists for all the tested carriers. We further propose countermeasures including not only long-term

Attack	Features	Mirsky et al. [82]	Tsiatsikas et al. [100]	Tu et al. [101]	Yang et al. [107]	Bitsikas et al. [43]
Denial of Services	Victim (Individual/Infrastructure)	Infrastructure	Infrastructure	Infrastructure	Individual	Both
	Service priority obtained	-	-	-	Higher	-
	Require service subscriptions?	✗	✗	✗	○	✗
	Attack stealthiness	High	High	High	Medium	High
Free services/ Data overcharge	Victim (Individual/Infrastructure)	-	-	-	Individual	Both
	Service priority obtained	-	-	-	Normal	Highest
	Require service subscriptions?	-	-	-	○	✗
	Attack stealthiness	-	-	-	Low	High

Attack	Features	Wang et al. [105]	Peng et al. [88]	Peng et al. [91]	Li et al. [76]	Our Work
Denial of Services	Victim (Individual/Infrastructure)	Infrastructure	Infrastructure	Infrastructure	Individual	Both
	Service priority obtained	-	-	-	Higher	Highest
	Require service subscriptions?	✗	✗	✗	○	✗
	Attack stealthiness	High	High	High	Medium	High
Free services/ Data overcharge	Victim (Individual/Infrastructure)	-	-	-	Individual	Both
	Service priority obtained	-	-	-	Normal	Highest
	Require service subscriptions?	-	-	-	○	✗
	Attack stealthiness	-	-	-	Low	High

♯: 3GPP standards stipulate different requirements (e.g., [21]) for both mobile devices and the infrastructure to ensure the emergency service availability. Hence, traditional DoS attacks may not be applied to emergency service users.

Table 3.3: Comparison of proposed attacks and prior art (DoS, free service, and overcharge attacks) using selected features.

security designs, which can address the vulnerabilities completely based on their root causes, but also standard-compliant short-term remedies, which mitigate the impact of the vulnerabilities. We finally evaluate the short-term remedies based on an emulation prototype.

This work makes three key contributions: (1) we identify six vulnerabilities regarding emergency services, as well as validate them experimentally and analyze root causes; (2) we devise two proof-of-concept attacks by exploiting the identified vulnerabilities and assess their real-world impact with three major U.S. cellular carriers and two Taiwanese carriers; (3) we propose a suite of standard-compliant solutions and evaluate them based on a prototype. The lessons learned can secure both cellular network carriers and mobile users.

3.2: Cellular Emergency Service Primer

Network architecture. Figure 3.1 depicts a 4G/5G network architecture supporting cellular emergency services. The emergency service requests (calls or texts) are initiated by the UE with or without a valid SIM card and finally routed to PSAPs, which are connected to the cellular network through the Internet (IP) or the public switched telephone network (PSTN). Within the cellular network, an emergency service request from the UE in turn traverses radio access network (RAN), core network, and IP Multimedia Subsystem (IMS). Notably, 5G and 4G use distinct network entities for similar network functions; for example, the RAN uses base stations (BSs) to offer radio access;

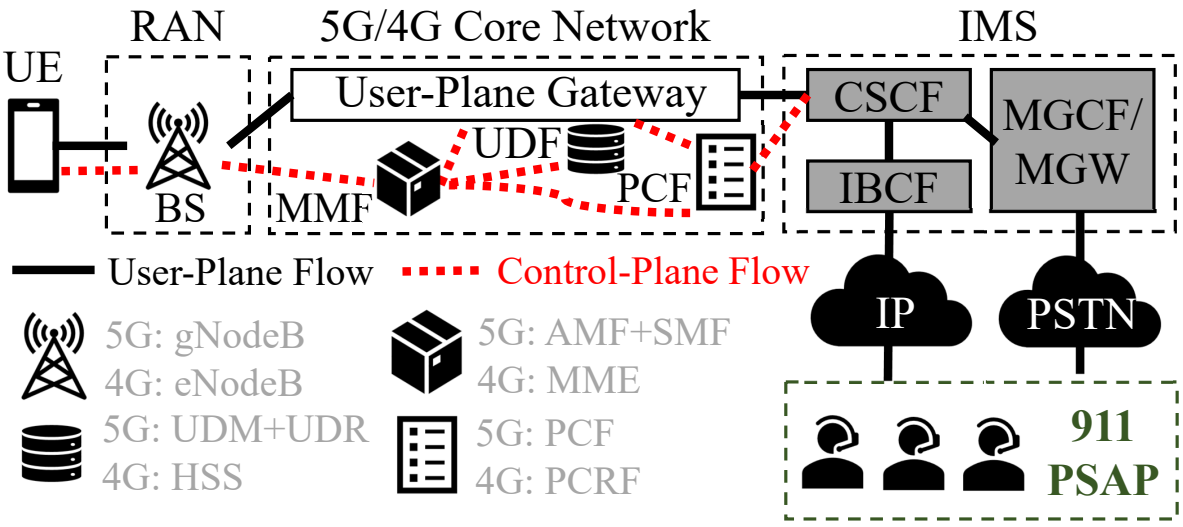


Figure 3.1: 5G/4G emergency service architecture.

the BS is referred to as gNodeB in 5G and eNodeB in 4G. For simplicity, we intentionally avoid 5G/4G telecom jargons which are shown at the left bottom of Figure 3.1, but use generic names of network entities throughout this chapter.

In the core network, the user-plane gateway (UPG) in the user plane is to route user traffic packets from the UE to the IMS network and eventually to the external network (e.g., PSAPs); it provides the emergency IP connectivity for emergency services with the functionality of UE IP address assignment and IMS server selection. In the control plane, there are three main control functions: (1) Mobility Management Function (MMF) manages radio access, user mobility, authentication, resource reservation, and emergency IP connectivity establishment; (2) User Data Function (UDF) is responsible for storing user and service subscription information; (3) Policy Control Function (PCF) is in charge of generating billing policies, QoS parameters, routing control rules and so on. The PCF also creates policies for the emergency IP connectivity and provisions them to the UPG or the MMF to assist in the control for voice and text emergency services.

The IMS provides emergency voice and text services over IP for UEs. It consists of three key network entities: Call Session Control Function (CSCF, referred to as IMS server hereafter), Media Gateway Control Function/Media Gateway (MGCF/MGW), and Interconnect Border Control Function (IBCF). The IMS server is responsible for IMS service signaling, which runs Session

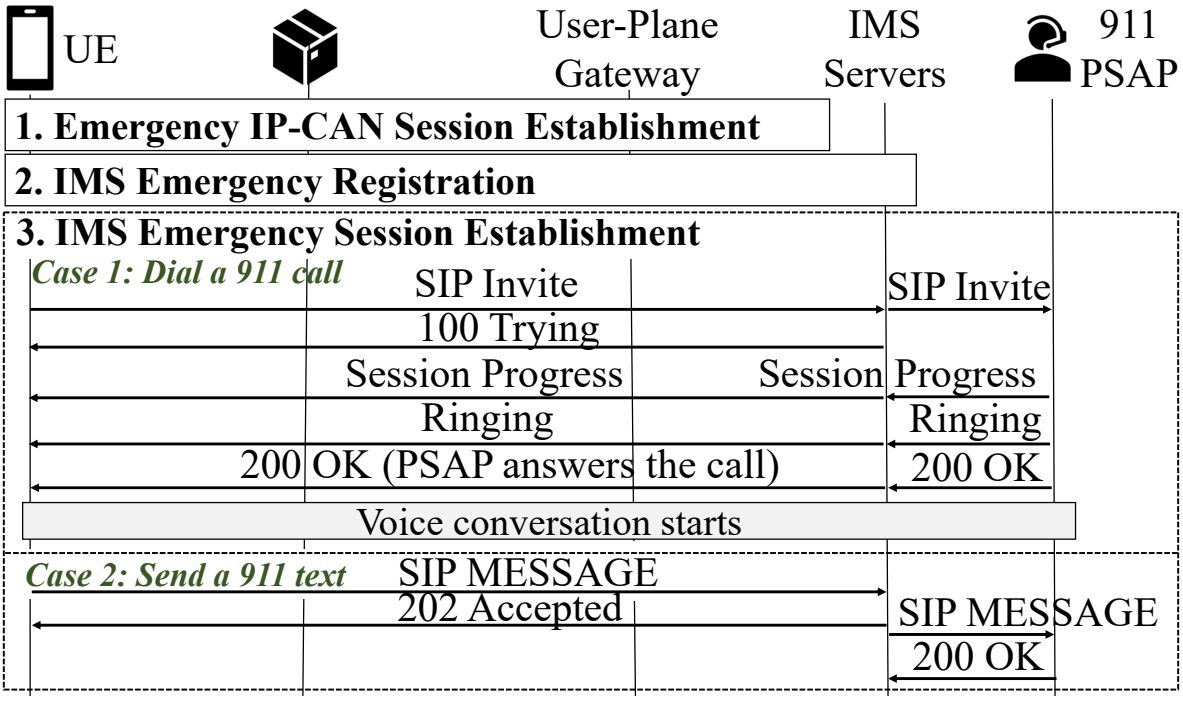


Figure 3.2: IMS emergency service flow.

Initiation Protocol (SIP) [93]. The MGCF/MGW is connected to the traditional PSTN, whereas the IBCF is a session border controller which is interconnected to other IP/IMS networks.

IMS emergency service flow. Figure 3.2 illustrates a service flow for the cellular emergency voice/text service. To establish an emergency session with the PSAP, the emergency UE needs to perform the following three actions. First, *Emergency IP-CAN Session Establishment* allows the UE to obtain the emergency IP connectivity to communicate with the IMS server; an IP-CAN session is identified by the UE's IP address and identity information. Second, *IMS Emergency Registration* [13, 28] has the IMS server and the UE authenticate with each other and enables the UE to register the emergency service. Third, *IMS Emergency Session Establishment* allows an emergency UE to establish an IMS emergency call/text session with the PSAP [13, 28, 52, 53] through the IMS server. The UE sends SIP INVITE and SIP MESSAGE messages to the IMS server for establishing emergency call and text sessions, respectively. Notably, anonymous UEs may be still allowed to access the IMS emergency service without being registered in accordance with local regulatory requirements [30].

3.3: Threat Model, Methodology, and Ethical Consideration

Threat model. In this work, the adversary uses an SDR-based UE to attack operational cellular networks and cellular UEs; the SDR-based UE does not have any SIM card installed, but can successfully connect to operational cellular networks. There are two attacks presented in Sections 3.4.4 and 3.5.4, respectively. In the former, the victims are the cellular users who connect to operational emergency services using anonymous UEs. In the latter, the victims are cellular operators and non-emergency cellular users. For these attacks, neither operational cellular networks nor victim UEs are compromised; it is assumed that the adversary adheres to all cryptographic assumptions (e.g., a ciphered message cannot be decrypted without the ciphering key).

Experimental methodology. We validate the presented vulnerabilities and attacks in the operational cellular networks of three U.S. carriers and two Taiwan carriers, which are denoted as US-I, US-II, US-III, TW-I and TW-II, respectively. Two kinds of emergency UEs are tested in the experiment: (1) SDR-based UEs developed based on the srsRAN [97], which is an open-source 4G/5G software radio suite; and (2) commercial off-the-shelf (COTS) UEs, including Samsung Galaxy S8/S10/S21, Google Pixel 3/5, and Apple iPhone 13. To prevent emergency calls or texts from being accidentally sent to the cellular infrastructure during the experiment, we use the SDR-based UEs with a fine-grained control over network operations to validate vulnerabilities and execute proof-of-concept attacks, but employ the COTS UEs as victim devices in the proposed attacks.

Notably, all the vulnerabilities and attacks are validated in only 4G networks, but they can be also applied to 5G networks; more discussions are given in Section 3.7. There are two reasons for the limited validation. First, there is no any SDR-based platform that can serve as 5G UE to stably connect to operational 5G networks at the submission of this dissertation. While the latest srsRAN [97] offers the 5G UE support, it can be challenging to connect its emulated UE to operational 5G networks since it requires to connect the emulated UE and the base station using a physical cable, or to have a precise clock setting synchronized with the target 5G network.

Second, experimenting with COTS UEs on operational 5G networks is currently not feasible

due to two issues. First, carriers in most areas support only the 5G NSA (Non-standalone) network [51], where the 5G UE will use VoLTE (Voice over LTE) rather than VoNR (Voice over New Radio) for voice services. This phenomenon is observed on all the tested carriers around our campus. Second, according to 3GPP standards [27], if a UE fails in an emergency call attempt, the 5G UE should automatically make a second attempt in other domains (e.g., circuit-switched (CS) fallback, allowing a UE to switch to 3G and access 3G CS voice services). The second attempt cannot be intercepted when generated by the cellular modem.

Ethical consideration. We understand that some feasibility tests and attack evaluations may be detrimental to cellular network carriers and users. We thus proceed with this preliminary study in a responsible manner. Specifically, there were three approaches adopted in the experiment methodology to avoid adverse effects on the infrastructure and cellular user. First, all transmitted messages strictly adhere to 3GPP standards, including both control-plane signalings and IMS signalings, thereby preventing any abnormal behaviors on the infrastructure side. Their volume was comparable to that of normal cellular users. Second, all the victim devices in the experiments were our own devices, so no benign users were harmed. Third, we not only subscribed to *unlimited service plans* for all the experiment devices, but also minimized the resource consumption in the experiments. Specifically, we used SDR-based UEs with only a single antenna and a maximum transmission rate of only 3 Mbps, so the resource consumed by the experiments is much less than that offered by the unlimited plans. Moreover, all the vulnerability validation and attack experiments were conducted with small-scale tests based on the principle of identifying security issues in cellular emergency services rather than exacerbating damages. Notably, in all the experiments, no emergency calls or text messages were sent to operational IMS servers or PSAPs.

Responsible disclosure. We have reported the identified issues and the proposed solutions to U.S. carriers, as well as 3GPP and GSMA standard organizations, and received positive feedback from most of them. Specifically, two U.S. carriers classified the reported issues as **high-level security concerns**, and one of them offered **a security award** for the disclosure. For the 3GPP, after our disclosure, we had a meeting with the chair and key members of the TSG SA3 working group,

which focuses on security and privacy in the 3GPP organization, and were suggested to submit our findings to their next regular SA3 meeting for further discussion. For the GSMA, we reported to its Coordinated Vulnerability Disclosure (CVD) program; currently, we are collaborating with them to validate and address the discovered vulnerabilities. Notably, since the discovered vulnerabilities have not been addressed for the tested carriers, their names are not disclosed in this dissertation.

3.4: Denial of Cellular Emergency Service

For emergency use, UEs shall be always allowed to make emergency calls/texts through a cellular network no matter whether they have valid service subscriptions, according to the FCC 911 regulations [84]. That is, for any U.S. cellular networks, anonymous UEs (i.e., those without valid mobile service subscriptions or SIM cards)can access their cellular emergency services. The goal of this anonymous access is to maximize the availability of emergency services through cellular networks in emergency conditions. It can be also enabled for the UEs with valid subscriptions at the time when they are unable to access the emergency services from their home carrier networks; they are thus allowed to connect to other carrier networks and have the emergency services. However, we discover that such anonymous emergency service access is not well protected, thereby leading to a potential security threat, DoCES. It is mainly rooted in three vulnerabilities: unverifiable emergency IP-CAN session requests (V1), inconsistent emergency IP-CAN session support (V2), and improper cross-layer security binding (V3). In the following, we first introduce each vulnerability and then present the DoCES attack with several variants.

3.4.1: V1: Unverifiable Emergency IP-CAN Session Requests

Since an anonymous UE that attempts to consume the emergency service of a cellular network does not have any security association with the network infrastructure, the establishment procedure of the emergency IP-CAN session cannot be protected and its initial request is naturally unverifiable. When a duplicate establishment request is maliciously presented to the network, the network cannot differentiate it from the initial request. The impact of that malicious duplicate request depends on how the network deals with multiple emergency IP-CAN session requests from the same anony-

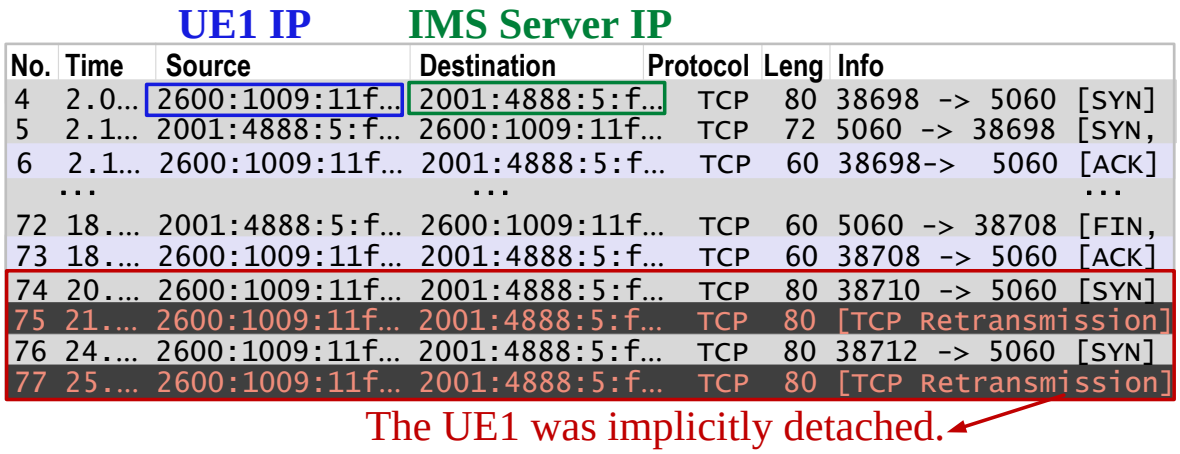
mous UE.

Surprisingly, the 4G and 5G standards take different approaches to handle the duplicate request. The 4G standard (i.e., TS24.301 [21]) stipulates that the MMF shall either reject it with a reason that multiple PDN connections for a given APN are not allowed, or accept it while implicitly detaching the existing established emergency IP-CAN session (i.e., the infrastructure detaches the session without providing any notification to its owner UE.). On the other hand, the 5G standard (i.e., TS23.501 [17]) specifies that the duplicate request shall be always rejected.

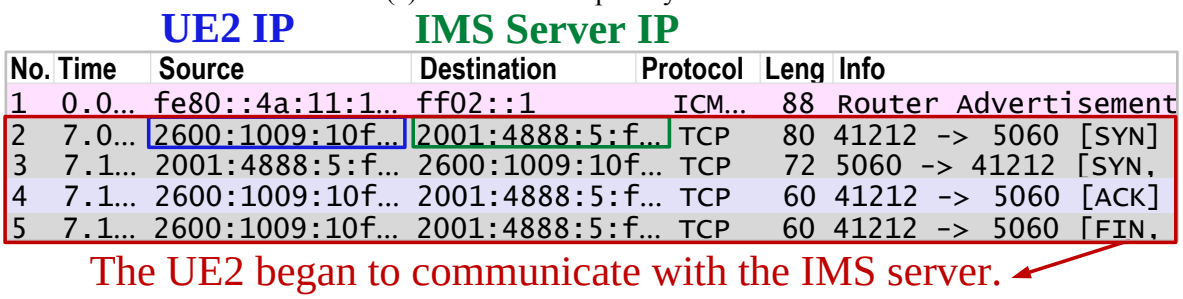
As a result, the adversary may have a chance to prevent anonymous UEs from accessing the emergency services by sending fabricated emergency requests to the network before or after valid requests. Since the requests are not ciphered or integrity-protected, they can be easily fabricated based on the same device ID.

Experimental validation. We validate this vulnerability using two SDR-based UEs: UE1 and UE2; neither of them has a SIM card installed. At the beginning, UE1 performs the establishment procedure of an emergency IP-CAN session with a tested 4G cellular network. Afterwards, UE2 sends the same cellular network a duplicate establishment request with the UE1's device identity, i.e., International Mobile Equipment Identity (IMEI). Once the UE1's emergency IP-CAN session is interrupted by the duplicate request, UE1 can be implicitly detached and then lose the IP connectivity. To detect whether this implicit detachment indeed happens, we make UE1 keep attempting to establish a new TCP connection with the assigned IMS server; the failure of any TCP connection establishment can indicate the loss of the IP connectivity.

We conduct this experiment with all the five carriers. The results show that the UE2's duplicate request can successfully interrupt the ongoing emergency IP-CAN session of the UE1 for three carriers, namely US-I, TW-I, and TW-II, but it does not work for the other two carriers, i.e., US-II and US-III. We here present only the experimental result observed from US-I; the similar results observed from TW-I and TW-II are omitted. As shown in Figure 3.3a, the implicit detachment of the UE1 hinders its TCP connection attempts through its emergency IP-CAN session; moreover, the UE2 can communicate with the IMS server over the new IP-CAN session established based on



(a) The UE1 is implicitly detached.



(b) The UE2 establishes an emergency IP-CAN session successfully.

Figure 3.3: UE2's duplicate request makes UE1's ongoing emergency IP-CAN session be detached from the OP-I network.

the duplicate request, as shown in Figure 3.3b.

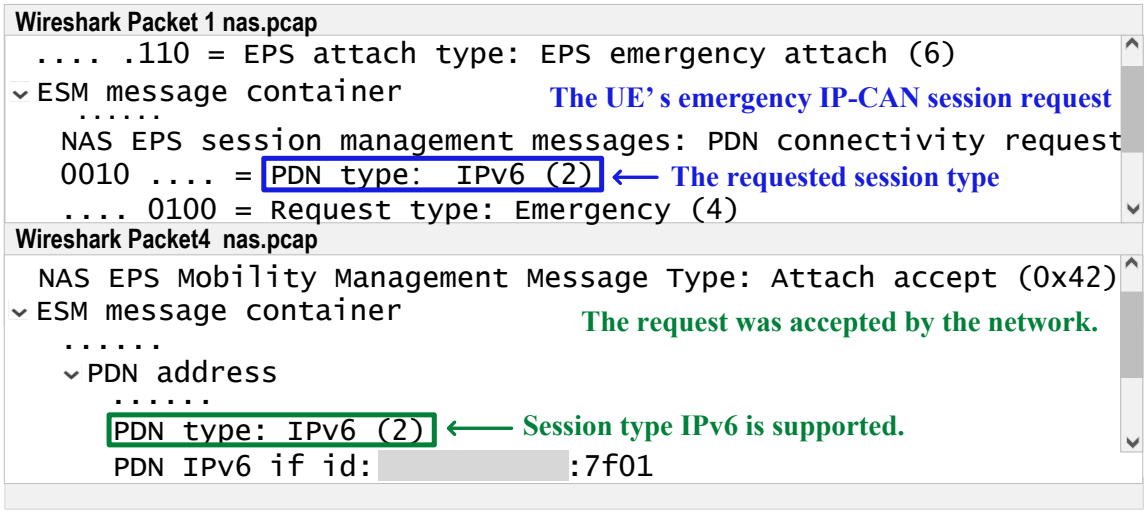
Root cause and lessons. The emergency IP-CAN session requests from anonymous UEs are unverifiable, since they do not have any security context shared with the cellular networks. However, allowing anonymous UEs to have the emergency services cannot be simply prohibited, since it is critical for emergency conditions. Moreover, duplicate emergency session requests cannot be simply forbidden either, because they may be sent by benign anonymous UEs after a system or software crash. It thus calls for a new security mechanism that cannot only secure the cellular network with offered emergency services but also keep the high availability of the emergency services to anonymous UEs.

3.4.2: Vulnerability 2: Inconsistent Emergency IP-CAN Session Support

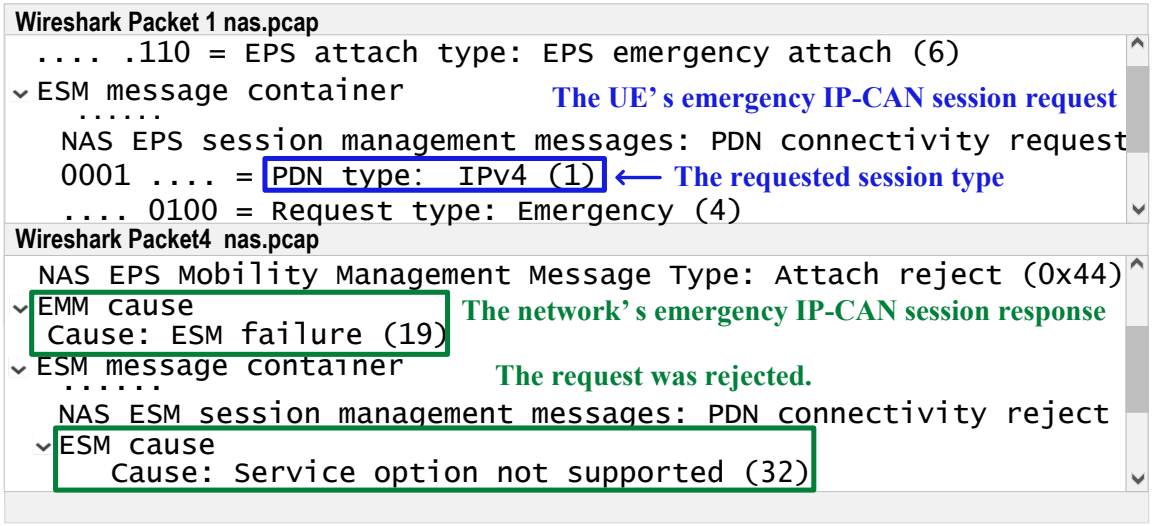
To establish an emergency IP-CAN session successfully, the UE and the cellular infrastructure (i.e., MMF in Figure 3.1) need to settle down all service options, including security algorithms, IP-CAN session types (e.g., IPv4 or IPv6), for the emergency IP-CAN session. The unsuccessful session options negotiation between the UE and the infrastructure (e.g., the UE insists on using an option that is not supported by the infrastructure) can lead to the failure of establishing an emergency IP-CAN session. Although both 3GPP and GSMA stipulates mandatory options for emergency IP-CAN sessions, not all requirements are consistent between these two international telecommunication standardization organizations. For example, GSMA [52] requires the UE and the infrastructure to support the IP-CAN session types of IPv4 and IPv6, whereas 3GPP has relatively loose requirements. In particular, [15, 21] allows UEs to support three types of IP-CAN sessions, namely IPv4-only, IPv6-only, and IPv4v6 (i.e., supporting both IPv4 and IPv6). Moreover, the infrastructure may override the UE-requested IP-CAN session type based on its operator policies, user subscriptions, or local regulatory regulations. Such inconsistent emergency IP-CAN session support between GSMA and 3GPP may lead to improper assumptions, operations and implementations on both UE and infrastructure sides, thereby resulting in unexpected emergency IP-CAN session establishment failures and may be exploited by adversaries to launch various UE blocking attacks.

Experimental Validation. We validate this vulnerability by using one SDR-based UE without any SIM card. The UE is configured to request the following three session types in turn, IPv4-only, IPv6-only, and IPv4v6, while performing the emergency IP-CAN session establishment for three times in each experiment run. The experiment is run for each of the tested five carriers.

The experimental results yield two findings. First, the UE can successfully establish an emergency IP-CAN session with each of the session types from US-II and TW-I, and obtain both IPv4 and IPv6 addresses when requested; it indicates that these two carriers adhere to the GSMA regulation. Second, the other three carriers, namely US-I, US-III, and TW-II, support only one session type; specifically, they support IPv6, IPv6, and IPv4, respectively. So, they follow the 3GPP regulation. Take US-III as an example. As shown in Figure 3.4, the UE can successfully establish



(a) Session establishment succeeds when the IPv6 type is requested.



(b) Session establishment fails when the IPv4 type is requested.

Figure 3.4: US-III: only IPv6 is supported for the emergency IP-CAN session, but both IPv4 and IPv6 types work for non-emergency IP-CAN sessions.

an emergency IP-CAN session with the IPv6 address type, whereas the establishment request is rejected when the IPv4 address type is requested, as shown in Figure 3.4b; notably, US-III supports both IPv4 and IPv6 for non-emergency IP-CAN sessions (e.g., accessing the Internet). The error is an ESM (EPS Session Management) failure with a cause, Service Option Not Supported [21]. The ESM failure is also observed from US-I and TW-II when an unsupported session type is requested, but with different causes, Insufficient Resources [21] and Service Option Not Supported, respectively.

Root Cause and Lessons. The root cause lies in the inconsistent regulations between 3GPP and GSMA; the IP-CAN session type may be merely one instance of them. Although the committees of both standards have their own rationalities, such as ensuring service availability for emergency users and complying with regulatory requirements, we believe that a closer collaboration between them is still necessary to develop consistent designs for cellular emergency services.

3.4.3: V3: Improper Cross-layer Security Binding

The UE with a valid mobile subscription cannot establish IPSec security associations with the IMS server for the emergency services until it completes the IMS emergency registration [9], since the IPSec ciphering and integrity keys are derived from the registration procedure. It appears that the network-layer security (i.e., IPSec) is bound to the application-layer security (i.e., SIP registration). Therefore, when anonymous UEs are allowed to skip the IMS registration due to no security context shared with the core network, the IPSec security associations with the IMS server cannot be built. It can leave the IMS emergency sessions of anonymous UEs to be unprotected; thus, the sessions may suffer from attacks.

Experimental Validation. We validate this vulnerability by observing whether anonymous UEs indeed have unprotected IMS emergency call sessions. In the experiment, COTS UEs and operational cellular networks are considered. In order to prevent any emergency call signaling messages from being routed to PSAPs, we develop a smartphone application, namely 911-CallBlocker, which discards all the SIP INVITE messages sent from the smartphone to the network infrastructure. After activating the 911-CallBlocker at the tested smartphone without any SIM card (i.e., anonymous UE), we dial 911 while using TCPDump to record all the packets. Notably, we find that the emergency calls of the TW-I/TW-II-certified phones without SIM cards are made based on the 3G CS call technology, instead of the IMS-based one; thus, the 911-CallBlocker cannot prevent them from being routed to PSAPs. To avoid the possible ethical issue, the validation experiment is conducted for only three US carriers.

For all the tested carriers, we obtain the same observations. First, the IMS emergency registration procedure is not performed. Second, the SIP INVITE messages are all sent in plain-text without

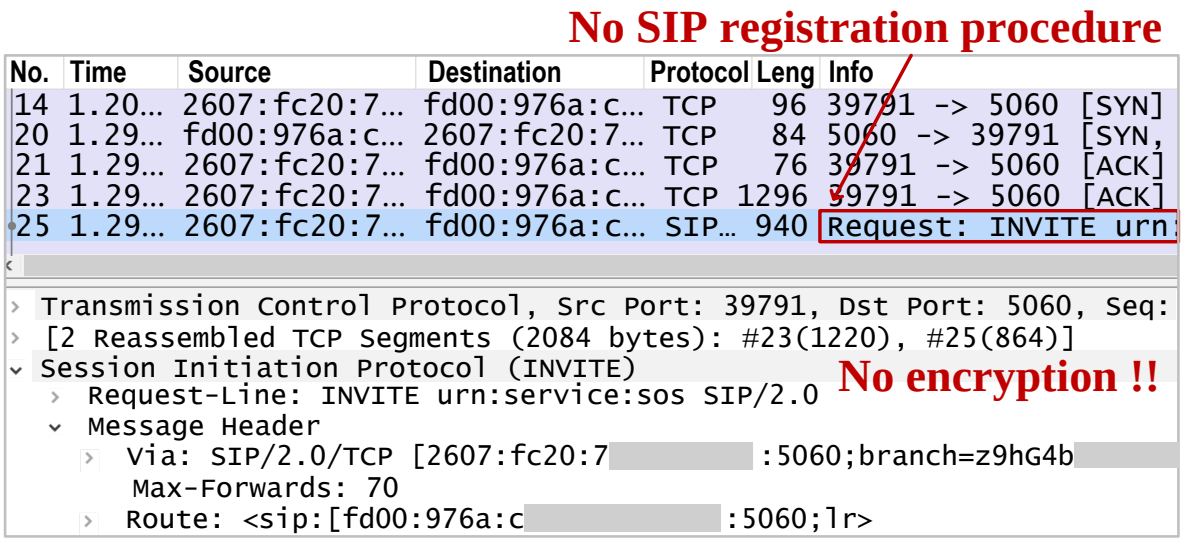


Figure 3.5: An unencrypted emergent call message is observed for a COTS phone without any SIMs in the US-III network.

ciphering protection. Figure 3.5 shows a representative trace from an anonymous UE connecting to the emergency service of the US-III network. Thus, the critical session information (e.g., call-ID and call tag) can be leaked to the adversary; it can thus allow the adversary to manipulate ongoing emergency call sessions.

Root cause and lessons. The current cross-layer security design that binds the IPSec security association establishment to the IMS registration does not come without any reasons. It is necessary for non-emergency UEs to do the IMS registration; when the registration fails, no IMS services are provided to the UEs. That is, the IPSec is needed only when the registration succeeds; the cross-layer security binding is thus reasonable and can work properly.

However, this security binding should not be directly applied to the cellular emergency services without any modifications. Anonymous emergency UEs can skip the IMS registration but are still allowed to establish IMS emergency sessions. Without the registration, the improper security binding causes the IPSec security association establishment to be skipped. Such design is explicitly stipulated in the 3GPP/GSMA emergency service standards [28, 54], so it can happen in all standard-compliant mobile devices. As a result, it calls for a security mechanism that is decoupled from the IMS registration and can protect the emergency service sessions.

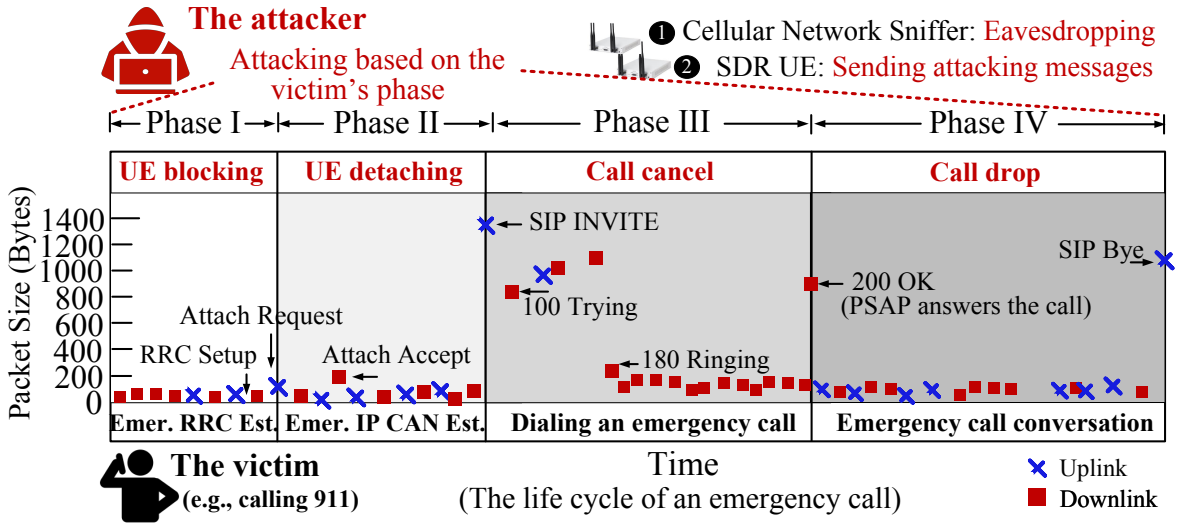


Figure 3.6: DoCES attack with four variants, namely UE blocking, UE detaching, call cancel, and call drop.

3.4.4: Proof-of-concept Attacks

We exploit the above three vulnerabilities to launch the DoCES attack against anonymous UEs. This attack contains four attack variants that together can almost cover the entire life cycle of an emergency call, as illustrated in Figure 3.6; specifically, they are *UE blocking*, *UE detaching*, *call cancel*, and *call drop* attacks. Launching this attack requires two device components: (1) a cellular network sniffer, which eavesdrops on the communication of nearby UEs and identifies attackable UEs (i.e., anonymous UEs initiating cellular emergency services), and (2) an SDR-based UE, which sends attack messages to the cellular networks where victim UEs are. Notably, this attack does not require the adversary to deploy rouge cellular infrastructure near victims. Moreover, the adversary does not need to be at the scene of victims; instead, the sniffer, together with the attack UE, can be deployed at any location where the victims' communication can be eavesdropped on.

We next present the experimental setting and then elaborate on each attack variant. Note that the following evaluation results demonstrate that the adversary could prevent mobile users from accessing emergency services in certain settings, but these should not be interpreted as common failures of operational cellular systems.

Experimental Setting. We evaluate the DoCES attack with four variants on an emulation testbed

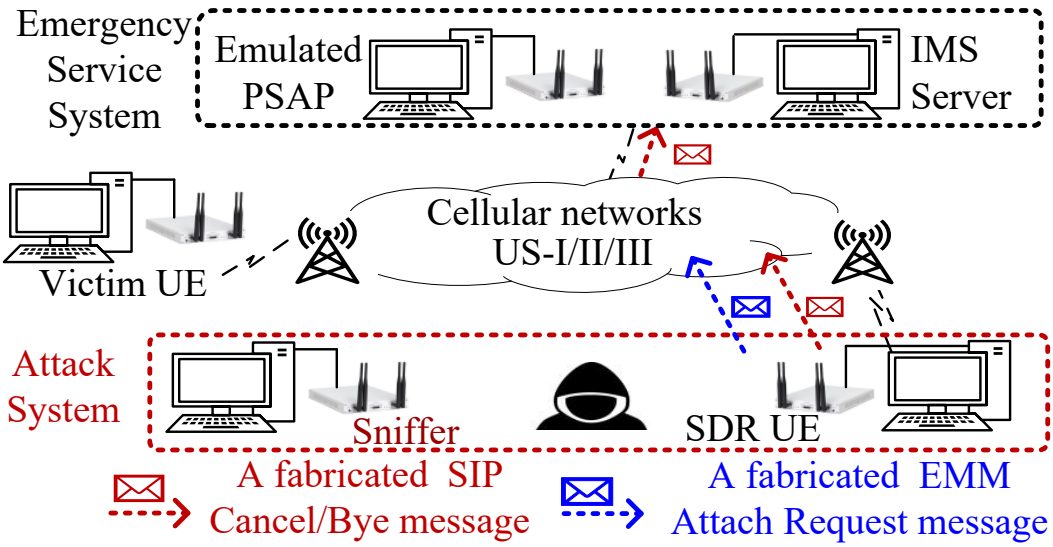


Figure 3.7: An emulation testbed for DoCES attack evaluation.

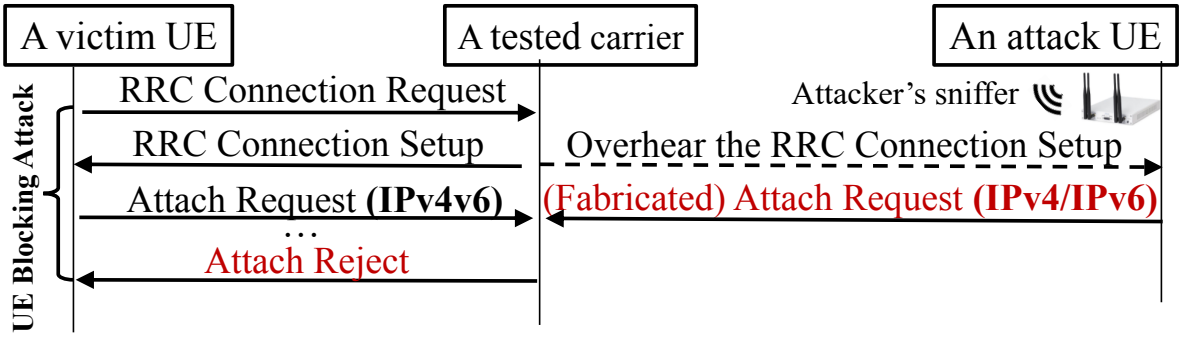
deployed over the networks of the three U.S. carriers. Using the emulation testbed is to prevent any emergency calls from being sent to PSAPs. Figure 3.7 shows the testbed with three major parts, namely the emergency service system, the attack system, and the victim UE. The emergency service system includes an IMS server developed based on the open-source LinPhone VoIP SIP server [46] and an emulated IP-based PSAP; both of these two components are emulated using SDR-based UEs connecting to the tested cellular network via emergency IP-CAN sessions. Thus, all the SIP messages generated by the victim UE are sent to the emulated PSAP rather than actual PSAPs. The attack system consists of a cellular network sniffer and an SDR-based UE with the LinPhone VoIP SIP client installed; the UE also connects to the tested cellular network with an emergency IP-CAN session. The victim UE is built based on the same SDR-based UE as the one in the attack system. Notably, only the IMS-related activities are emulated, but the underlying communications are still based on the emergency IP-CAN sessions established between the SDR-based UEs and the operational cellular networks.

UE Blocking Attack. We exploit the vulnerability V2 to devise the UE blocking attack that can cause the victim UE's emergency IP-CAN session request to be rejected. To launch this attack, the adversary needs to know the unsupported type of the emergency IP-CAN session for the target carrier network, and then overshadows the victim's Attach Request message using a fabricated

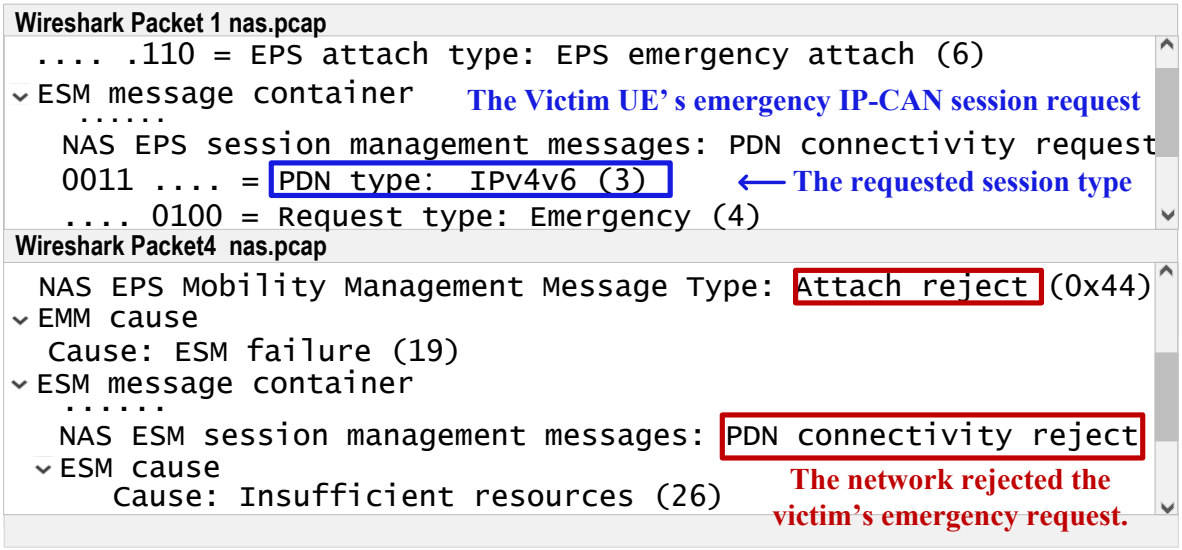
message that requests a unsupported session type.

Figure 3.8a illustrates the procedure of this attack. To establish an emergency IP-CAN session, the victim UE initially sets up a RRC (Radio Resource Control [33]) connection with the base station. In the RRC Connection Request message, the cause of the RRC connection establishment shall be set to "emergency". Such emergency connection message can be identified by the adversary using a cellular network sniffer and then its sender is considered as a potential victim UE. Given the information contained in the RRC messages, the SDR-based attack UE can fabricate a request message of the emergency IP-CAN session establishment with an unsupported session type for the target network and transmit it using a stronger signal to overshadow the victim's request message. In particular, the SDR-based attack UE is implemented on a SDR platform using srsRAN (v20.10.1) [97] to monitor Physical Downlink Control Channel (PDCCH) to collect the uplink and downlink control information (i.e., uplink and downlink channels assignment information) [26] from nearby cellular devices. To overshadow a victim device's Attach Request message, we modify the values of the transmission gain (`tx_gain`) to generate stronger signals and transmit them using victim's assigned uplink channels; notably, a successful overshadowing attack requires to generate signals with at least 3dB stronger than the victim's signals [107]. Once the base station accepts this fabricated request message, the victim will get the Attach Reject message due to the requested, unsupported session type.

We evaluate this attack with 10 experiment runs in the US-I network. After the victim UE exchanges the RRC connection messages with the base station, the attack UE overhears the RRC Connection Setup message and then sends out a fabricated Attach Request message with the unsupported session type, IPv4. Although the Attach Request message sent by the victim UE specifies the IPv4v6 address type, as shown in Figure 3.8b, it is rejected with an Attach Reject message; all the experiment runs yield the same result and confirm the effectiveness of the UE blocking attack. Notably, although our open-source cellular radio sniffer can be used for only downlink traffic which cannot accurately distinguish participating victim devices from others, it can be done by other commercial sniffers (e.g., WaveJudge 5000 LTE Analyzer). We thus conduct this experiment



(a) Attack procedure.



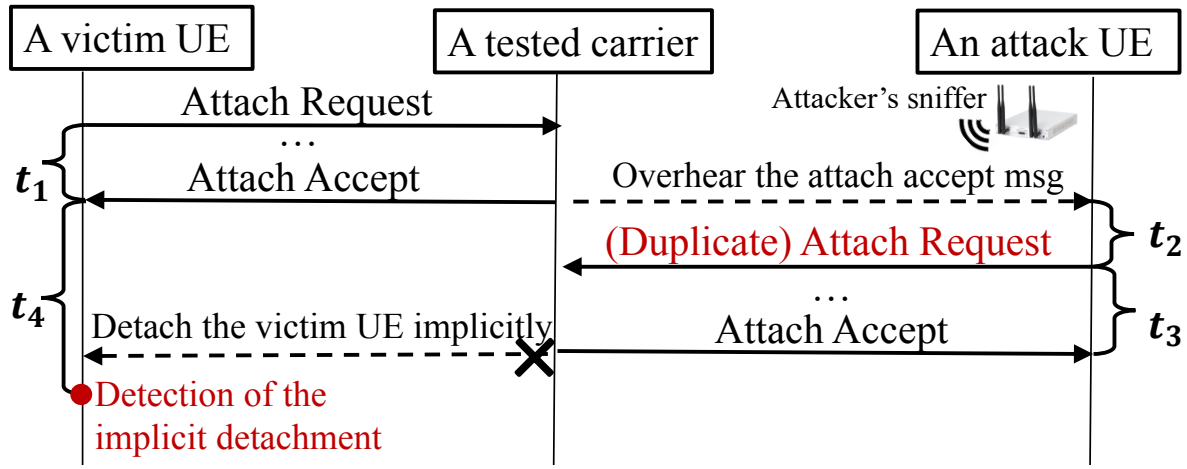
(b) The victim UE's emergency IP-CAN session request with the requested IPv4v6 type is rejected by US-I after a fabricated request with a requested type IPv4 is sent by the attack UE; the EMS error cause is Insufficient Resources.

Figure 3.8: UE blocking attack.

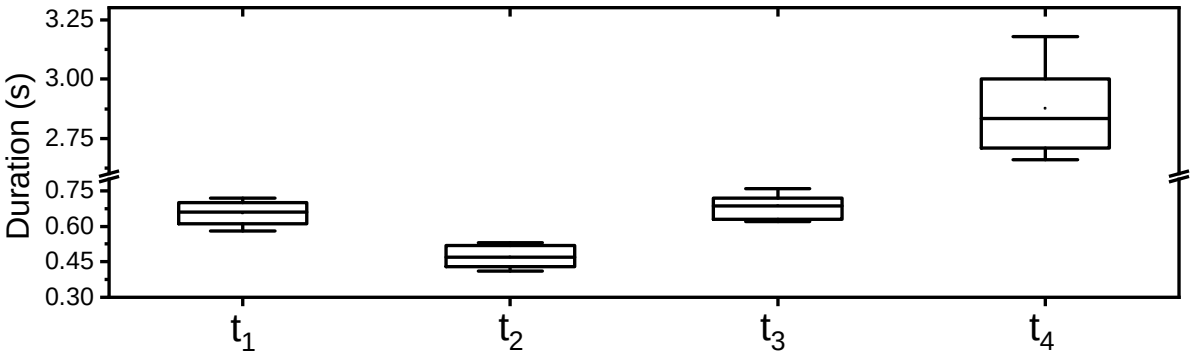
in a controlled environment (i.e., at our laboratory during holidays) to prevent real emergency calls from being blocked.

UE Detaching Attack. We next devise the UE detaching attack that implicitly detaches emergency UEs based on the vulnerability V1. To exploit the V1, the attacker needs to identify potential victim UEs which are establishing emergency IP-CAN sessions, and obtain their device IDs. To this end, a cellular network sniffer can be deployed to monitor particular control-plane signaling messages including EMM Attach Accept and EMM Attach Request [21] from nearby cellular UEs.

Figure 3.9a illustrates the attack procedure. While a victim UE nearby the sniffer performs the EMM Attach procedure [21] to establish an emergency IP-CAN session with a cellular network,



(a) Attack procedure.



(b) The time durations shown in the above figure (0/25/50/75/100th percentiles).

Figure 3.9: UE detaching attack.

the sniffer in the attack system can overhear the EMM Attach Accept message, which indicates the finish of the session establishment, from the cellular network. Afterwards, the SDR-based attack UE can fabricate a duplicate Attach Request message using the UE's IMEI. Once the attack succeeds, the network implicitly detaches the victim UE while replying Attach Accept to the attack UE.

We evaluate this attack by conducting the attack procedure for 10 runs in the US-I network. The evaluation result shows that the victim UE can be implicitly detached in all the experiment runs; that is, it does not receive any notification from the network after being detached. Figure 3.9b shows the measured values of the time durations in the attack procedure. It is observed that the attacker can successfully detach the victim UE within 2.66∼3.18 s (i.e., t4) right after the emergency session is established. Note that getting the IMEI requires capturing the EMM Attach Request message from

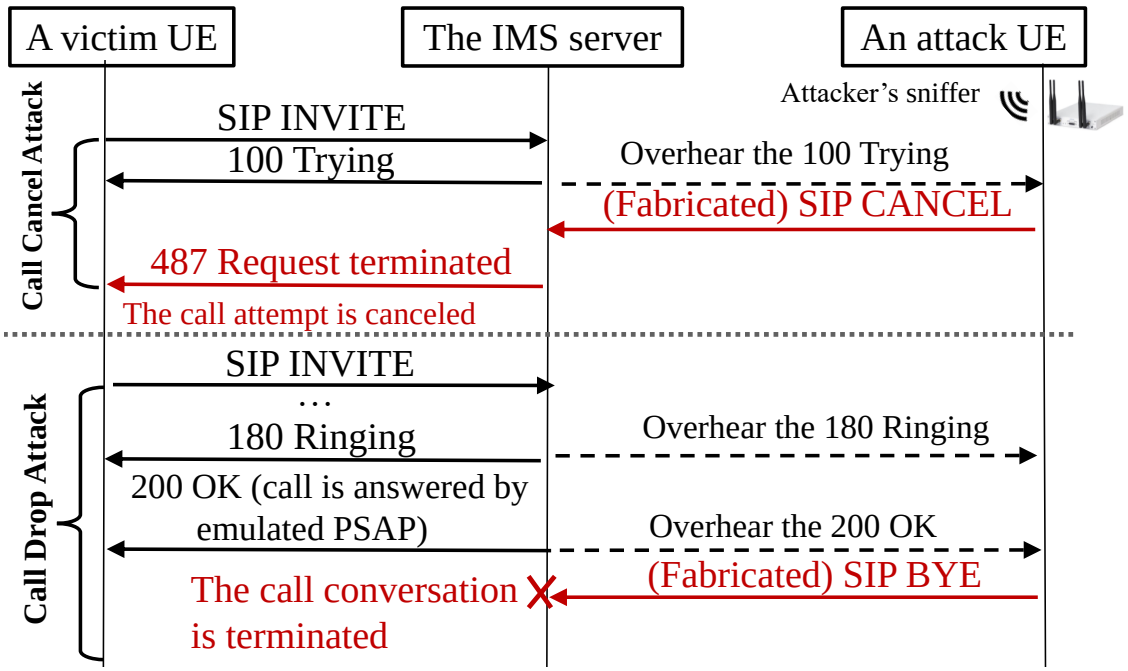


Figure 3.10: Message flows of call cancel and call drop attacks.

the uplink traffic, the victim UE's IMEI is thus pre-given in the experiment due to the limitations of our open-source cellular network sniffer.

Call Cancel Attack. We then devise the call cancel attack, which cancels the victim UE's emergency call attempt, by exploiting the vulnerability V3; it allows the attacker to overhear and fabricate SIP messages. As shown in the upper part of Figure 3.10, in this attack, a fabricated SIP Cancel message is sent to the IMS server as soon as a SIP 100 Trying message sent to the victim is overheard (see Figure 3.2). After receiving the fabricated message, the IMS cancels the victim UE's call attempt by replying with a message of Request Terminated. Notably, to fabricate a valid SIP Cancel message, the adversary can obtain required session information including Call-ID, tag@From, and branch@Via [93], from the SIP 100 Trying message.

In the evaluation, the victim UE initiates a SIP call to the emulated PSAP, but the PSAP does not answer the call. Specifically, the victim UE sends a SIP INVITE message with emulated PSAP's number to the IMS server. Meanwhile, the attack system can overhear the SIP 100 Trying message from the network sniffer and then compose a SIP Cancel message; afterwards, the SDR-based attack UE sends this fabricated SIP Cancel message to the IMS server. The result shows that the

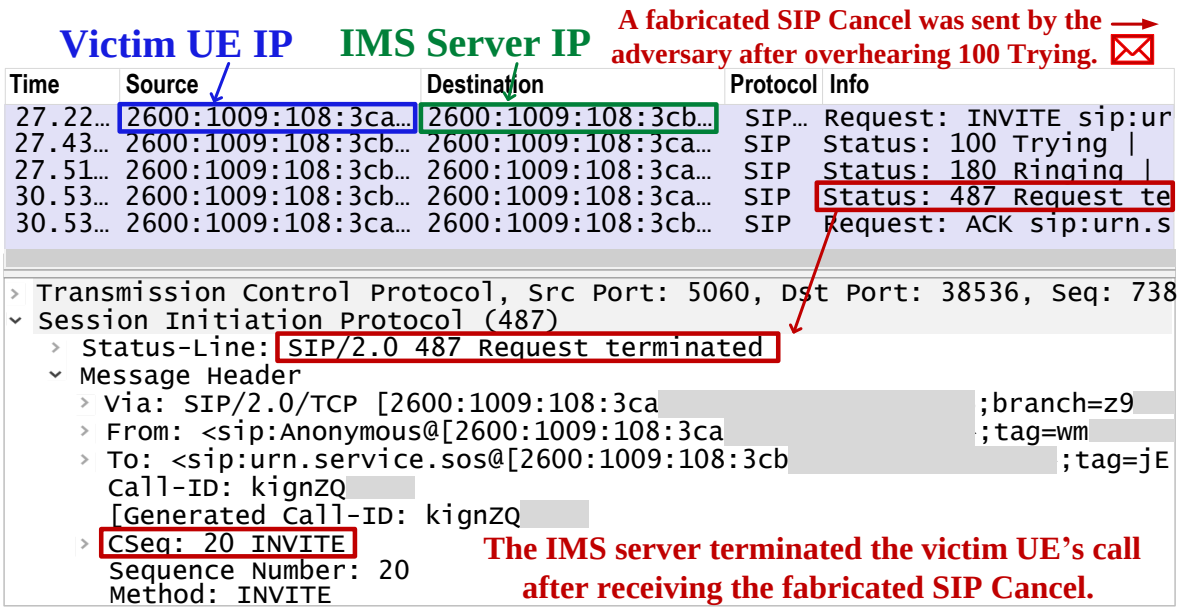


Figure 3.11: An emergency call is terminated by a fabricated SIP CANCEL message sent by the adversary.

victim UE receives a message of the 487 Request terminated from the IMS server; it indicates that the victim UE's emergency call is successfully canceled. Figure 3.11 shows a representative trace of this successful attack result in the US-I network; the same results are observed in all the three carriers.

Call Drop Attack. The attacker can also exploit the V3 to launch the call drop attack by sending a forged SIP Bye message after overhearing the SIP 200 OK message. It can cause an ongoing emergency call of the victim UE to be terminated. This attack is launched by sending a fabricated SIP message to the IMS server, but it has two major differences. First, it can terminate an ongoing emergency call conversation between the victim and the PSAP. Second, the fabricated SIP message is the SIP Bye, which requires an additional piece of SIP session information, tag@To, compared with the SIP Cancel; it can be collected from the SIP 180 Ringing. As shown in the lower part of Figure 3.10, after overhearing the SIP 200 OK message, the attacker can send a fabricated SIP Bye message to the IMS server on behalf of the victim UE. Once the IMS server accepts the fabricated message, the victim UE's ongoing emergency call will be terminated. The experiment setting of this attack evaluation is the same as the previous one, besides that the emulated PSAP answers the victim's call. The result shows that the the victim UE does not receive any messages from the IMS

server but the voice conversation is terminated.

3.5: Emergency IP-CAN Session Hijacking

The emergency IP-CAN session is established whenever a cellular emergency service is requested. Particularly, the emergency service request can be issued from anonymous UEs and be free of charge for cellular users due to its emergency purpose [21,23,28,54]. It can be thus more vulnerable than other non-emergency services. However, we discover that no additional security mechanisms are introduced to protect the emergency IP-CAN session; thus, it could be arbitrarily established and then hijacked to launch a variety of attacks, e.g., free data/voice/text service and DoS attacks. In the following, we first identify three vulnerabilities, namely non-atomic cellular emergency service initialization (V4), improper access control on emergency IP-CAN sessions (V5), and one-size-fits-all prioritization for emergency IP-CAN sessions (V6); then, three proof-of-concept attacks are proposed.

3.5.1: V4: Non-atomic Cellular Emergency Service Initialization

The cellular emergency service initialization is triggered right after a user submits an emergency call/text request on the UE. It consists of three actions, as described in Section 3.2. For the timely delivery of an emergency service request, the initialization is expected to have the atomic property where those three steps are executed continuously without being decoupled or being interleaved with other UE actions. Specifically, the UE can only do IMS emergency registration or/and establish an emergency session with a PSAP whenever an emergency IP-CAN session, which is built for the exclusive use, is established. After the initialization, the emergency service request can reach the PSAP.

However, the cellular network infrastructure may not fulfill this property, since no related security mechanisms are stipulated in the 3GPP/GSMA standards [21, 23, 28, 54]. It may allow an adversary to establish an emergency IP-CAN session to abuse while skipping the last two initialization actions. Without the IMS emergency registration or/and session establishment, the IMS server and the PSAP cannot be aware of the abuse. More threateningly, the emergency IP connectivity

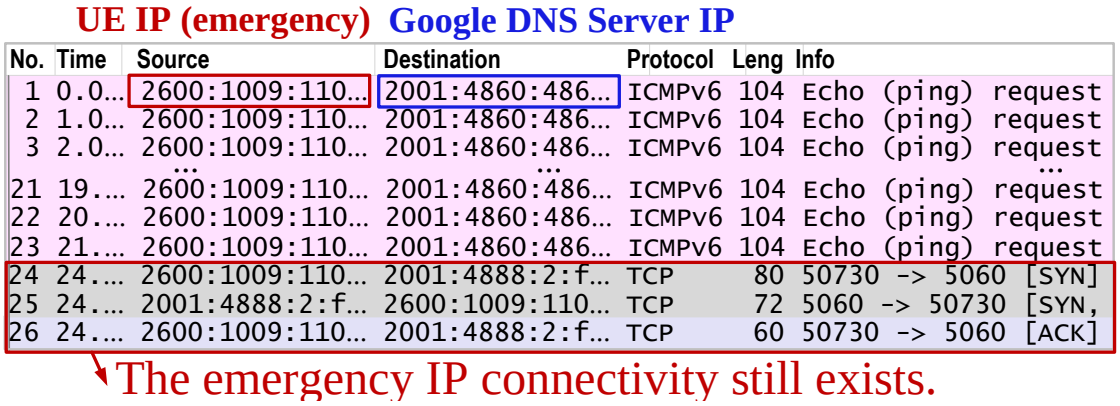


Figure 3.12: The UE can keep the emergency IP-CAN session active by periodically sending packets out.

can be requested by anonymous UEs, so it is challenging to trace back to the adversary.

Experimental Validation. We validate this vulnerability by developing an SDR-based UE using the srsRAN [97]. The UE without any SIM card installed is made to perform the emergency IP-CAN session establishment with five carriers, but skip the last two initialization actions and transmit no packets to the infrastructure.

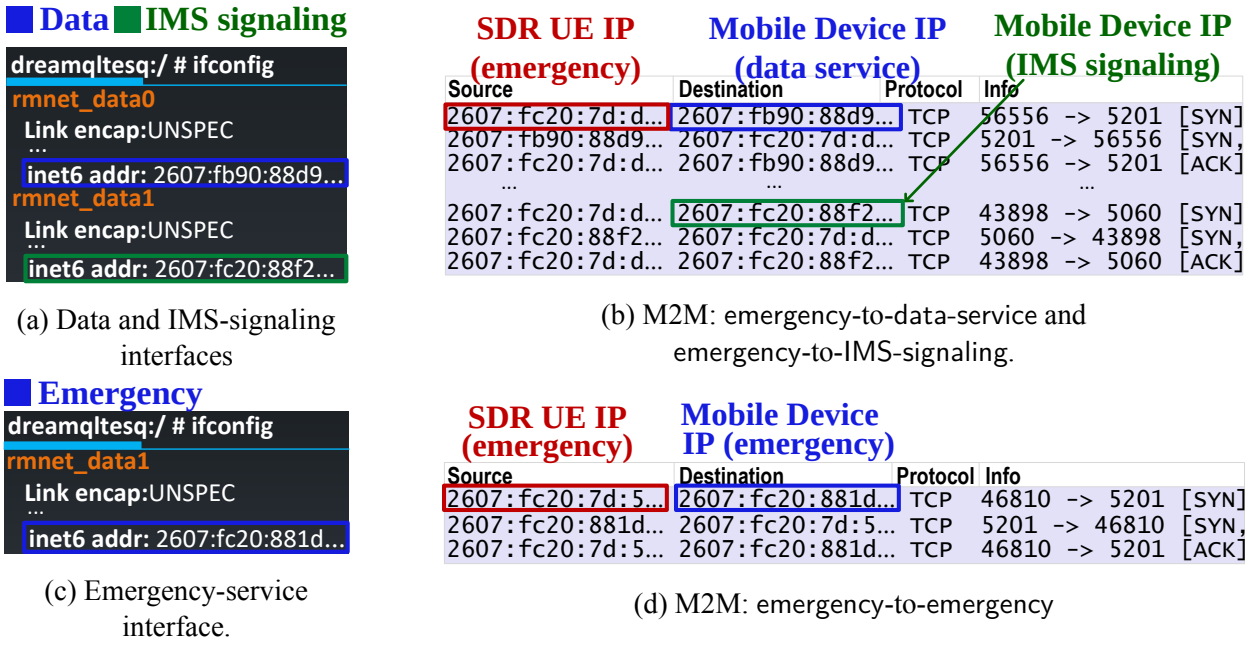
We have two findings. First, the anonymous UE can successfully obtain an IP address for the established emergency IP connectivity from each carrier. Second, the emergency IP connectivity can be interrupted by the infrastructure (i.e., the UE is implicitly detached), after a period of time; 10s, 5s, 3s, and 30s are taken by US-I, US-II, US-III, and TW-I, respectively. For TW-II, it is observed that the emergency IP connectivity can last for longer than 60 seconds without interruption. It can be thus inferred that an inactivity timer is deployed by carriers to protect the emergency IP connectivity from being abused. Nevertheless, we discover that the UE can prevent the interruption by sending packets out periodically; moreover, the destination is not necessarily to be the IMS server. As shown in Figure 3.12, the UE can keep the emergency IP connectivity active by sending ICMP packets to the Google DNS server; notably, no ICMP response packets are received by the UE, but the major purpose that the emergency IP connectivity appears to be in use with those outgoing packets has been achieved. In sum, *an adversary can obtain the emergency IP connectivity and keep it active for a long time.*

Root cause and lessons. This vulnerability can be attributed to a design defect that the cellular infrastructure does not enforce the atomicity of the cellular emergency service initialization. This design defect appears when the emergency service migrates from the 2G/3G circuit-switched (CS) system to the 4G/5G packet-switched (PS) one without a careful security review. In the CS system, the emergency service initialization is completely taken charge of by a single network entity, MSC (Mobile Switch Center [2]), so the atomicity can be easily ensured by the MSC.

However, the emergency service becomes to be IMS-based in the PS system and the initialization is decomposed into two parts, the emergency IP-CAN session establishment and the IMS emergency registration/session establishment, which are managed by the MMF and the IMS server, respectively. Without an additional security mechanism stipulated to protect the emergency service initialization among them, they do not cooperate to ensure the atomicity. Specifically, the MMF can know which UEs obtain the emergency IP connectivity, but have no information about whether those UEs continue to proceed with the IMS emergency service operation; on the other hand, the IMS server does not know which UEs have gained the emergency IP connectivity. Thus, it calls for a concerted solution to ensure the atomicity.

3.5.2: V5: Improper Access Control on Emergency IP-CAN Sessions

The access control on emergency IP-CAN sessions is fulfilled by the PCF to provision PCC (Policy and Charging Control) rules for MMFs or UPGs [7, 19]. For an IP-CAN session, each PCC rule identifies a set of service flows based on the 5-tuple information (i.e., source/destination IP addresses, source/data port numbers, and transport protocol ID) and the corresponding service flows are managed based on an associated policy control setting, including precedence, QoS parameters (e.g., maximum uplink/downlink throughput), gate status (allowed or disallowed), etc. Thus, for the exclusive use of the emergency service, the emergency IP-CAN session should be restricted to deliver traffic to the IMS server based on given PCC rules. However, the cellular network standards [7, 19] do not stipulate such a regulation or give the PCF the information of the IMS server assigned to emergency UEs during their emergency IP-CAN session establishment, so the restriction may be ignored. Without the access control, adversaries may abuse emergency IP-CAN



(a) Data and IMS-signaling interfaces

(b) M2M: emergency-to-data-service and emergency-to-IMS-signaling.

(c) Emergency-service interface.

(d) M2M: emergency-to-emergency

Figure 3.13: An SDR-based UE uses the emergency IP-CAN session to communicate with another UE in OP-III.

sessions to access the Internet or other cellular devices.

Experimental validation. We conduct an experiment to examine whether the emergency IP-CAN session is restricted to only service flows between the UE and the IMS server. Two types of service flows which do not reach the IMS server are tested for those three U.S. 4G carriers: mobile-to-Internet (M2I) and mobile-to-mobile (M2M), which represent the communication between the UE using the emergency IP-CAN session and Internet hosts, and the communication between that emergency UE and another tested UE, respectively. For the M2M case, we further test three kinds of IP-CAN sessions that may be used by the tested UE: (1) the data-service IP-CAN for Internet access, (2) the IP-CAN of the IMS call signaling, and (3) the emergency IP-CAN. Notably, the UE creates a network interface for each IP-CAN session; as shown in Figure 3.13a, the interfaces of the data-service and IMS-signaling IP-CAN sessions can be observed, whereas Figure 3.13c shows the interface of the emergency IP-CAN session.

In this experiment, we still use the SDR-based UE without SIM card to obtain an emergency IP-CAN session from each tested carrier network. For the M2I case, the UE is tested to communicate with the Google DNS server using the emergency IP-CAN. In the M2M case, two phones are

Carriers	Mobile-to-Internet	Mobile-to-Mobile		
		E2E	E2IMS	E2D
US-I	X	O	X	X
US-II	X	O	X	O
US-III	X	O	O	O
TW-I	X	O	O	X
TW-II	X	O	O	X

Table 3.4: The available communication cases based on the emergency IP-CAN session vary with carriers.

connected to the tested carrier network; one phone with a valid SIM card can obtain two IP-CAN sessions for *data service* and *IMS signaling*, respectively, whereas the other phone without SIM card can obtain an emergency IP-CAN session. Four phone models, including Samsung Galaxy S8/S10/S21 and Google Pixel 3/5, are tested. The SDR-based UE is tested to communicate with those two phones through each of those three different IP-CAN sessions based on their corresponding IP addresses. The tested communication is based on the ICMP echo request/reply and the TCP three-way handshake.

Table 3.4 summarizes the result for all the five tested carriers. We have two observations. First, the M2I communication based on the emergency IP-CAN is forbidden for all the tested carriers. Second, all the carriers allow the emergency IP-CAN to have the M2M communication, but the allowable cases vary with the carriers. Specifically, the US-III allows the communication for all the three different cases, as shown in Figure 3.13, whereas US-I permits only the emergency-to-emergency (E2E) communication; US-II permits two communication types, namely E2E and emergency-to-data-service (E2D); TW-I and TW-II allow E2E and emergency-to-IMS-signaling (E2IMS). In sum, all the tested carriers have improper access control on the emergency IP-CAN session.

Root cause and lessons. The root cause of this vulnerability is a lack of an access control mechanism on the emergency IP-CAN session in the standards, so it can be attributed to a design defect.

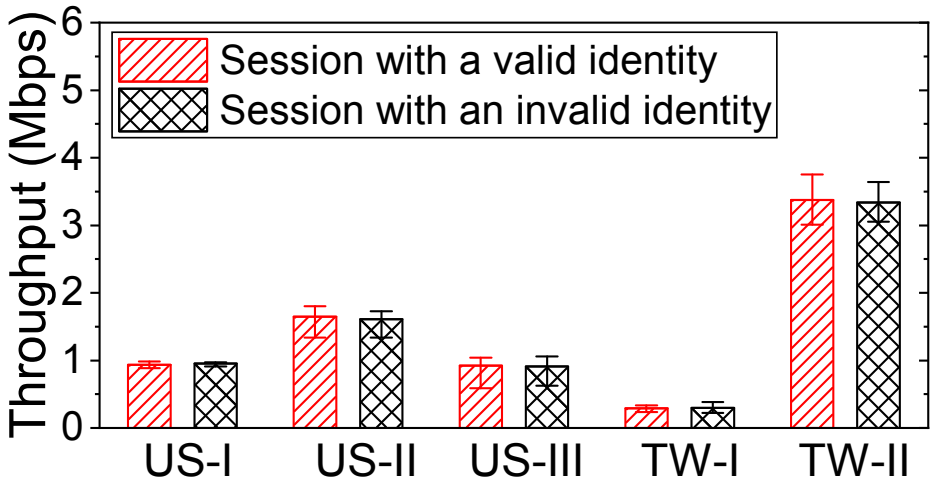
At the first glance, designing the access control mechanism is straightforward, since the only requirement is to install the PCC rules that can restrict the emergency IP-CAN to the IMS server only. Specifically, during the emergency IP-CAN session establishment, the MMF or the UPG should provide the PCF with the IMS server information and then the PCF produces the corresponding PCC rules for the installation.

However, the real situation is much more complex; the IMS server may not be always determined during the emergency IP-CAN session establishment. The IMS server can be also assigned based on the DNS (Domain Name Service) or DHCP (Dynamic Host Configuration Protocol) services after the UE obtains the emergency IP-CAN [13]. In this case, the PCC rules cannot be produced and installed until the IMS emergency registration proceeds; during the registration, the IMS server needs to notify the PCF after receiving the UE's SIP Register message [1]. But, the adversary is allowed to skip the registration and bypass this notification. Thus, installing the PCC rules for the access control should be designed to be independent of the emergency registration.

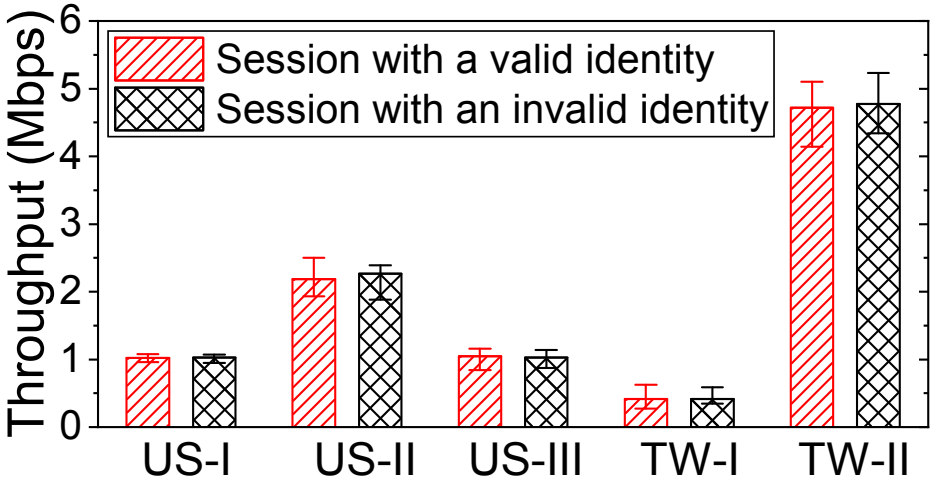
3.5.3: Vulnerability 6: One-size-fits-all Prioritization for Emergency IP-CAN Sessions

To ensure the quality of cellular emergency services, the infrastructure is designed to prioritize emergency IP-CAN sessions according to the 3GPP standard [28]. However, this does not imply that all the requested emergency sessions shall be prioritized indiscriminately; specifically, the emergency sessions requested by invalid UE IDs (i.e., IMEIs), which can escape from tracking, are not handled differently from those with valid IDs. Such the one-size-fits-all prioritization approach may be exploited by the adversary to grab prioritized resource by abusing emergency services with invalid IDs. Notably, a valid IMEI is composed of three parts: (1) Type Allocaiton Code (TAC), a unique 8-digit code assigned by GSMA to identify the device model and manufacturer; (2) Serial Number (SNR), a 6-digit code assigned by the device manufacturer to identify each equipment within the TAC area; (3) Check Digit (CD), a single digit used to avoid manual transmission errors [11]. The TAC and the SNR form a globally unique ID for being identified.

Experimental Validation. We validate this vulnerability for the five tested carriers by checking whether the emergency IP-CAN session requested by an invalid IMEI can be built successfully and then receive the network resource comparable to that requested by a valid IMEI. This experiment consists of three steps. First, we generate an invalid IMEI (i.e., 300000000000000) and confirm its invalidity using many online IMEI checkers [68, 69], including those provided by carriers [70, 103]. Second, an SDR-based UE is employed to establish an emergency IP-CAN session using the generated invalid IMEI and a valid IMEI, respectively. Third, we measure the uplink/downlink throughput of those two different emergency IP-CAN sessions using IPerf with 10 runs each.



(a) Uplink Throughput



(b) Downlink Throughput

Figure 3.14: The 25th/50th/75th percentiles of uplink and downlink throughput on emergency IP-CAN sessions with valid/invalid user identity.

Figure 3.14 shows the throughput statistics for those two kinds of emergency sessions from each of the five tested carriers. We observe that for each carrier, all the emergency IP-CAN sessions have comparable uplink and downlink throughput performance. For instance, in the US-II network, the median uplink/downlink throughput for the emergency IP-CAN sessions with the invalid IMEI is 1.61 Mbps/2.26 Mbps, which is similar to 1.65 Mbps/2.19 Mbps obtained from the emergency IP-CAN sessions with a valid IMEI. These results confirm that the network infrastructure fails to differentiate the priority of the emergency sessions with valid and invalid IMEIs; no noticeable restrictions are imposed on those with invalid UE IDs.

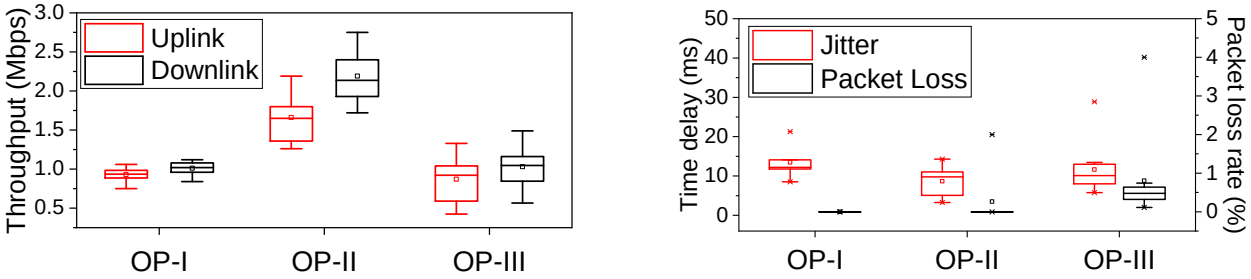
Root Cause and Lessons. The vulnerability in question may have its root in the regulation of the local regulatory authority, which aims to maximize the availability of cellular emergency services. For instance, the FCC mandates that cellular carriers must forward all the wireless 911 calls to the PSAP regardless of call validation results [84]. Consequently, it seems reasonable to prioritize emergency IP-CAN sessions with the one-size-fits-all method. However, on second thought, it may not be the case due to two primary reasons: (1) it is uncommon for benign mobile users to access emergency services using invalid IMEIs; and (2) the local regulatory authority does not prevent carriers from imposing some restrictions on suspicious or malicious emergency sessions. We thus believe that it is critical to develop a new prioritization mechanism for emergency services, thereby being able to strike a balance between their availability and security.

3.5.4: Proof-of-concept Attacks

We devise three proof-of-concept attacks, namely free data/voice/text services, data DoS/over-charge, and remote scanning, using the vulnerabilities V3 and V4. The cost of these attacks is to have an SDR platform compatible with 4G/5G networks; it serves as a M2I gateway that provides the free services over an emergency IP-CAN session, and an attack UE for the first and last two attacks, respectively. We next elaborate on the details of each attack.

Free data/voice/text service attack. The adversary can exploit the E2E communication, the delivered data of which are free of charge, to obtain free data/voice/text service. To achieve it, an M2I gateway needs to be deployed to forward data between the UE with an emergency IP-CAN

Figure 3.15: Exploiting the E2E communication to enable free data service using a Mobile-to-Internet gateway.



(a) Throughput.

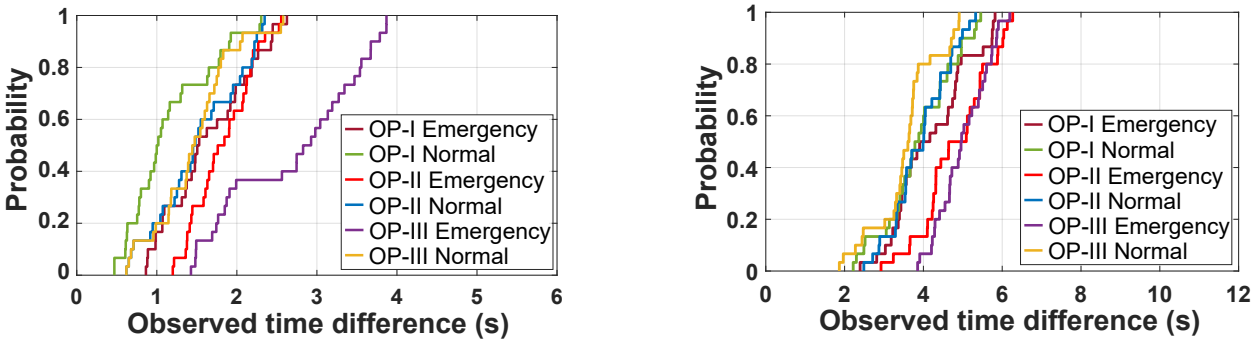
(b) Packet loss rate and jitter.

Figure 3.16: The min/med/max and 25th/75th percentiles of throughput, jitter, and packet loss rate for the data service over the emergency communication channel.

session and the Internet, as shown in Figure 3.15. At the gateway, the SDR UE connects to the cellular infrastructure using an emergency IP-CAN session and receives/transmits all data to/from the other UEs through the free E2E communication, the Wi-Fi router connects to the Internet, and the computer forwards data between the SDR UE and the router.

We next evaluate the data service over that free-of-charge communication channel in all the three carrier networks. We use IPerf to assess its throughput, jitter, and packet loss rate with 20 runs each. As shown in Figure 3.16, the median values of the uplink and downlink throughput range from 0.83 Mbps to 2.17 Mbps, all the jitter values are smaller than 30 ms, and all the packet loss rates are smaller than 1%. Note that the measured throughput is constrained by the SDR-based UE, which supports only a single antenna [26] with the current srsRAN version (20.10), so the adversary may increase the throughput using more advanced UEs in this attack.

We further use Google Voice over the free-of-charge channel to have voice and text services at no cost [104]. We assess the voice and text services by considering the call setup time and the text delivery time, respectively. Figure 3.17 plots the CDF results by comparing the attack with normal cases, where the UE with a valid mobile service subscription uses the Google voice. It is seen that



(a) Call setup time

(b) Text delivery time

Figure 3.17: The CDF results of the call setup and text delivery times observed in the emergency attacks and normal cases.

this attack can offer comparable performance to normal cases. Specifically, they have the ranges of the call setup time, 0.86s∼3.87s and 0.47s∼2.58s, respectively, whereas those of the text delivery time are 2.39s∼6.27s and 1.87s∼5.46s, respectively.

Data DoS/overcharge attack. The adversary can further use the E2D communication to launch a data DoS/overcharge attack against cellular users. The spamming data can be generated from the attack UE's emergency interface at no cost and sent to a victim UE's data interface, thereby consuming the data quota of the victim's data service plan. It can cause the victim UE to suffer from an overcharged bill or the data DoS, where its subscribed data quota is exhausted. In particular, massive cellular IoT devices (e.g., water and electricity meters) are more vulnerable to this attack, since they usually have only a small amount of data quota with high unit rates (e.g., $0.99 per MB) in common IoT service plans. The prerequisite of this attack is to obtain the IP addresses of potential victim UEs. To target cellular IoT devices in this attack, the adversary can remotely identify their IP addresses by probing them based on the operation of the cellular IoT power saving mechanism (PSM) [105]. The adversary can also attack specific UEs and steal the information of their IP addresses by installing the malware or launching phishing attacks.

We validate the feasibility of this DoS/overcharge attack for both OP-II and OP-III using four different victim UEs, including Samsung Galaxy S8 and S10, Google Pixel 3 and 5. Each validation test consists of the following three steps. First, we obtain the latest data usage amount three days after powering off the victim UE. Second, after powering on the victim UE, we use the attack UE to

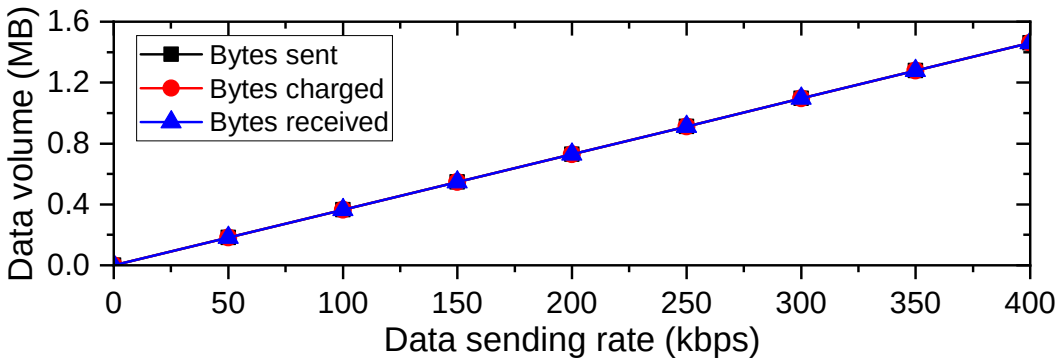


Figure 3.18: The volume of spamming data which are sent, received, and charged from the data DoS/overcharge attack against a victim device in the OP-III network.

send spamming data from its emergency interface to the victim UE's data interface. The spamming packets are the UDP datagrams created by the attack UE using a randomly selected UDP destination port number and the victim UE's IP address. The victim UE may reply ICMP Port Unreachable error message to the attack UE. Third, we power off the victim UE and keep it for three days; afterwards, we query the latest data usage amount again.

We show the evaluation result of OP-III only, since the attack becomes unavailable for OP-II during the evaluation experiment[2]. In the experiment, we vary spamming rates from 50 Kbps to 400 Kbps and for each test, the spamming attack lasts for 30 s. Figure 3.18 shows the volume of spamming data which are sent, received, and charged in the OP-III network. It can be seen that the victim is charged for all the spamming data.

Remote scanning attack The E2D communication also allows the adversary to scan victim UEs remotely for vulnerability discovery while bypassing cellular network firewalls. Specifically, the adversary can send probing packets (e.g., TCP SYN) to various port numbers of the victim UEs, and then determine which ports are open and which services are running at each victim UE based on the responses (e.g., TCP SYN+ACK or ICMP Port Unreachable) corresponding to the probing packets. The collected information of each UE is then used to query the CVE (Common Vulnerabilities and

[2]This attack was successfully validated for OP-II in August 2021, but it became unavailable later in December 2021 when a comprehensive attack experiment was conducted. The observed difference between these two experiment times is that the IP addresses assigned to non-emergency IP-CAN sessions change from IPv6-based to IPv4-based, whereas those of emergency IP-CAN sessions are still IPv6-based. Such changes in the network configuration/infrastructure could be the reason why the E2D communication over V4 becomes unavailable in the OP-II network.

No.	Service ID	Service Application	Protocol	Port	Reported CVE
1	saphostctrl	AirDrop - File Share For Android	TCP	1128	CVE-2019-9832
2	lm-x	Opera Mini Browser		6200	CVE-2021-23253
3	ultraseek-http	AirDroid - File Transfer&Share		8765	CVE-2019-9599
4	amcs	Sand Studio -Screen mirroring		8766	CVE-2015-5661
5	http	ES - File Explorer, File Manager		59777	CVE-2019-6447
6	upnp	UPnP Simple Service Discovery	UDP	1900	CVE-2021-27239
7	bfd-control	Bidirectional Forwarding Detection		3784	CVE-2021-28496
8	zeroconf	Multicast DNS (mDNS)		5353	CVE-2017-6519
9	oma-ulp	OMA User Plane Location		7275	CVE-2016-10416
10	unknown	Eques Smart Door Control		27341	CVE-2019-15745

Table 3.5: The result of the remote scanning attack against a Samsung S8 in the OP-III network; only the services and ports with reported CVE are listed.

Exposures) database to examine whether the UE has any potential security vulnerabilities.

We validate this attack by using Nmap, which is an open-source utility for network discovery and security auditing, to send the probing packets from the attack UE's emergency interface to the victim UE's data interface. This validation test is conducted in OP-II and OP-III, both of which allow the E2D communication, with three victim UEs, including Samsung S8, Pixel 5, and iPhone 13. We discover that to scan 5,000 ports, the attack UE needs to send and receive around 322.8 KB and 306.1 KB, respectively, and it takes around 13 s. Table 3.5 summarizes the scanning result obtained from S8 in OP-III with a list of services and ports associated with reported CVE vulnerabilities.

3.6: Countermeasures

All the discovered vulnerabilities, except for the vulnerability V6, root in design defects of the cellular emergency services stipulated in the 3GPP/GSMA standards. However, addressing them based on their root causes to have a secure design may not be practical in the short term, since the required design changes lie in some core network functions and even security functions of billions of UEs. It cannot be achieved without significant effort or a long time. In the following, we first present long-term secure designs that can address the vulnerabilities, together with their expected overhead, and then introduce four short-term, yet low-overhead, remedies that can mitigate those vulnerabilities.

3.6.1: Long-term Security Designs

We present the design change required for those five vulnerabilities rooted in the design defects of cellular emergency service standards below.

V1 (unverifiable emergency IP-CAN session requests). It calls for a device-level authentication mechanism, which can make differences on emergency IP-CAN session requests from different UEs, even when the UEs do not have SIM cards. It requires each UE to have device credentials (e.g., certificates), but it is not easy to upgrade each UE to get and install a carrier-certified certificate since the process requires the device owner to be involved but not an automatic upgrade with a software patch due to security concerns.

V2 (inconsistent emergency IP-CAN session support). Resolving such inconsistencies requires collaborative efforts from 3GPP and GSMA to align their specifications for supporting emergency services so that the network carriers and device manufactures can adhere to the same requirement. However, it requires a closer coordination and communication between 3GPP and GSMA to identify all inconsistent specifications, design solutions for dealing with the differences, and update all the relevant documents including testing specifications.

V3 (improper cross-layer security binding). The cross-layer security binding between the establishment of IPSec security association and the IMS registration shall be decoupled. However, such design change could incur a large overhead, since the general IMS operation for both emergency and non-emergency services needs to be modified; specifically, the derivation of the IPSec security context needs to be removed from the IMS registration procedure.

V4 (non-atomic cellular emergency service initialization). The three steps in the cellular emergency service initialization need to be combined into an atomic operation. Specifically, the request of the emergency IP-CAN session establishment piggybacks the requests of both IMS emergency registration and session establishment procedures. Once this combined request arrives at the core network, the corresponding emergency call attempt can reach the IMS server so that the emergency IP-CAN session cannot be hijacked without raising awareness from the IMS. However, handling that combined request requires modifications on the MMF, the UPG, and the IMS server, which

cannot be done in a short time.

V5 (improper access control on emergency IP-CAN sessions). The MMF or the UPG shall provide the PCF with the IP address of the IMS server assigned to each emergency UE so that the PCF can install a proper access control rule that can restrict the emergency IP-CAN session to the IMS server only. However, the assignment of the IMS server can be done through the DHCP or DNS service, after the establishment of the emergency IP-CAN session [13]; there could still exist a window period when the emergency IP-CAN session is not restricted and may be abused. Thus, the IMS server assignment shall be executed during the emergency IP-CAN session establishment. However, this proposed design can incur a large overhead due to the required support of multiple core network functions, e.g., MMF, UPG, PCF, and IMS server.

3.6.2: Short-term Remedies

In this section, we propose a suite of standard-compliant remedies, which can reduce attack incentives or mitigate attack damage, instead of fully addressing the vulnerabilities.

(1) Restricted resource on duplicate/suspicious emergency IP-CAN session (for V1 and V6). Simply rejecting each duplicate emergency session request or each emergency session request with an invalid UE ID is seemingly an effective solution to address V1 and V6, respectively, but the duplicate/suspious ones may be sent by benign UEs in some rare but still possible scenarios. For example, while a user is having an emergency call, the smartphone may be accidentally rebooted due to some unexpected software/hardware errors [38, 57]; this accidental event does not allow the smartphone to perform the detach procedure of the emergency IP-CAN session and the session is not released, so when the user dials an emergency call again after the smartphone reboots, a duplicate emergency session request can be generated. Moreover, benign users may purchase used phones whose IMEIs were modified by previous owners to invalid ones for some reasons.

As a result, this simple-rejection method may hurt the availability of the emergency service for benign UEs. In order to not only defend against the DoCES attack but also keep the service high availability, we propose to accept duplicate/suspicious emergency session requests but restrict their session capability; the existing emergency sessions that are duplicated will be kept.

Specifically, the duplicate/suspicious emergency IP-CAN sessions are restricted to only the access of basic IMS emergency services (e.g., 31 Kbps for voice calls with the basic audio codec [6]), but not allowed to access video calls or voice calls with high audio quality codecs. Even though duplicate/suspicious emergency sessions are established by the adversary, the resources available to be abused are limited, since these duplicate/suspicious emergency sessions are granted only the minimum resource supporting the basic IMS emergency service; the attack incentive can be thus greatly reduced. On the other hand, when the duplicate/suspicious ones are created by benign UEs, they are still available to offer the emergency services.

(2) Enabling CS Emergency Services Timely (for V2). When inconsistent capabilities between UEs and the 5G/4G infrastructure cannot be fully addressed, we propose that the infrastructure should guide the UEs to use the CS-based emergency services supported by itself or other nearby networks. It can provide the UEs with a 3GPP-stipulated EMM error code EPS services not allowed [21], thereby preventing them from getting stuck in a network that cannot provide them with IMS-based emergency services. Moreover, to prevent unnecessary CS fallback switches, the infrastructure should only trigger the switch when receiving the emergency IP-CAN session request with the same service option twice; it implies that the requested UE insists on the requested service options.

Enabling TLS protection over IMS emergency session (for V3). The vulnerability V3 can be addressed by enabling the ciphering and integrity protection over IMS emergency sessions. However, emergency UEs may not have credentials to do IMS emergency service registration and then establish IPSec security associations with their IMS servers. We then propose a standard-compliant method that an emergency UE establishes a TLS session with its IMS server using only the server's certificate prior to the IMS emergency service registration [9]. The TLS session can protect the IMS signaling messages with ciphering and integrity, thereby preventing fabricated SIP messages. Notably, this approach does not require significant support from carriers, since it was originally stipulated by the cellular network standards [9] to be used as an optional security mechanism to improve the security of IMS service access.

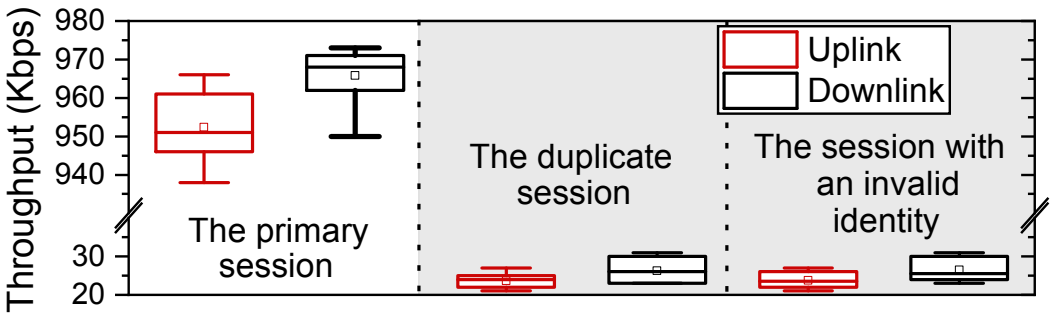


Figure 3.19: Short-term remedy evaluation for (1) restricted resource on duplicate/suspicious emergency IP-CAN sessions.

(4) Delay authorization of emergency IP-CAN session (for V4 and V5). To address vulnerabilities V4 and V5, we propose to delay authorization of each emergency IP-CAN session. The initial IP-CAN session obtained from the emergency IP-CAN session establishment for a UE is deemed as a temporarily-authorized session, the availability of which is only authorized for a short time period (e.g., 3 s); moreover, the bandwidth of this temporarily-authorized session is also limited to a small value (e.g., 31 Kbps). Its permanent authorization is delayed until the IMS server assigned to the UE receives SIP messages from the UE, and then determined by the IMS server. If no anomaly happens, the IMS server authorizes the session permanently by instructing the PCF to remove the session's time constraint and install proper PCC rules to restrict the IP-CAN session to the IMS server only. With this mechanism, even though the adversary may abuse the IP-CAN session during the initial, temporarily-authorized time period, their incentive can be largely decreased by that short abuse time. Notably, not all UPGs understand the IMS-related messages, so the permanent authorization of the emergency IP-CAN session cannot be done at the UPG during its establishment procedure.

3.6.3: Prototype and Evaluation

We prototype and evaluate the above four standard-compliant remedies. To emulate the cellular emergency service architecture, we use srsRAN (v20.1) [97], Open IMS Core [86], and LinPhone Voice client [46] to serve as the 4G LTE infrastructure, the IMS core with an IMS server, and the Voice over IMS app, respectively.

• **Restricted resource on duplicate/suspicious emergency IP-CAN sessions.** We upgrade srsRAN

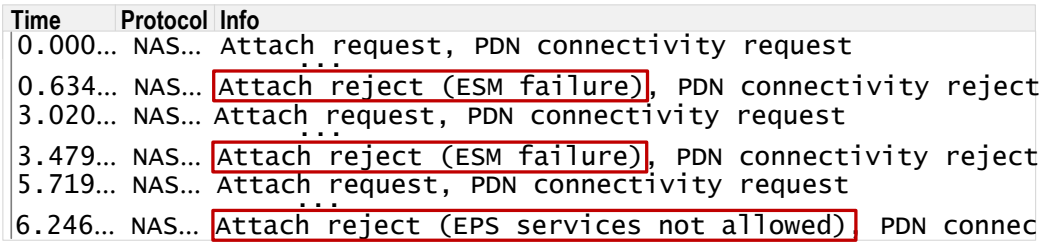


Figure 3.20: Short-term remedy evaluation for (2) enabling CS fallback switches

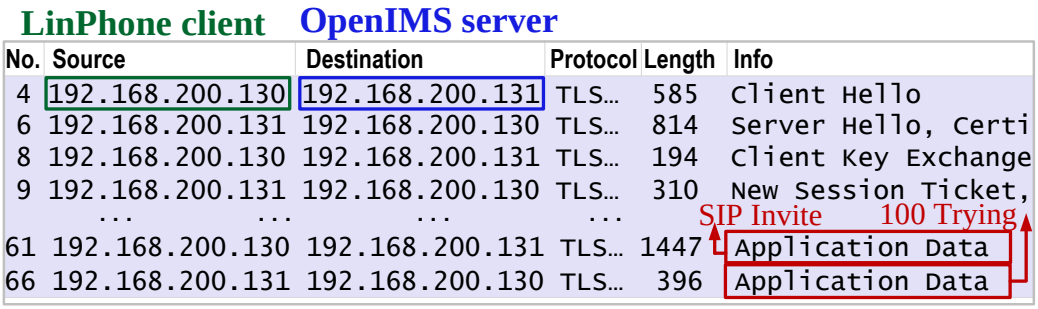


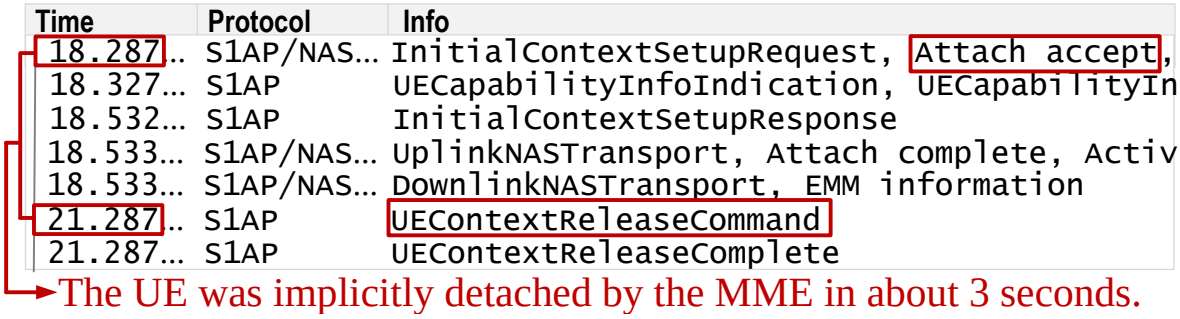
Figure 3.21: Short-term remedy evaluation for (3) enabling TLS-protected IMS emergency sessions.

to support the emergency IP-CAN session establishment and modify the PCF to limit the maximum throughput of duplicate emergency IP-CAN sessions and the ones with invalid user identities to 31 Kbps. In the experiment, three types of emergency IP-CAN sessions are evaluated, namely the primary (first) session, the secondary (duplicate) session, and the session with an invalid IMEI, on the testbed in terms of throughput performance. Figure 3.19 plots the throughput result obtained from 10 experiment runs. It is observed that the maximum throughputs of the secondary and invalid-IMEI emergency IP-CAN sessions are limited to 31 Kbps, whereas that of the primary one is as high as 973 Kbps. Together with the proposed delay authorization method, this remedy can largely decrease adversaries' incentives.

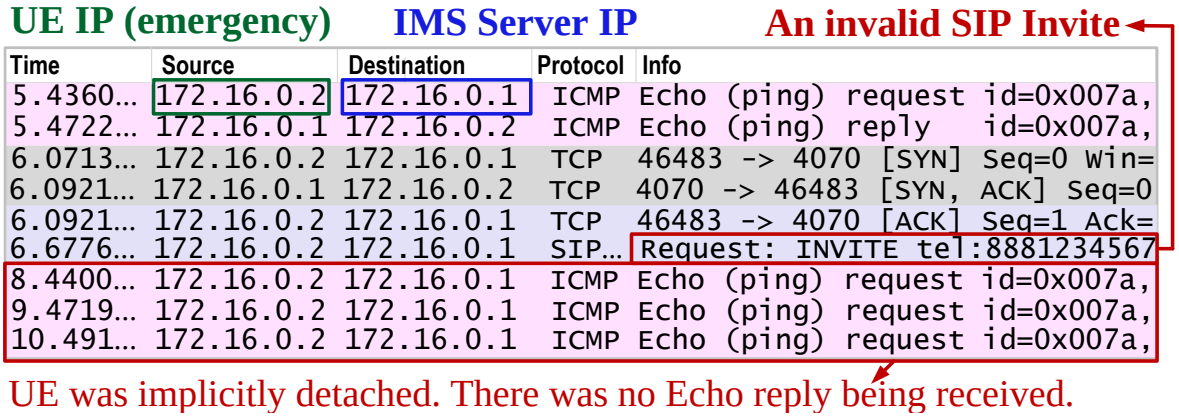
• **Enabling CS Emergency Services Timely.** We modify the emergency IP-CAN session establishment procedure in srsRAN. Specifically, when a UE attempts to establish an emergency IP-CAN session and its requested service option is not supported by the network, the network rejects the request with the EMM error cause of the ESM failure for the first two attempts. The ESM failure is to notify the UE that there is a failure in the emergency session management and it needs to change

the requested service option. However, if the UE insists on using the option that is not supported by the network, on the third attempt, the network rejects the emergency UE's request with the EMM cause of the EPS services not allowed and then guides the UE to switch to a 2G/3G network for accessing CS-based emergency services, as shown in Figure 3.20. This can prevent the UE blocking attacks, where attackers exploit unsupported service options and cause the victim's emergency IP-CAN session establishment to fail.

• **Enabling TLS protection over IMS emergency session.** We enable the TLS support on the OpenIMS server and LinPhone Voice client. As illustrated in Figure 3.21, all the SIP messages of the emergency call establishment are protected by the established TLS session between the client and the server. It can thus prevent the DoCES attack, which relies on the SIP messages sent in plaintext.



(a) MME implicitly detaches UE.



(b) Dialing a non-emergency call.

Figure 3.22: UE is implicitly detached by MME when no valid IMS emergency session is established within 3 seconds.

• **Delay authorization of emergency IP-CAN session.** We modify the PCF server to restrict the

access of the emergency IP-CAN sessions with specified PCC rules at the UPG. For the delay authorization mechanism, a 3 s timer is set for each emergency IP-CAN session right after it is established. By default, after 3 s, it will be terminated by the UPG and its PCC rules will be removed; the Delete Bearer Request message [8] is sent to the MMF for the termination. For normal emergency service requests, the IMS server can receive a valid SIP INVITE message for the emergency IP-CAN session within that 3 s; then, it will authorize the emergency IP-CAN session by sending the AAR (Authentication Authorization Request) message [1] to the PCF through the standardized Rx interface [1].

We evaluate this remedy for the UE in three tested scenarios: (1) transmitting nothing to the infrastructure, (2) transmitting an invalid SIP INVITE message with a non-emergency phone number to the IMS server, and (3) transmitting a valid SIP INVITE message using urn:service:sos as the recipient's number to the IMS server. As shown in Figure 3.22, the UE will be implicitly detached by the infrastructure if no valid SIP INVITE message is received within 3 s after its emergency IP-CAN session is established. The result shows that the adversary cannot keep the emergency IP-CAN session being alive for a long time without a valid IMS emergency session.

3.7: Discussion

Launching attacks from COTS UEs? Some attacks (e.g., data DoS/spamming/free attacks) can be launched from COTS UEs, but they need to be finished within a short time period, because the UEs can be switched to the legacy 3G network, where the attacks are not allowed, after they fail to communicate with the IMS emergency service server. We have developed a tool on the COTS UEs to intercept all the SIP messages and reply to some critical messages so that any emergency calls will not be sent to PSAPs after an emergency IP-CAN session is established. However, the tool can only delay the fallback switch without avoiding it. Notably, completely preventing the fallback requires to compromise the UEs' modems or finds COTS UEs supporting 4G/5G network services only.

Potential DoS attacks. The emergency IP-CAN sessions have higher priority than the non-emergency ones, so the adversary can exploit the vulnerability V1 (unverifiable requests) to estab-

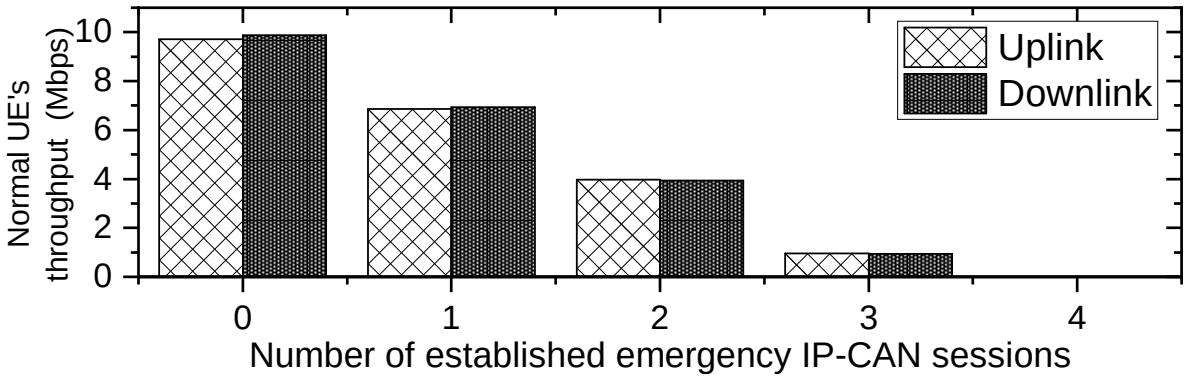


Figure 3.23: The median throughput values of the victim UE vary with number of emergency IP-CAN sessions in a cell.

lish multiple concurrent emergency sessions and generate as many packets as possible to exhaust a cell's limited radio resource, thereby causing a cell DoS attack where non-emergency UEs have no available bandwidth for network services. Due to the ethical reason, this DoS attack cannot be assessed in operational networks. We then evaluate it using our srsRAN testbed with SDR-based UEs and 4G LTE infrastructure. On the testbed, we set the maximum bandwidth value to 3 Mbps, which is the maximum uplink/downlink bandwidth observed in the tested carrier networks.

In the attack evaluation, we build multiple concurrent emergency IP-CAN sessions using ZeroMQ [108] and generate as much uplink traffic as possible from each session, while measuring the uplink/downlink throughput of a victim UE connecting to the same 4G network. We vary the number of concurrent emergency sessions from 0 to 4 and have 10 runs for each experimental setting. As shown in Figure 3.23, the uplink/downlink throughput values of the victim UE decrease with the increasing number of the emergency sessions; they reach 0 Mbps when there are 4 concurrent emergency sessions. This result confirms the feasibility of this attack.

However, the proposed short-term remedy, delay authorization of emergency IP-CAN session, can defend against this attack. It not only allows initial emergency sessions to be temporarily authorized for only a short time period (e.g., 3 s), but also limits the bandwidth of those temporarily-authorized sessions (e.g., 31 Kbps). Therefore, without thousands of emergency sessions being established within that short time period, a LTE cell with more than 100 Mbps bandwidth cannot be saturated; launching this DoS attack becomes almost impossible.

Applicability of vulnerabilities/attacks in 5G networks. We consider that the discovered vulnerabilities V2, V3, and V4, as well as their corresponding attacks, may still exist in 5G networks, according to an analysis of the related 3GPP/GSMA standards [13, 17–19, 23, 28]; however, V1 is not applicable to 5G networks, as described in Section 3.4.1. We elaborate on each vulnerability below. The V2 allows anonymous emergency UEs to establish IMS emergency sessions without doing IMS registration; it is a design issue of the IMS system. As the 4G network, the 5G cellular emergency service is supported by the IMS [13], so the V2 can also happen in 5G networks. The V3 stems from a design defect that the 4G MME does not know whether the 4G UE with an emergency IP-CAN session indeed establishes an IMS emergency session with PSAPs. We discover that this defective operation still exists in 5G networks. Specifically, the 5G AMF (Access and Mobility Management Function) [17] serving the similar role as the 4G MME is responsible for the emergency IP-CAN session establishment, but no interfaces are introduced for the communication between the AMF and the IMS emergency server; the AMF has no way of knowing any IMS emergency session establishment, so the V3 can be still applicable to 5G networks. For the V4, the PCF in 4G networks does not have information about the IMS emergency service server assigned to each emergency UE, so it cannot restrict the access of the UE's emergency IP-CAN session to the server only. According to the 5G standard [19], the PCF is still not given any information about the IMS emergency server. Thus, the V4 can be applied to 5G networks.

3.8: Summary

This chapter presents our research on enhancing emergency services (9-1-1) security over mobile networks, given the emergency services serve as a critical lifeline for individuals in urgent situations and mobile networks offer mobile users with ubiquitous emergency services. For emergency uses, anonymous UEs are usually allowed to access cellular emergency services, according to regulatory authority requirements. However, such emergency support increases the attack surface of cellular networks. It leads us to discover six security vulnerabilities and exploit them to develop several attacks including free data service, data DoS, and DoCES. All of the vulnerabilities root in either cellular design defects or commonly observed operational slips, which happen because some

conventional non-emergency functions and services are directly applied to the emergency service operation without being carefully reviewed from security aspects. We have experimentally validated the vulnerabilities and attacks with three representative U.S carriers and two major Taiwan carriers, and shown that both carriers and mobile users may suffer from the attacks. We finally propose short-term remedies and evaluate their feasibility, but the ultimate solution still requires a concerted effort from the standard community, carriers, and device vendors.

Studying emergency service security, such as whether attackers can block a victim's emergency services or take advantage of service carriers during emergency communications, is critically important. However, it also raises a further question. In real-world scenarios, there are various types of emergencies that can occur under heterogeneous network conditions. How to systematically examine more emergency service designs to ensure their reliability, including service accessibility and resilience, is highly needed and even more challenging. This is what we will investigate in the next chapter.

CHAPTER 4: IMPROVING THE ACCESSIBILITY AND RESILIENCE OF EMERGENCY SERVICES (9-1-1)

4.1: Overview

In this chapter, we propose a more systematic approach to improving the reliability of emergency services[3]. Specifically, ensuring they remain accessible and resilient under heterogeneous network environment.

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 [84] 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 [15, 17, 28] allows User Equipment (UE) to access emergency services

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 [58, 78, 79, 106, 109] 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.

[3]This chapter is based on previously published work by Yiwen Hu, Min-Yue Chen, Haitian Yan, Chuan-Yi Cheng, Guan-Hua Tu, Chi-Yu Li, Tian Xie, Chunyi Peng, Li Xiao, and Jiliang Tang, titled "Uncovering Problematic Designs Hindering Ubiquitous Cellular Emergency Services Access " published at the Proceedings of the 30th Annual International Conference on Mobile Computing and Networking (MobiCom 2024). DOI: 10.1145/3636534.3690704 [63].

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 identify 11 such defects, summarized in Table 4.2 (§4.5), categorized into problematic network selection for initiating emergency calls (§4.6), emergency-unaware 9-1-1 call operation (§4.7), and network escalation forbidden during emergency calls (§4.8). 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 chapter 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.

4.2: Cellular Emergency Service Primer

Heterogeneous Cellular Architecture Supporting Emergency Services. Figure 4.1 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,

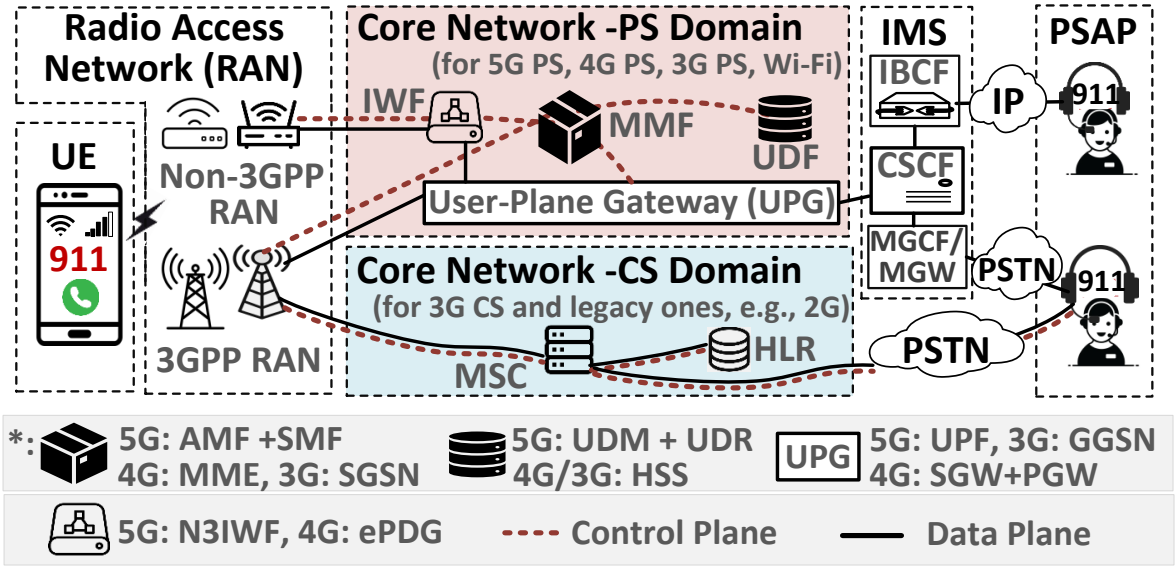


Figure 4.1: Cellular emergency service architecture.

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.

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) [21, 23] manages user mobility, authentication, and session connectivity, including emergency IP connectivity. The User Data Function (UDF) [10, 31] stores user and service subscription information to assist the MMF in user authentication. The Inter-working Function (IWF) [16, 18] 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) [20] 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 net-

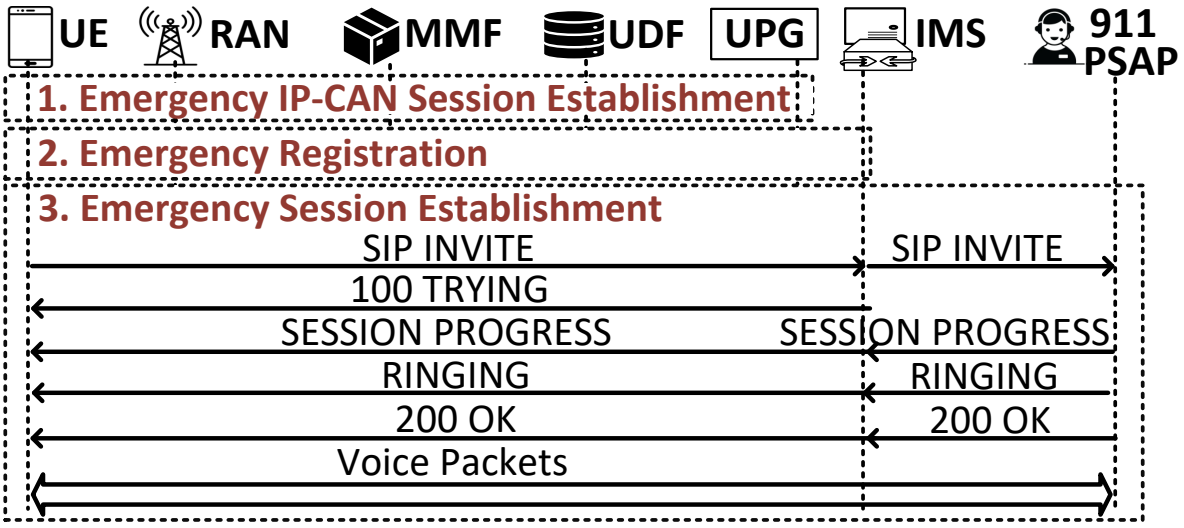


Figure 4.2: Emergency service flow.

work 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) [93]. 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 [15, 17, 20] from both home and visited PLMNs [15, 17], and Wi-Fi networks from the home PLMN. Figure 4.2 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* and authentication with the IMS server [13,28]; (3) *establishing an IMS emergency session* with the PSAP [13, 28, 52, 53]. 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 [30].

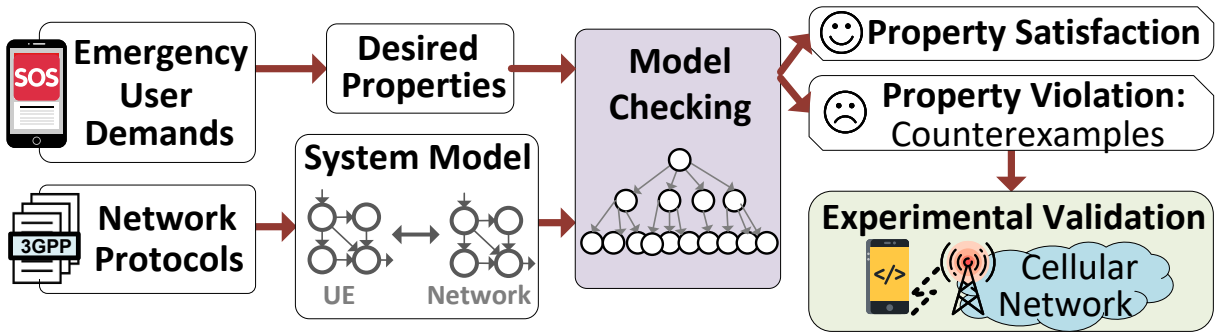


Figure 4.3: The overview of M911-Verifier.

4.3: 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.

4.3.1: Overview of M911-Verifier

Figure 4.3 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 [25, 33, 36], PS/CS services [20,21,23], mobility [15–18,21,23], and emergency services [20,28], in adherence

to the 3GPP standard. Specifically, each protocol (e.g., EPS Mobility Management (EMM)/EPS Session Management (ESM) [21]) 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 [59, 83], which typically use a constant loss rate (e.g., 50%), our approach correlates transmission loss with signal strength, establishing an inverse proportional relationship. As 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 [21] 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$\rightarrow$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.

4.3.2: Challenges and Our Approaches

The model checking technique has gained popularity in recent years for systematically examining cellular network protocols [42, 60, 64, 65, 73, 102]. 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 [84]. 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 [25, 33, 36]. 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. [64] 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. [42] and Cremers et al. [47] conducted a formal analysis of the 5G authentication and key agreement protocol. Additionally, Klischies et al. [73] 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.

4.3.3: Implementation and Evaluation

We implement two major components for M911-Verifier using Python and SPIN [59], a widely used model-checking tool for network protocol verification [92, 94, 102]: 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 [96].

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 [60]. 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

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 3GPP standard [29].
‡: Refer to Dual Radio Voice Call Continuity (DRVCC) design in 3GPP standard [14].

Table 4.1: Summary of non-stationary emergency service use scenarios observed on M911-Verifier.

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 4.1. 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 4.4, 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.

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

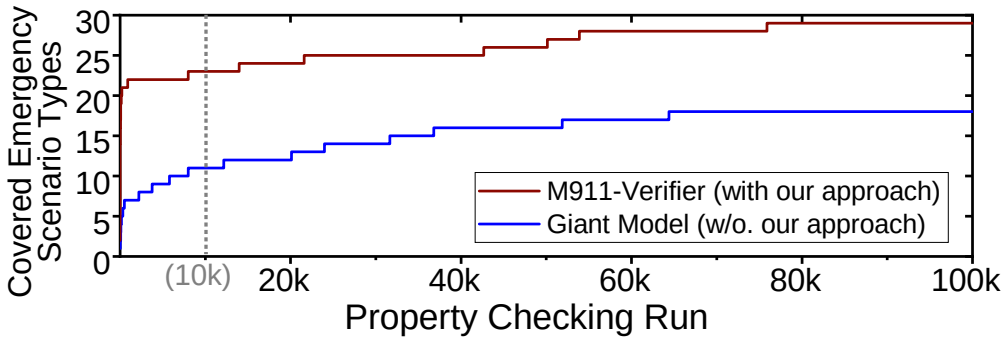


Figure 4.4: Number of emergency use scenarios increases with property checking runs.

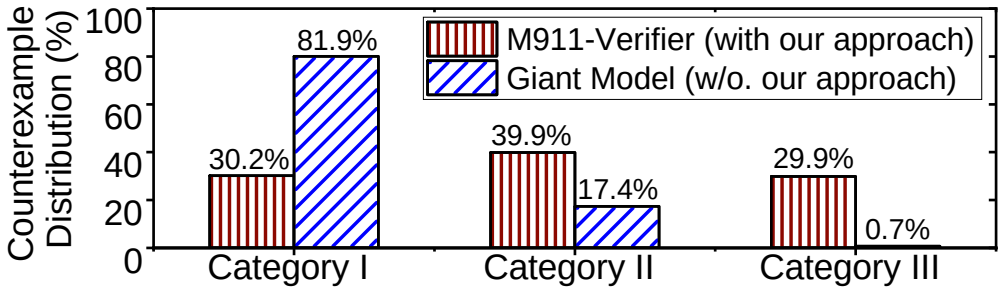


Figure 4.5: Counterexample distributions for each category of UE status at termination of property checking.

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 4.5 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. 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 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 others (Details in §4.5).

4.4: 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 op-

erational 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[4], 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 [20], thereby bypassing Emerg-Call-Blocker's SIP-based call signaling interception. To address this, we employ Cellular Pro [37], 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

[4]The applications developed in this chapter, including Emerg-Call-Blocker and Emerg-Call-Dialer, can be downloaded from [39].

using Optical Character Recognition (OCR) [80], 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[5]**.** 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.

4.5: 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 4.2. Notably, Table 4.2 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 net-

[5]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	Validated?
Problematic Network Selection for Initiating Emergency Calls (§4.6)	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 [16, 17] 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 [28] 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 [12], 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 [17] 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 [28] prohibits UEs without a security context from accessing emergency services via non-3GPP RAN.	○
Emergency-unaware 9-1-1 Call Operation (§4.7)	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 [67], not all Wi-Fi signalings can indicate the emergency usage, leaving service providers unaware of emergency services.	○
Network Escalation Forbidden During Emergency Calls (§4.8)	NF-1	An emergency call drops when the emergency UE moves from a 4G cell to 5G a cell.	φ_2	The 3GPP standard [18] 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 [28] 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 as they share the same standards with non-emergency ones.
×: No validation results due to ethical issues.

Table 4.2: Summary of findings identified by M911-Verifier.

work 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 Limited_Session_Establishment property. For NS-4 and NS-5, both violating Availablity_Guaranteed property, the initiation of emergency calls may be rejected due to the prior improper session termination, and anonymous UEs cannot initiate emergency services through non-3GPP RANs due to the absence of security context, respectively.

Emergency-unaware 9-1-1 Call Operation. This category contains counterexamples from design defects violating Availability_Guaranteed property, which can result in some emergency-unaware operations for initiating emergency services. These counterexamples can cause emergency service requests to be rejected by the network, leading to unnecessary delays up to several minutes. EU-1 and EU-3 present 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 §4.6; EU-1 and EU-2 in §4.7; and NF-1 and NF-2 in §4.8.

4.6: 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 [4, 12, 16–18, 24,

29,32,35] 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.

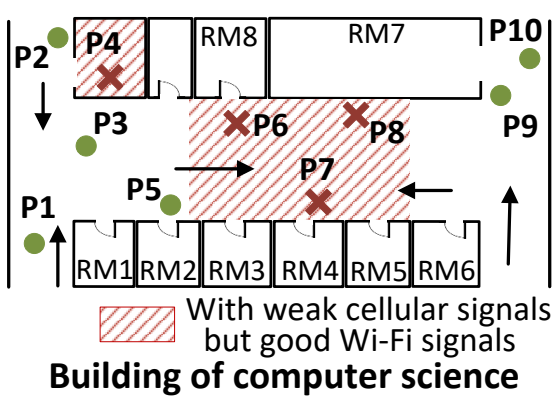
In the following, we present the identified issues from two major network selection scenarios: (1) problematic UE restriction on network selection among 3GPP and non-3GPP radio access networks within the same PLMN; and (2) unfair UE limitation on network selection across home PLMN and visited PLMN. The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

4.6.1: Inferior to Non-Emergency Calls - Restrictions within PLMN

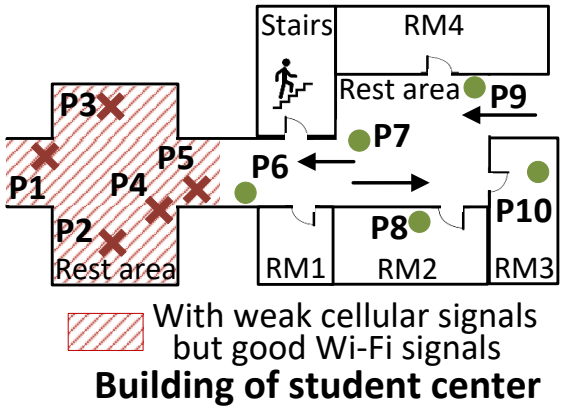
Cellular emergency calls can be made through both 3GPP and non-3GPP RANs. Logically, even when a UE has poor connectivity to 3GPP RANs, emergency call setup times may not be prolonged if there is strong connectivity from non-3GPP RANs (e.g., Wi-Fi). However, 3GPP standards [16, 17] prohibit UEs from 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 [33] spent before switching to another RAN.

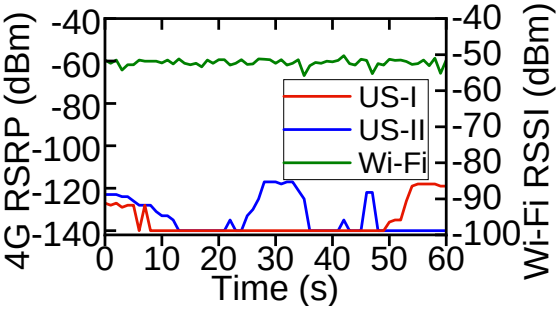
This problematic restriction, "3GPP-always-preferred", leads M911-Verifier to discover counterexamples that violate two major properties, namely Applicable_Access_Guaranteed and Limited_Session_Establishment. All the violations occur when UEs connect to 3GPP RANs with poor or near-deadzone signal strength.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



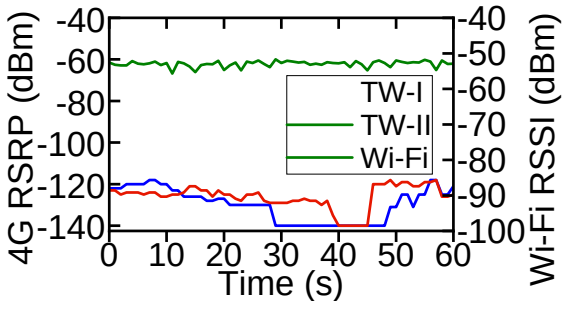
(a) U.S. exp. locations.



(b) Taiwan exp. locations.



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



(d) RSRP/RSSI at location P4 (TW).

Figure 4.6: Experiments were conducted for restrictions within PLMN in the U.S. and Taiwan.

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.

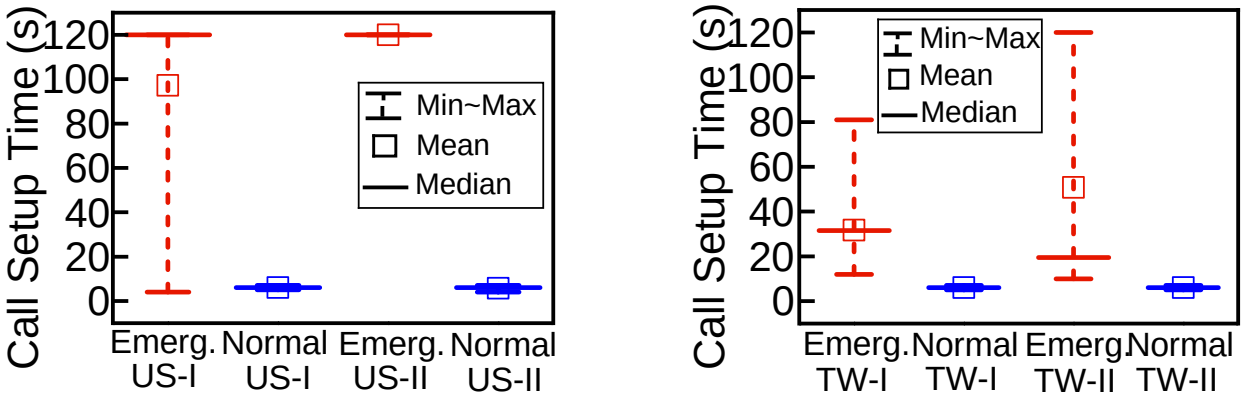
◇ **Selecting Nonexistent RANs.** Another observation is that UEs may attempt to initiate emer-

gency 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 [28]. 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 [4, 21], 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.

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 4.6a and 4.6b, 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



(a) Under US-I/US-II

(b) Under TW-I/TW-II

Figure 4.7: 3GPP-Always-Preferred design results in minutes of emergency call setup delay in US-I, US-II, TW-I, and TW-II.

(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 4.6a and 4.6b, the emergency call setup times for UEs were significantly longer than those for non-emergency calls. For example, at location P7 in Figure 4.6a, 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 4.7. 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 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 4.7b. 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

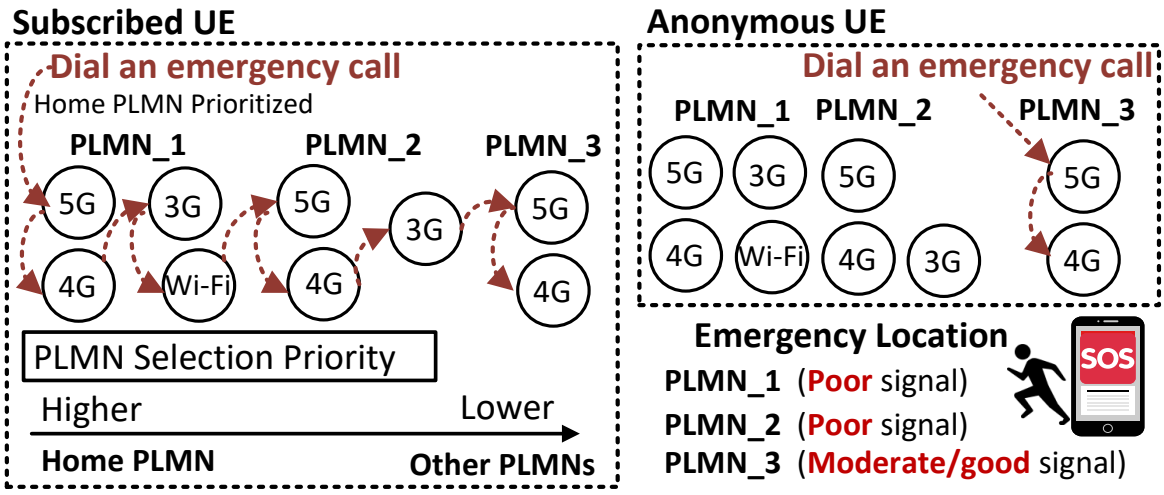
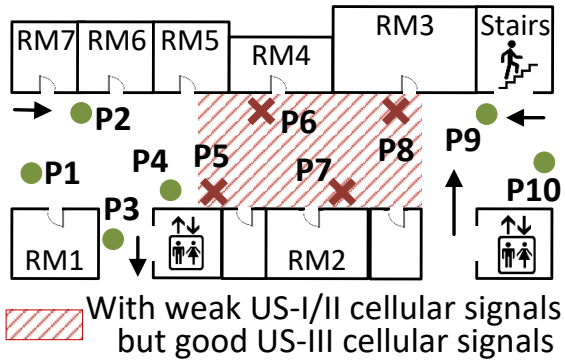


Figure 4.8: Subscribed UE prioritizes its home PLMN for dialing an emergency call, whereas anonymous UE does not.

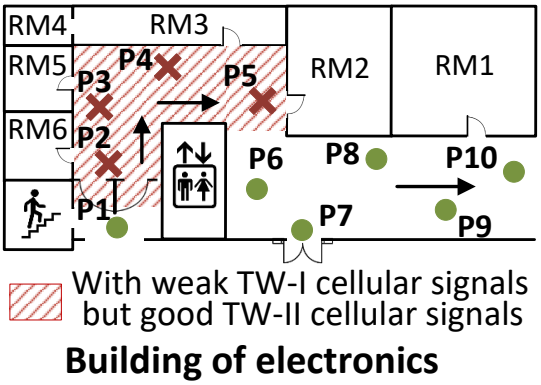
US-II did not support the combined EPS/IMSI attach procedure. In the validation experiment, we observed this issue occurring in US-I. During the initial attachment, the UE received an acceptance message from the 4G network, which also indicated attachment to a 3G network. After the UE's first emergency 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 [21], 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.

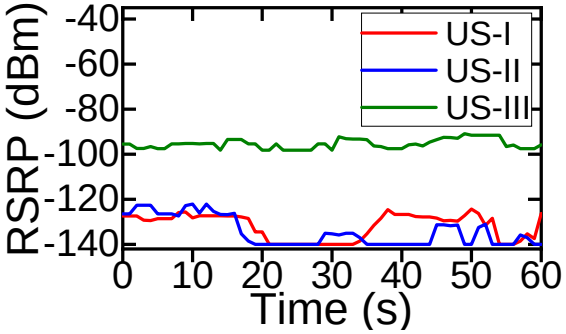
Root Cause and Lessons Learned. The design principle of 3GPP-always-preferred for emergency services is not made without rationale. According to the 3GPP standard [3,15,17], 3GPP RANs and networks not only guarantee transmission bitrates for the delivery of emergency services but also prioritize them over non-emergency ones. This ensures emergency service quality, especially in case of network congestion. However, this design principle may unexpectedly cause negative real-



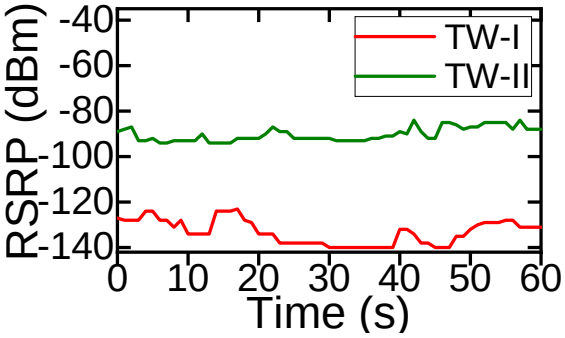
(a) U.S. exp. locations.



(b) Taiwan exp. locations.



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



(d) RSRP at location P3 (TW).

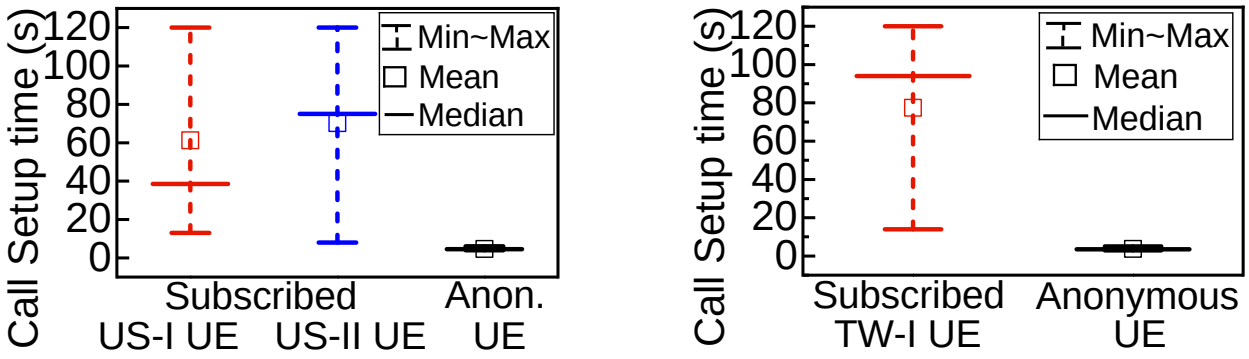
Figure 4.9: Experiments were conducted for limitation across PLMNs in the U.S. and Taiwan.

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.

4.6.2: 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 [12], while also being allowed to access emergency services from all available PLMNs. This may incur a large overhead for UEs, as illustrated in Figure 4.8. 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



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

(b) Users of TW-I

Figure 4.10: Subscribed UEs suffer longer emergency call setup times compared to anonymous UEs.

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 §4.6.1. 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 4.9 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 4.10, subscribed UEs experienced significantly longer emergency call setup times compared to anonymous UEs. Specifically, setup times were 61.3, 70.2, 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

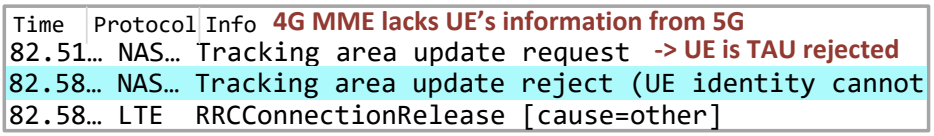
PLMNs for accessing mobile services since connecting to visited PLMNs can incur roaming service fees. However, this reasoning does not apply to emergency services, as they are critical and provided free-of-charge according to the GSMA standard [54]. Therefore, subscribed UEs should not be restricted but should be allowed, like anonymous UEs, to select the best PLMN to guarantee the quality of emergency services.

4.7: Emergency-unaware 9-1-1 Call Operation

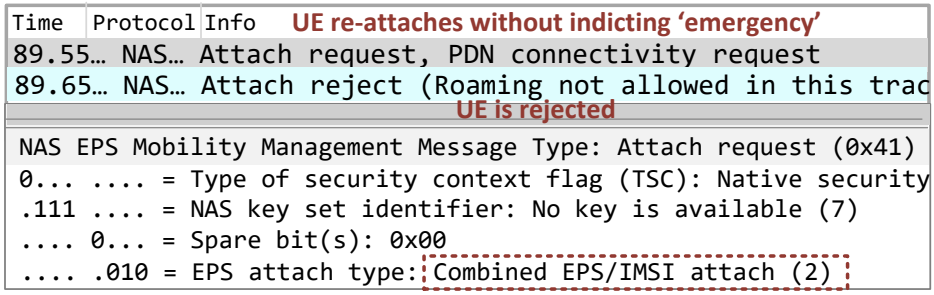
All cellular operations need to be aware of signaling messages from emergency services so that they can be prioritized and handled differently from non-emergency services (e.g., call validation is skipped for emergency services [84]). When some operations are imprudently designed to be unaware of emergency 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 [18] 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.

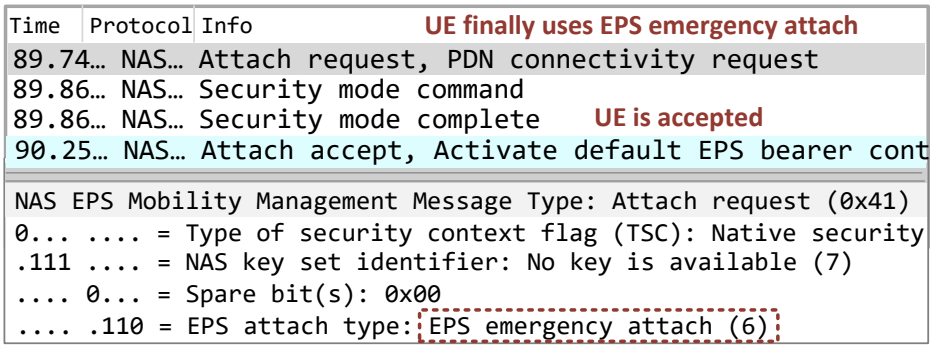
The failure of UE-initiated fallback for emergency services can occur due to the loss of the Handover Command message from the 5G MMF to the UE, typically caused by weak signals or the expiration of inter-system coordination [36]. If the UE does not receive the handover message, it proceeds with a mobility 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 [21], which is not prioritized, to the 4G network for emergency services.



(a) Tracking Area Update without the "emergency" indication



(b) Attach without the "emergency" indication



(c) Re-Attach with the "emergency" indication

Figure 4.11: Emergency service fallback from 5G to 4G without network coordination includes three messages, where only the last Re-Attach message has the "emergency" indication.

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 4.11 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 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 [21], 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 [45]), 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 [34]. These requests are transmitted via NAS 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 [33] and S1AP [34], respectively. The RRC and S1AP headers include a field indicating RRC establishment cause, such as emergency or mobile-originated signaling. However, the NAS protocol [21] does not consider the RRC establishment cause in S1AP messages [21] for prioritizing emergency-related requests. Thus, there is a need for an explicit emergency indication in all emergency-related requests to make related procedures emergency-aware.

4.8: Network-Escalation Forbidden During Emergency Calls

Emergency UEs may experience mobility while engaged in emergency calls. Like non-emergency UEs, the 3GPP standard [15,18,29] 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 [18]; and (2) from 2G/3G

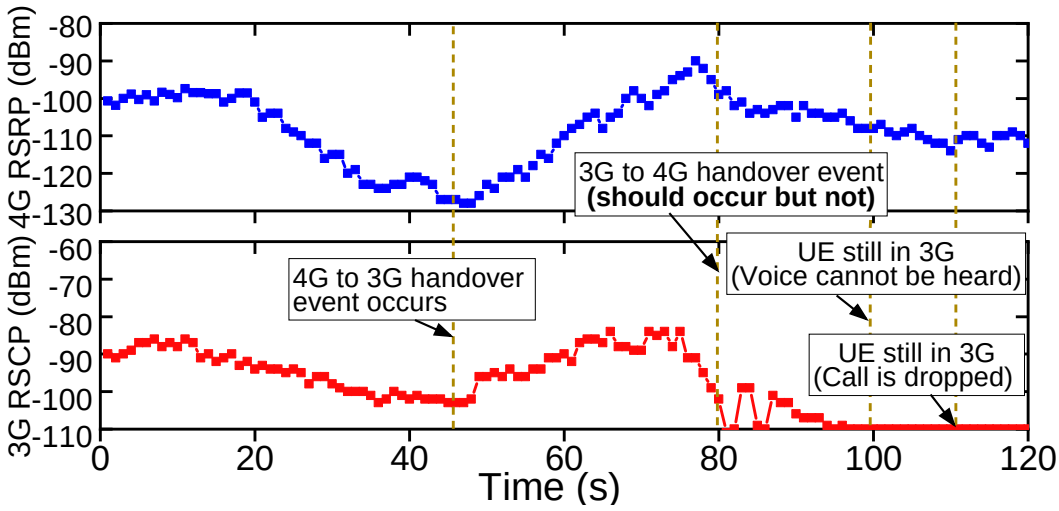


Figure 4.12: A call dropped due to forbidden 3G→4G handover.

with CS-based call service to 4G/5G with PS-based call service [29]. 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 4.12. 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.

4.9: 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

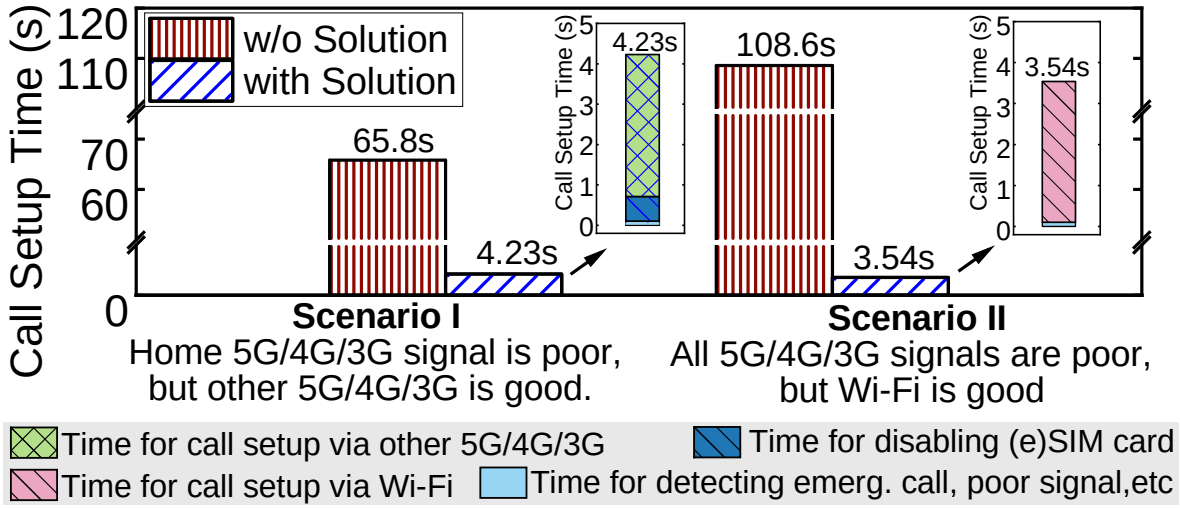


Figure 4.13: Call setup time vary with/w.o. solutions.

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.

4.9.1: 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 [39] 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.).

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 §4.6. The emergency call setup time was measured with and without our solution, with 10 runs per device. The results are illustrated in Figure 4.13.

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 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 MMF. Second, the MMF was modified to prioritize these NAS messages. 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 its effectiveness, we measured how quickly a COTS phone (Pixel 5) re-initiates an emergency attachment after receiving "Tracking area not allowed" or "UE identity cannot be derived by the network" errors (see §4.7). We conducted 10 tests for each error. Results show after receiving the"Tracking area not allowed," the UE entered a limited service state and began an emergency attachment in about 0.17s. Conversely, with another error, the UE continued a normal attachment without entering the limited state.

4.9.2: 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 [9]. 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.

4.10: 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 [39] 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.

4.11: Summary

This chapter presents a systematic methdology to study emergency service designs and improve the emergency service reliability (i.e., maintaining service accessibility and resilience) under any heterogeneous network conditions, as long as wireless coverage exists. 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.

With the continuous advancement of cellular networks—from 4G to 5G, and even toward future generations like 6G—emergency services are also steadily improving. For example, driven by the requirements of regulatory authorities and standard organizations, next-generation emergency services will soon be introduced with enhanced capabilities. These include multimedia support such as emergency video calls, broader access through technologies like direct-to-cell satellite communications, and expanded scenarios such as autonomous driving and mobile health. In the next chapter, we will conclude our current work and discuss new research opportunities.

CHAPTER 5: CONCLUSION AND FUTURE WORK

In this chapter, we conclude our current work and then discuss new research opportunities on innovating and securing next-generation emergency services and other related research areas.

5.1: Conclusion

Mobile networks are indispensable to modern life, delivering essential services such as voice, text, data access, and life-saving emergency communications. They also power mobile applications in areas like financial management and healthcare monitoring, and support advancements in vehicle-to-everything (V2X) communications. Given these critical and widespread use cases, enhancing the reliability and security of mobile infrastructure is of paramount importance. Any disruption or misuse of mobile services can significantly affect users' daily lives and work, pose life-threatening risks (e.g., targeting emergency services), or lead to substantial financial losses for carriers and their partners. This dissertation presents several notable contributions toward powering the infrastructure for critical services, ensuring secure and reliable emergency communications over cellular networks.

For the security and reliability of emergency services, mobile networks such as 4G, 5G, and Wi-Fi are mandated by standards organizations (e.g., 3GPP, GSMA) and regulators (e.g., FCC) to ensure ubiquitous, free, and high-priority emergency access. While well-intentioned, these requirements significantly increase the complexity of mobile network design and implementation, potentially introducing new security risks. Existing research has largely focused on vulnerabilities at the user equipment (UE) level, leaving the security of the supporting network infrastructure largely unexamined. Furthermore, ethical constraints severely limit access to operational emergency infrastructure, making real-world validation and analysis particularly challenging. We pioneered new research methodologies for studying critical 9-1-1 emergency access. To discover flaws, we

built an emergency-specific model-checking framework for efficient analysis across standards. For real-world verification, we developed tools that safely test operational carrier networks without disrupting emergency services, moving beyond prior simulation-based studies. These tools are open-sourced to promote broader research engagement. We not only conducted fundamental research but also applied the resulting insights to address real-world problems. We discovered vulnerabilities and leveraged them to develop proof-of-concept attacks including denial of emergency access and emergency session hijacking. We validate them across real-world mobile infrastructure in the U.S. and Taiwan. Moreover, we discovered that even without attacking scenarios and in locations with sufficient wireless signal coverage, the users may still experience prolonged emergency call setup time, call initiation failures, and call drops due to the design defects in mobile standards. Our findings and solutions have been reported to major carriers, vendors (Samsung, Google, Motorola), and global standards organizations to enhance user and network security.

In the following, I will briefly summarize the research work contained in this dissertation and discuss my future research plans:

Enhancing the Security of Emergency Services (9-1-1) The availability of emergency services is a foundational requirement for public safety, and mobile networks play a central role in maximizing access to emergency services. To meet this goal, standardization organizations such as 3GPP and GSMA, along with regulators like the FCC, mandate that mobile networks provide emergency access to all users including those without subscriptions, free of charge and with higher priority than non-emergency service. However, these design choices, while well-intentioned, can open the back door to new security vulnerabilities. Because emergency services are closely integrated with general mobile infrastructure, any weakness in their design and implementation may lead not only to the denial of life-saving communications but also to broader impacts on the mobile ecosystem. In this work, I led a team to identify six security vulnerabilities in emergency services across the three top-tier U.S. 5G/4G mobile networks: (V1) unverifiable emergency IP-CAN (IP Connectivity Access Network) session requests, (V2) Inconsistent Emergency IP-CAN Session Support, (V3) improper cross-layer security binding, (V4) non-atomic cellular emergency service initialization, (V5) im-

proper access control on emergency IP-CAN sessions, and (V6) One-size-fits-all Prioritization for Emergency IP-CAN Sessions. To demonstrate the real-world implications of these vulnerabilities, we developed two proof-of-concept attacks. The first attack, denial of cellular emergency service (DoCES), allows the adversary to prevent mobile users from accessing emergency services, using only two SDR (Software-defined Radio) platforms serving as an attack UE and a sniffer. This attack includes four variants, namely UE blocking, UE detaching, call cancel, and call drop, targeting different call phases to deny users' emergency services. The second attack hijacks emergency sessions to gain unauthorized access to high-priority network resources, enabling abuses such as obtaining free data/voice/text access from critical emergency network resources, launching data overcharging, and remote service scanning attacks towards non-emergency services IoT users. We have experimentally validated the vulnerabilities and attacks with three representative U.S carriers and two major Taiwan carriers, and shown that both carriers and mobile users may suffer from the attacks. We finally propose short-term remedies and evaluate their feasibility, but the ultimate solution still requires a concerted effort from the standard community, carriers, and device vendors.

Improving the Reliability of Emergency Services (9-1-1) Emergency services are critical lifelines, and both regulators and standards bodies (e.g., 3GPP) have mandated wide accessibility through various radio access technologies (5G/4G/Wi-Fi), network generations (5G/4G/3G), and public land mobile networks (PLMNs) such as AT&T and Verizon. However, this broad support introduces complex protocol interactions that are difficult to validate and prone to errors. Moreover, accessing to operational emergency infrastructures for experimental validation is heavily restricted, due to ethical concerns, making real-world analysis challenging. To address this, we developed M911-Verifier, an emergency-specific verification framework that integrates model checking to systematically diagnose 3GPP emergency service protocols. Model checking explores all possible system states to detect violations of expected behavior, but is often hindered by scalability issues. Our framework mitigates this by dynamically loading and analyzing protocol procedures, enabling effective exploration across diverse mobile generations and technologies. Using M911-Verifier, we identified eleven previously unknown issues in emergency call handling. These include long call

setup times (up to 2 minutes in our testing), call initiation failures, and call drops, even in areas with adequate signal coverage. For example, we found that in some indoor locations, 90% of emergency calls cannot be established within two minutes due to flawed network selection mechanisms, while non-emergency calls at the same locations can be completed in five seconds. We experimentally validated these findings across three major U.S. carriers and two in Taiwan. To ensure no disruption to public safety, we built Emerg-Call-Blocker, a smartphone-based tool that prevents calls from reaching PSAPs during experimental testing. Most of the discovered issues have been validated on operational cellular networks in the U.S. and Taiwan in a responsible manner. For disclosure, we have engaged with carriers and standards organizations to report the identified design flaws, propose solutions, and support ongoing efforts to strengthen emergency call reliability.

In conclusion, cellular networks provide mobile users with ubiquitous access to emergency services. To meet regulatory requirements, anonymous user equipment (UEs) are typically permitted to access these services. However, this support for emergency access introduces significant complexity into system design and expands the attack surface of cellular networks. In this dissertation, we proposed and developed systematic framework to explore the emergency service standard design by combining model checking technologies, we have identified multiple security vulnerabilities and design flaws that not only enable the development of serious attacks but also threaten the reliability of emergency communications. These issues primarily stem from the direct application of non-emergency procedures and services to emergency scenarios without proper review. We have experimentally validated these findings across five carrier networks. To mitigate the identified vulnerabilities, we propose a set of recommended solutions, though their successful deployment will require coordinated efforts from standards bodies, carriers, and device manufacturers.

5.2: Future Work

Mobile networks (5G, 6G, and beyond), with ultra-fast speeds, millisecond-level latency, and ubiquitous coverage, are supposed to become the most indispensable component in future life. They also provide a broader platform for transformative technologies like trustworthy AI and large-scale

machine learning, enabling more powerful applications in autonomous driving, healthcare, and industrial automation. These advancements promise to make our work and lives more intelligent and convenient. However, integrating them into mobile systems is complex, presenting new challenges and creating new attack surfaces that may threaten the security and privacy of both users and infrastructure. Below, I outline three future research directions on building Intelligent and Secure Mobile Networks.

◇**Innovating and Securing Next-Generation Emergency Services (NG-9-1-1).** Regulatory authorities (e.g., FCC) and standards organizations (e.g., 3GPP, GSMA) are speeding up the transition to next-generation emergency services, enhancing communications through voice, text, video, images, and multimedia through multiple access networks such as 5G and beyond, Wi-Fi, and satellite. NG-9-1-1 also demands closer coordination between devices and networks for faster responses and accurate location tracking. Transitioning to the next generation is far from straightforward, requiring design innovation, systematic examination, and thorough testing over mobile networks to enhance system reliability and security.

Studying emergency services is challenging due to the complexity of standard protocols and the difficulty of experimental validation, which can raise ethical concerns and disrupt critical services. In my previous research, we developed a model-checking framework to uncover design flaws in existing emergency standards, validated responsibly within carrier networks. To further innovate and secure the next generation of services, my plan includes three tasks: (1) Enhance the existing framework by integrating large language models (LLMs) for intelligent standard analysis. Given the vast and scattered nature of emergency service standards, LLMs can improve efficiency. However, applying open-source LLMs to standard documents is not trivial, as unique cellular-specific challenges need to be addressed. For example, specialized terminology in cellular standards makes alignment with high-level regulatory language difficult. (2) Develop an experimental platform to responsibly validate discovered issues, with a particular focus on integrating satellite access into the testing platform for emergency services. Satellite emergency service access is a new and underexplored area which requires careful reviews and tests from a security perspective. (3) Propose

more intelligent applications, such as automatic emergency detection and accurate localization for people with disabilities, and advance emergency service management in open radio access networks (O-RAN) for faster service scheduling and anomaly detection. I believe that by leveraging my expertise in mobile network standards and collaborating with researchers in AI/NLP, we can propose innovative methodologies to address technical challenges. For the identified flaws that impede the accessibility, reliability, and security of next-generation emergency services, we can utilize cross-disciplinary technologies to resolve them.

◇**Safeguarding 5G and Beyond V2X (Vehicle-to-Everything) Communications.** Given the ubiquitous coverage of mobile networks, V2X communication is a key enabler for the future of autonomous driving. It facilitates timely signaling transmission among vehicles and with traffic elements, such as traffic lights and roadside signs. Many insightful papers on autonomous driving security have been published in prestigious AI, security, and mobile conferences/journals, with generous funding from organizations such as NSF. However, existing research studies primarily focus on enhancing autonomous driving from the vehicle's perspective. For instance, some studies introduce noise using lasers or other light sources that interfere with vehicle sensor cameras, misleading AI systems into misclassifying stop signs or speed limits.

Despite this progress, the reliability and security of V2X communication remain largely unexplored. Compared to conventional mobile services, V2X communication operates in more complex and constantly changing network environments due to mobility. Attackers may have greater opportunities to exploit vulnerabilities in standard mobility designs such as the authentication and security key derivation involving different radio access networks and mobile generations, to compromise V2X communication. This could enable them to send duplicated or outdated signaling messages or replace benign messages with malicious ones. Such attacks could lead to erroneous AI decisions regarding routing schedules or collision avoidance. Therefore, there is a critical need to conduct research on V2X communication protocols.

◇**Exploring Ultra Reliable Low Latency Communication for Mobile Health (mHealth).** 5G mobile networks introduce the ultra-reliable low latency communication (URLLC) technology for

providing time-bound data delivery (less than 1 millisecond) and 99.999% reliability. Healthcare is one of its major use cases for remote diagnosis and surgery, medical IoT Sensors, and virtual reality headsets. Given these applications, URLLC communication between devices and network infrastructures must not only be accessible but also highly secure, ensuring that data is available to authorized medical personnel while preserving confidentiality. There is an urgent need to assess its security design, particularly in areas such as Packet Data Convergence Protocol (PDCP) packet duplication and Low-Density Parity Check Codes (LDPC), which are two other protocols and codes used in 5G architecture to enhance the reliability of URLLC data, for example, whether they are resisted to side-channel attacks. More specifically, whether attackers using sniffing devices could potentially infer sensitive details, such as the type of medical surgery or the surgery phase, by analyzing encrypted communication packets. With the widespread adoption of mobile devices and the ubiquitous access, ultra-fast speed, and extremely low latency provided by 5G networks, mobile health holds strong potential for impactful growth and technological advancement. Consequently, ensuring the security and reliability of mobile health communications becomes essential, presenting many new challenges and research opportunities to explore.

BIBLIOGRAPHY

[1] 3GPP. TS 29.211: Rx Interface and Rx/Gx signalling flows (Release 6), June 2007. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1671.

[2] 3GPP. TS 23.002: Universal Mobile Telecommunications System (UMTS); Network architecture (Release 17), March 2021. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=728.

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

[4] 3GPP. TS 23.272: Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2 (Release 17), Sept. 2021. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=835.

[5] 3GPP. TS 23.380: IMS Restoration Procedures (Release 17), Dec. 2021. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=848.

[6] 3GPP. TS 26.114: IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction (Release 17), Dec. 2021. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1404.

[7] 3GPP. TS 29.212: Policy and Charging Control (PCC); Reference points (Release 17), Sept. 2021. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1672.

[8] 3GPP. TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (Release 17), Dec. 2021. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1692.

[9] 3GPP. TS 33.203: Access security for IP-based services (Release 17), Dec. 2021. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2277.

[10] 3GPP. TS 33.401: 3GPP System Architecture Evolution (SAE); Security architecture (Release 17), Dec. 2021. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296.

[11] 3GPP. TS 23.003: Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification, Sept. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729.

[12] 3GPP. 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), Sept. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=789.

[13] 3GPP. TS 23.228: IP Multimedia Subsystem (IMS); Stage 2 (Release 18), Dec. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=821.

[14] 3GPP. TS 23.237: IP Multimedia Subsystem (IMS) Service Continuity; Stage 2 (Release 17), March 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=826.

[15] 3GPP. TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 18), Dec. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=849.

[16] 3GPP. TS 23.402: Architecture enhancements for non-3GPP accesses (Release 18), Dec. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=850.

[17] 3GPP. TS 23.501: System architecture for the 5G System (5GS) (Release 18), Dec. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144.

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

[19] 3GPP. TS 23.503: Policy and charging control framework for the 5G System (5GS); Stage 2 (Release 18), Dec. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3334.

[20] 3GPP. TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (Release 18), Dec. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1015.

[21] 3GPP. TS 24.301: Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 18), Sept. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1072.

[22] 3GPP. TS 24.302: Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 (Release 17), Sept. 2022. https://portal.3gpp.org/desktopmodules/

Specifications/SpecificationDetails.aspx?specificationId=1073.

[23] 3GPP. TS 24.501: Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (Release 18), Sept. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3370.

[24] 3GPP. TS 25.304: User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode (Release 17), April 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1167.

[25] 3GPP. TS 25.331: Radio Resource Control (RRC); Protocol specification (Release 17), April 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1180.

[26] 3GPP. TS 36.213: Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (Release 17), Jan. 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2427.

[27] 3GPP. TS 22.101: Service aspects; Service principles (Release 17), Jun. 2023.

[28] 3GPP. TS 23.167: IP Multimedia Subsystem (IMS) emergency sessions (Release 18), March 2023. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=799.

[29] 3GPP. TS 23.216: Single Radio Voice Call Continuity (SRVCC); Stage 2 (Release 18), June 2023. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=816.

[30] 3GPP. TS 24.229: IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 18), Jan. 2023. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1055.

[31] 3GPP. TS 33.501: Security architecture and procedures for 5G System (Release 18), Jan. 2023. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169.

[32] 3GPP. TS 36.304: Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode (Release 18), Jan. 2024. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2432.

[33] 3GPP. TS 36.331: Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (Release 18), Jan. 2024. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2440.

[34] 3GPP. TS 36.413: Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP) (Release 18), Jan. 2024. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2446.

[35] 3GPP. TS 38.304: NR; User Equipment (UE) procedures in Idle mode and in RRC Inactive state (Release 18), Jan. 2024. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3192.

[36] 3GPP. TS 38.331: NR; Radio Resource Control (RRC) protocol specification (Release 18), Jan. 2024. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3197.

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

[38] Androidcentral. Shutting and rebooting down during calls, 2015. https://forums.androidcentral.com/moto-x/575325-shutting-rebooting-down-during-calls.html.

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

[40] Nils Aschenbruck, Matthias Frank, and Peter Martini. Present and future challenges concerning dos-attacks against psaps in voip networks. In *Fourth IEEE International Workshop on Information Assurance (IWIA'06)*, pages 6–pp. IEEE, 2006.

[41] ATT. Ways to manage international usage Find out how to keep your charges predictable when traveling abroad.., 2024. https://www.att.com/support/article/wireless/KM1040974/.

[42] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. A formal analysis of 5g authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 1383–1396, New York, NY, USA, 2018. Association for Computing Machinery.

[43] Evangelos Bitsikas and Christina Pöpper. You have been warned: Abusing 5g's warning and emergency systems. In *Proceedings of the 38th Annual Computer Security Applications Conference*, ACSAC '22, page 561–575, New York, NY, USA, 2022. Association for Computing Machinery.

[44] Min-Yue Chen, Yiwen Hu, Guan-Hua Tu, Chi-Yu Li, Sihan Wang, Jingwen Shi, Tian Xie, Ren-Chieh Hsu, Li Xiao, Chunyi Peng, et al. Taming the insecurity of cellular emergency services (9-1-1): From vulnerabilities to secure designs. *IEEE/ACM Transactions on Networking*, 2024.

[45] CISCO. Cisco Mobility Management Entity Overview, 2021. 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.

[46] Belledonne Communications. Linphone - for smartphones, tablets and desktop platforms, 2020. https://www.linphone.org/.

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

[48] Ericsson. Ericsson Mobility Report November 2024., 2024. https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/november-2024.

[49] Christoph Fuchs, Nils Aschenbruck, Felix Leder, and Peter Martini. Detecting voip based dos attacks at the public safety answering point. In *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, pages 148–155, 2008.

[50] Mat Goebel, Christian Dameff, and Jeffrey Tully. Hacking 9-1-1: infrastructure vulnerabilities and attack vectors. *Journal of medical Internet research*, 21(7):e14383, 2019.

[51] GSMA. 5G Implementation Guidelines, July 2019.

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

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

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

[55] GSMA. Shaping the future of mobile connectivity together. Become a GSMA member., 2024. https://www.gsma.com/home/.

[56] Mordechai Guri, Yisroel Mirsky, and Yuval Elovici. 9-1-1 ddos: Attacks, analysis and mitigation. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 218–232, 2017.

[57] Harvey. How to fix a Galaxy S9 that reboots on its own during calls, 2022. https://thedroidguy.com/how-to-fix-a-galaxy-s9-that-reboots-on-its-own-during-calls-1091448.

[58] Ahmad Hassan, Arvind Narayanan, Anlan Zhang, Wei Ye, Ruiyang Zhu, Shuowei Jin, Ja-

son Carpenter, Z. Morley Mao, Feng Qian, and Zhi-Li Zhang. Vivisecting mobility management in 5g cellular networks. In *Proceedings of the ACM SIGCOMM 2022 Conference*, SIGCOMM '22, page 86–100, New York, NY, USA, 2022. Association for Computing Machinery.

[59] G.J. Holzmann. The model checker spin. *IEEE Transactions on Software Engineering*, 23(5):279–295, 1997.

[60] Kaiyu Hou, You Li, Yinbo Yu, Yan Chen, and Hai Zhou. Discovering emergency call pitfalls for cellular networks with formal methods. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '21, page 296–309, New York, NY, USA, 2021. Association for Computing Machinery.

[61] Yiwen Hu, Min-Yue Chen, Guan-Hua Tu, Chi-Yu Li, Sihan Wang, Jingwen Shi, Tian Xie, Li Xiao, Chunyi Peng, Zhaowei Tan, et al. Unveiling the insecurity of operational cellular emergency services (911): Vulnerabilities, attacks, and countermeasures. *GetMobile: Mobile Computing and Communications*, 27(1):39–43, 2023.

[62] 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. Uncovering insecure designs of cellular emergency services (911). In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, MobiCom '22, page 703–715, New York, NY, USA, 2022. Association for Computing Machinery.

[63] Yiwen Hu, Min-Yue Chen, Haitian Yan, Chuan-Yi Cheng, Guan-Hua Tu, Chi-Yu Li, Tian Xie, Chunyi Peng, Li Xiao, and Jiliang Tang. Uncovering problematic designs hindering ubiquitous cellular emergency services access. In *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, pages 1455–1469, 2024.

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

[65] Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino. 5greasoner: A property-directed security and privacy analysis framework for 5g cellular network protocol. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 669–684, New York, NY, USA, 2019. Association for Computing Machinery.

[66] Syed Rafiul Hussain, Imtiaz Karim, Abdullah Al Ishtiaq, Omar Chowdhury, and Elisa Bertino. 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*, CCS '21, page 1082–1099, New York, NY, USA, 2021. Association for Computing Machinery.

[67] IEEE. 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)*, pages 1–3534, 2016.

[68] IMEIcheck.com. IMEI Number Check., 2023. https://imeicheck.com/imei-check.

[69] IMEI.INFO. Check IMEI number to get to know your phone better., 2023. https://www.imei.info/.

[70] imeipro.info. Free US cell phone IMEI checker, 2023. https://www.imeipro.info/att-imei-check.html.

[71] Seung Wook Jung. Captcha-based ddos defense system of call centers against zombie smartphone. *International Journal of Security and Its Applications*, 6(3):29–36, 2012.

[72] Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim. Touching the untouchables: Dynamic security analysis of the lte control plane. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1153–1168, 2019.

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

[74] Gyuhong Lee, Jihoon Lee, Jinsung Lee, Youngbin Im, Max Hollingsworth, Eric Wustrow, Dirk Grunwald, and Sangtae Ha. This is your president speaking: Spoofing alerts in 4g lte networks. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '19, page 404–416, New York, NY, USA, 2019. Association for Computing Machinery.

[75] Seunghyeon Lee, Changhoon Yoon, Heedo Kang, Yeonkeun Kim, Yongdae Kim, Dongsu Han, Sooel Son, and Seungwon Shin. Cybercriminal minds: an investigative study of cryptocurrency abuses in the dark web. In *NDSS*, pages 1–15. Internet Society, 2019.

[76] Chi-Yu Li, Guan-Hua Tu, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu, and Xinbing Wang. Insecurity of voice solution volte in lte mobile networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, page 316–327, New York, NY, USA, 2015. Association for Computing Machinery.

[77] Chi-Yu Li, Guan-Hua Tu, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu, and Xinbing Wang. Insecurity of voice solution volte in lte mobile networks. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 316–327, New York, NY, USA, 2015. ACM.

[78] Yuanjie Li, Haotian Deng, Jiayao Li, Chunyi Peng, and Songwu Lu. Instability in distributed mobility management: Revisiting configuration management in 3g/4g mobile networks. *SIGMETRICS Perform. Eval. Rev.*, 44(1):261–272, jun 2016.

[79] Yuanjie Li, Qianru Li, Zhehui Zhang, Ghufran Baig, Lili Qiu, and Songwu Lu. 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*, SIGCOMM '20, page 344–358, New York, NY, USA, 2020. Association for Computing Machinery.

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

[81] Yisroel Mirsky and Mordechai Guri. Ddos attacks on 9-1-1 emergency services. *IEEE Transactions on Dependable and Secure Computing*, 18(6):2767–2786, 2021.

[82] Yisroel Mirsky and Mordechai Guri. Ddos attacks on 9-1-1 emergency services. *IEEE Transactions on Dependable and Secure Computing*, 18(6):2767–2786, 2021.

[83] Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker, and Michael Deardeuff. How amazon web services uses formal methods. *Communications of the ACM*, 58(4):66–73, 2015.

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

[85] Andreea Ancuta Onofrei, Yacine Rebahi, Thomas Magedanz, Fokus Fraunhofer Institute, et al. Preventing distributed denial-of-service attacks on the ims emergency services support through adaptive firewall pinholing. *International Journal of Next-Generation Networks*, 2010.

[86] OpenIMSCore.org. Welcome to Open IMS Core's Homepage., 2008. http://openimscore.sourceforge.net/.

[87] Yueyang Pan, Ruihan Li, and Chenren Xu. The first 5g-lte comparative study in extreme mobility. *Proc. ACM Meas. Anal. Comput. Syst.*, 6(1), feb 2022.

[88] Chunyi Peng, Chi-yu Li, Guan-Hua Tu, Songwu Lu, and Lixia Zhang. Mobile data charging: New attacks and countermeasures. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, page 195–204, New York, NY, USA, 2012. Association for Computing Machinery.

[89] Chunyi Peng, Chi-yu Li, Guan-Hua Tu, Songwu Lu, and Lixia Zhang. Mobile data charg-

ing: New attacks and countermeasures. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 195–204, New York, NY, USA, 2012. ACM.

[90] Chunyi Peng, Chi-Yu Li, Hongyi Wang, Guan-Hua Tu, and Songwu Lu. Real threats to your data bills: Security loopholes and defenses in mobile data charging. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 727–738, New York, NY, USA, 2014. ACM.

[91] Chunyi Peng, Chi-Yu Li, Hongyi Wang, Guan-Hua Tu, and Songwu Lu. Real threats to your data bills: Security loopholes and defenses in mobile data charging. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, page 727–738, New York, NY, USA, 2014. Association for Computing Machinery.

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

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

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

[95] Manav Seth, Sneha Kumar Kasera, and Robert P Ricci. Emergency service in wi-fi networks without access point association. In *Proceedings of the 1st International Conference on Wireless Technologies for Humanitarian Relief*, pages 411–419, 2011.

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

[97] srsRAN. Get the srsRAN software and documentation., 2022. https://docs.srsran.com/en/latest/index.html.

[98] Budankailu Sameer Kumar Subudhi, Faruk Catal, Nikolay Tcholtchev, Kin Tsun Chiu, Yacine Rebahi, Michell Boerger, and Philipp Lämmel. Performance testing for voip emergency services: a case study of the emynos platform and a reflection on potential blockchain utilisation for ng112 emergency communication. *J. Ubiquitous Syst. Pervasive Networks*, 12(1):1–8, 2020.

[99] Hannes Tschofenig, Henning Schulzrinne, Murugaraj Shanmugam, and Andrew Newton. Protecting first-level responder resources in an ip-based emergency services architecture. In *2007 IEEE International Performance, Computing, and Communications Conference*, pages

626–631. IEEE, 2007.

[100] Zisis Tsiatsikas, Georgios Kambourakis, and Dimitrios Geneiatakis. At your service 24/7 or not? denial of service on esinet systems. In *International Conference on Trust and Privacy in Digital Business*, pages 35–49. Springer, 2021.

[101] G. H. Tu, C. Y. Li, C. Peng, and S. Lu. How voice call technology poses security threats in 4g lte networks. In *2015 IEEE Conference on Communications and Network Security (CNS)*, pages 442–450, Sept 2015.

[102] Guan-Hua Tu, Yuanjie Li, Chunyi Peng, Chi-Yu Li, Hongyi Wang, and Songwu Lu. Control-plane protocol interactions in cellular networks. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, SIGCOMM '14, page 223–234, New York, NY, USA, 2014. Association for Computing Machinery.

[103] Verizon. Tell us about your device., 2023. https://www.verizon.com/sales/byod/devicedetails/imei.html.

[104] Google Voice. Google Voice calling rates, 2022. https://voice.google.com/rates.

[105] Sihan Wang, Guan-Hua Tu, Xinyu Lei, Tian Xie, Chi-Yu Li, Po-Yi Chou, Fucheng Hsieh, Yiwen Hu, Li Xiao, and Chunyi Peng. Insecurity of operational cellular iot service: new vulnerabilities, attacks, and countermeasures. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, pages 437–450, 2021.

[106] Chenren Xu, Jing Wang, Zhiyao Ma, Yihua Cheng, Yunzhe Ni, Wangyang Li, Feng Qian, and Yuanjie Li. A first look at disconnection-centric tcp performance on high-speed railways. *IEEE Journal on Selected Areas in Communications*, 38(12):2723–2733, 2020.

[107] Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. Hiding in plain signal: Physical signal overshadowing attack on {LTE}. In *USENIX Security Symposium (USENIX Security)*, pages 55–72, 2019.

[108] ZeroMQ. ZeroMQ: An open-source universal messaging library, 2022. https://zeromq.org/.

[109] Zhehui Zhang, Yuanjie Li, Qianru Li, Jinghao Zhao, Ghufran Baig, Lili Qiu, and Songwu Lu. Movement-based reliable mobility management for beyond 5g cellular networks. *IEEE/ACM Transactions on Networking*, 31(1):192–207, 2023.