IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 12, 2020, accepted December 7, 2020, date of publication December 16, 2020,
date of current version December 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3045322

On Identifying Threats and Quantifying Cybersecurity Risks of Mnos Deploying Heterogeneous Rats

ANNA ANGELOGIANNI[1], (Graduate Student Member, IEEE), ILIAS POLITIS[1], (Member, IEEE), FARNAZ MOHAMMADI[2], (Student Member, IEEE), AND CHRISTOS XENAKIS[1], (Member, IEEE)

[1]Systems Security Laboratory (SSL), University of Piraeus, 185 34 Piraeus, Greece
[2]Passau Institute of Digital Security, University of Passau, 94032 Passau, Germany

Corresponding author: Anna Angelogianni (angelogianni@unipi.gr)

This work was supported in part by the European Union's Horizon 2020 EU Research & Innovation Program under Grant 833685 (H2020-EU.3.7.4-SPIDER), in part by the European Union's Horizon 2020 Stimulating innovation by means of cross-fertilisation of knowledge program under Grant 823997 (H2020-MSCA-RISE-2018-SECONDO), and in part by the Greek state funded Operational Programme Competitiveness, Entrepreneurship and Innovation 2014–2020 (EPAnEK) under Grant RECENT-$T1E\Delta K-03524$ and Grant CityZen-$T1E\Delta K-02121$.

ABSTRACT Wireless networks constitute a significant attack vector for adversaries due to their wide usage in our everyday life. As the fifth generation of wireless networks reaches maturity, several vulnerabilities affecting earlier generations have been resolved. Nevertheless the coexistence of legacy wireless technologies is giving rise to the risk of allowing adversaries to perform downgrade attacks, thus bypassing the improved security of the state-of-the-art communication networks. Vulnerabilities due to the trade-off between security and usability could also exist in the latest wireless networking technologies; hence mobile network operators need to be aware of the risks related to both protocol vulnerabilities and configuration defects. This paper proposes a methodology for the systematic identification of vulnerabilities associated with wireless access protocols and systems and the quantitative evaluation of the resulting risks for mobile operators using attack trees, while considering the current legislative frameworks. The proposed methodology has been designed to aid both, mobile operators towards planning more effective cybersecurity strategies and adopting efficient defences to minimise the probability of an attack and predict its impact on the operational, market and business aspects of mobile network operators. The proposed risk assessment analysis is evaluated over three distinct vertical scenarios, namely an emergency call, a high-speed train commute and a massive public event, with the most relevant threats and their impact being measured and discussed. The evaluation of the model revealed significant results for mobile network operators that are deploying a mix of legacy and state of the art cellular technologies.

INDEX TERMS Attack trees, risk analysis, wireless cellular networks, wireless security.

I. INTRODUCTION

Over the last few years the way people and machines communicate and interact with each other has undergone a tremendous revolution with wireless mobile communication networks playing a pivotal role. From providing solely voice communications to extremely high speed, ultra-low latency multimedia services, cellular networks have reached to the point where they constitute one of the most significant enablers of the Information Age. The current estimations of mobile subscribers is around 8 billion, with the potential of reaching 8.9 billions by 2025 [1]. Smart phones and mobile devices in general are used today not only for communication but to support different vertical services including electronic payments, navigation, healthcare and fitness monitoring, business management, etc. As the fifth generation (5G) of cellular networks is reaching maturity, is expected to play an essential role in the digital transformation of the economy and society, leading to an augmented dependency of user's and services on cellular network technologies [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Mostafa Zaman Chowdhury.

The densely deployed mobile cellular networks are also targets of malicious intruders as physical access on the components of the network (i.e., base stations, repeaters, etc.) is not required. Although cellular networks constitute an easy attack vector, a possible attack against them could seriously disrupt mission critical mobile communications (autonomous vehicles, connected cars) and user's perceived quality, while it could further affect their privacy [3].

The technological advancements in cellular network technologies have resolved several vulnerabilities discovered in the older versions, the coexistence of legacy technologies (Global System for Mobile communications - GSM, Universal Mobile Telecommunication System - UMTS, Long Term Evolution - LTE and 5G) lay the foundation for adversaries to perform downgrade attacks and consequently bypass the improved security of modern generations [4]. Vulnerabilities exist even in 5G due to the trade off between security and usability. Similarly to the butterfly effect [5], a seemingly insignificant alteration in the security configurations may have a massive effect on the overall security of the system, thus the risk. Mobile Network Operators (MNOs) need to carefully examine their risk, considering the vulnerabilities caused by the protocol's specifications, the coexistence of legacy wireless technologies and the MNO's security configurations on the access network.

On the other hand, the European Union (EU) directives such as the General Data Protection Regulation (GDPR) [6], the telecommunications EU directive [7], the ePrivacy [8] directive and the security of Network and Information Systems (NIS) [9] directive underline the importance of security by enforcing all organizations to adopt policies and controls for the protection of network's security and user's privacy by design. These regulations impose enormous financial sanctions in the event of information leakage harming both the organization's financial stability as well as its reputation.

Even though the European Commission (EC) as well as, the Federal Communications Commission (FCC) recognize the importance of security especially in the 5G era [10], [11], particular frameworks for vulnerability and risk assessment have yet to be proposed. For these reasons, MNOs need to heavily invest on the security of their infrastructure by studying every possible vulnerability that could affect the security of their network and consequently expose user's privacy. Due to the plethora of security-related parameters, each MNO has adopted its own security configurations and policies and as a result, it is confronted with different vulnerabilities. It is crucial to create an interoperable framework for identifying and quantifying the overall risk of MNO-specific infrastructures. Even though cellular networks have been thoroughly investigated since their first deployments three decades ago, there is a lack of systematic studies on the methods and procedures required for calculating the risk to MNO's, due to detected vulnerabilities.

This paper aims to identify the feasible attacks and assess the risks against the security of MNO's Radio Access Network (RAN), which is one of the four 3GPP's security domains [12], along with the related vulnerabilities caused by either protocol specifications or by MNO's decisions on security configurations. The outcome of this work is a detailed, comprehensive and systematic methodology aligned with the National Institute of Standards and Technology (NIST) framework's course of action [13], [14] to estimate the risk of an MNO in the RAN side. There is a clear motivation to define a risk analysis methodology that would incorporate the recently identified vulnerabilities and associated threats that legacy, state of the art and future generation cellular networks are exposed to. Moreover, a detailed and accurate mapping of the resulted impact of threats to the identified consequences that MNOs would suffer in case of an attack, is still a requirement that this paper is set to address. This study performs a comprehensible and holistic classification of the different plausible attacks and threats against all existing RAN technology generations, using the Confidentiality, Integrity, Availability (CIA) triad with the addition of a fourth parameter, which is the Privacy, due to its association with GDPR. Additionally, the proposed risk assessment model supports attack trees that allow an in-depth analysis of the attack paths, while offering an understandable graphical representation of attacks, threats, vulnerabilities and possible preventive measures; hence, allowing non-cybersecurity experts to comprehend the nature and impact of a vulnerability and its resulted risk. Moreover, the proposed methodology for determining and assessing the threats on RAN is customizable and scalable, since new leafs on the attack trees can be easily added, whenever new attacks and vulnerabilities are discovered. The current paper further extends previous research studies that consider risks horizontally, by incorporating different factors of the attack path that affect the security of the infrastructure, the qualitative and quantitative analysis of the vulnerability and the significance of its impact. Towards this end, a formalized evaluation metric of the impact of attacks is proposed, to estimate the risk of a MNO. The risk is considered as the probability of the occurrence of an unwanted event, multiplied by its impact to the system.

The rest of the paper is structured as follows, Section II briefly describes the key architectural components of cellular networks, while Section III presents the security features of each cellular technology. Section IV discusses the related work in the filed of security vulnerabilities and threats on cellular networks. In Section V the vulnerabilities of cellular networks are presented in details, while Section VI presents the proposed analytical model for estimating attack probabilities. Furthermore, Section VII provides an overview of the proposed countermeasures deployed by MNOs and Section VIII models in a systematic manner the threats affecting mobile cellular networks and defines the related attack trees. In Section IX the methodology for quantifying of the risk is defined, along with a proposed schema for measuring the impact of the attacks on MNOs based on socio-economic and technological criteria. The risk analysis model is evaluated in Section X, against three vertical scenarios that are design to cover all related threats and provide insight to

the impact that the deployment of legacy and state of the art cellular technologies has on MNOs. Finally, Section XI concludes the paper and drafts the future steps.

II. CELLULAR NETWORK ARCHITECTURE OVERVIEW

Driven from the ever increasing user requirements for higher data rate, low latency and extremely reliable ubiquitous mobile wireless services, the cellular network technologies have been rapidly involving over the last thirty years progressing from the circuit-switched GSM (Second Generation-2G) to the All-IP based 5G wireless networks [15]. Throughout this transition cellular network architectures have followed the same overall structure, which consists of three main parts, namely, the Mobile Station (MS), the RAN and the Core Network (CN), as shown in Fig. 1.

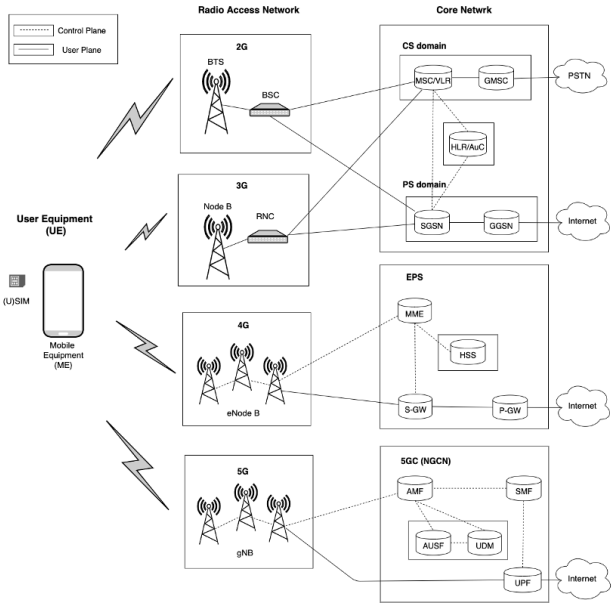


FIGURE 1. Overview of cellular network architectures.

Specifically, the MS consists of the User Equipment (UE) and the Service Identity Module (SIM) or the UMTS SIM (USIM) card. The SIM/USIM card includes a unique, for each user, International Mobile Subscriber Identity (IMSI) used for the identification of the subscriber. The first three bytes of IMSI signify the Mobile Country Code (MCC), while the next two or three bytes represent the Mobile Network Code (MNC). The remaining bytes stand for the mobile subscriber identification number (MSIN). Due to the IMSI's uniqueness, its use should be avoided as it can solely identify the user. To protect user's privacy a Temporary Mobile Subscriber Identity (TMSI) for 2G and 3G or Globally Unique Temporary Identifier (GUTI) for 4G and 5G is proposed instead. The RAN or GERAN (GSM EDGE RAN) in GSM is composed of the Base Transceiver Station (BTS), which is controlled by the Base Station Controller (BSC). In UMTS the RAN or UTRAN (UMTS RAN) is composed of the NodeB and the Radio Network Controller (RNC) that are equivalent to GSM, BTS and BSC.

The CN can be grouped into two distinct categories: i) the Circuit Switch (CS) and ii) the Packet Switch (PS) domain. In the CS domain, the BSC and the RNC, for 2G and 3G respectively, are connected to the Mobile Switching Center (MSC) which is responsible for routing calls. The MSC communicates with the Gateway Mobile Switching Center (GMSC), to route calls outside the mobile network, for example to the Public Switched Telephone Network (PSTN). The MSC and RNC are also connected to the Home Location Register/Authentication Center (HLR/AuC), which is a central database that contains details about the authorized subscribers of the network (e.g., IMSI, current location area of an MS, etc.) and produces authentication data. The Visitor Location Register (VLR) is a database for visiting subscribers. In the PS domain, the MSC and the RNC are connected to the Serving GPRS Support Node (SGSN), which is responsible for the delivery of data packets. Apart from the routing of data packets, the SGSN controls the authentication and charging functions of PS domain. The SGSN communicates with the Gateway GPRS Support Node (GGSN), which is the gateway of the cellular network to the external packet data networks including Internet.

In 4G technology, the access network consists only of eNb's which communicate with each other and the core network, acting as the BSC (2G) or RNC (3G) of the previous generations. The Mobility Management Entity (MME) is a key entity for the 4G technology. Among other, it communicates with the Home Subscriber Server (HSS), which a central database, for the authentication procedure. It is also responsible for the session, the connection and the mobility management. The Serving Gateway (S-GW) routes and forwards packets to the Packet Data Network Gateway (P-GW), while it is also an important entity for backwards compatibility purposes The P-GW is the entity that will provide eventually the connectivity with the Internet [16]. The communication of the UE with the core network is managed with the Non-Access Stratum (NAS) protocol which is responsible for the mobility and session management. The radio signaling between the UE and the eNodeB (eNb) is achieved through Radio Resource Control (RRC) protocol [17].

In 5G the access network is comprised of gNB similar to 4G eNb nevertheless, the core network architecture bears no resemblance with its ancestor. The RAN communicates with the Access and Mobility Function (AMF) responsible for the connection and mobility procedures. The latter is connected to the Authentication Server Function (AUSF), which supports the authentication, as well as the Unified Data Management (UDM) which generates the authentication credentials and manages the subscriber's information, such as the Subscription Permanent Identifier (SUPI) which is the 5G's equivalent to IMSI. The Session Management Function (SMF) provides the connectivity to the internet by allocating the UE's IP and managing the session and traffic steering to the User Plane Function (UPF). The SMF is also responsible for billing. Lastly, the UPF is the entity that communicates with the data network, responsible for

packet routing and forwarding [18]. In 5G in order to avoid sending the permanent identifier in plain text the Subscription Concealed Identifier (SUCI) is sent instead. The SUCI is the SUPI encrypted with the MNO's public key.

III. SECURITY FEATURES OF CELLULAR NETWORKS

A. GSM SECURITY FEATURES

The objective of the employed security features in the GSM and the General Packet Radio Service (GPRS) is to protect user's privacy without omitting any service or deteriorating the usability. To provide a certain level of security, cellular networks include functions for: i) authentication (i.e., A3), ii) encryption on signaling and user plane traffic (i.e., A5 for GSM or GEA for GPRS) and iii) generation of cipher key used for encryption (i.e., A8). The authentication key (K_i) is unique for every user i and secret, meaning that it is never send from the MS to the CN. A challenge-response scheme is used instead, which can verify whether the SIM/USIM possess indeed the correct key. The key K_i is stored within the SIM/USIM card for the MS side and in the HLR/AuC for the CN side. If the user is not connected to his home network, then the HLR/AuC will send the authentication triplets to the VLR or SGSN, for the CS or the PS domain of the visiting network, respectively. The encryption key (K_c) is produced using (K_i) and a random value send from the CN as input for the A8 algorithm. The encryption key K_c is used by A5 or GEA algorithms to encrypt data exchanged between the MS and the cellular network [17], [19].

B. UMTS SECURITY FEATURES

The 3G technology besides the functions used for i) authentication (i.e., f1), ii) encryption of user and signaling data (i.e., f8) and iii) generation of cipher key for encryption (i.e., f3), has introduced functions for: iv) integrity check on signaling data (i.e., f9) and v) generation of the key used for integrity (i.e., f4). Similar to 2G, the authentication scheme in 3G is a challenge-response scheme. The CN will send a random value along with the corresponding authentication token (AUTN) to the MS, which will verify the AUTN (mutual authentication) and send back its response (RES) using its private key. If the response matches the expected response (XRES) then the authentication procedure is terminated successfully. It should be noted that in 2G only the user authenticates to the network; the network is not authenticated to the user. In 3G and later generations, the authentication is mutual. UMTS and later cellular technologies further support a sequence counter (SQN) both in the UE and the CN side for synchronization, maintained in the USIM and the HLR/AuC respectively. An additional improvement of the 3G technology is the fact that the encryption continuous until the RNC, while in 2G the encryption terminates in the BTS for the CS and the SGSN for the PS domain.

The Authentication and Key Agreement (AKA) procedure takes place between the UE and the CN for the agreement of the session keys, the Cipher Key (CK) and the Integrity Key (IK). When the AKA procedure is performed, it protects the integrity of signaling messages as well as the confidentiality of both the signaling data and the user data.

C. LTE SECURITY FEATURES

Similarly to 3G, the 4G (LTE) supports, i) authentication (i.e., f1), ii) encryption (i.e., f8), iii) generation of cipher key for encryption (i.e., f3) as well as, functions for iv) the integrity check (i.e., f9) and the v) generation of key used for integrity (i.e., f4). Nevertheless, the generation and management of keys in 4G are a more complicated processes than those in previous generations. In LTE, apart from the authentication key K_i and the keys CK and IK, which were present also in 3G, there is an additional master key (K_{ASME}), which is used to generate the separate keys used for the communication with the Core and the Access Network (through the NAS and RRC protocol respectively). The K_{ASME} is derived from the CK and IK and is send from the HSS to the MME. Specifically, the K_{ASME} is used to generate the confidentiality and integrity keys for the secure communication, during signaling procedures, between the UE (K_{NASenc}) and the MME (K_{NASint}), as well as, between the UE and eNb (K_{eNb}). The K_{eNb} will be used to calculate the separate keys for integrity (K_{RRCint}) and confidentiality (K_{RRCenc}) of the signaling data among the UE and the eNb, and the key for confidentiality (K_{UPint}) of the user plane messages. There is no integrity key for user plane messages [16].

D. 5G SECURITY FEATURES

The 5th network generation resembles the key hierarchy of 4G but with adjustments justified by the differences in the core network architecture. The key (K_{AUSF}) derived from CK and IK, is shared between the ME and the Authentication credential Repository and Processing Function (ARPF)/Unified Data Management (UDM) and it is used within the boundaries of the home network. This key is used by the Authentication Server Function (AUSF) to generate the anchor key (K_{SEAF}) that used by the Security Anchor Function (SEAF) for the serving network. In turn, K_{SEAF} generates the shared key between the Access and Mobility Function (AMF) and the UE, named (K_{AMF}). The AMF is the entity responsible for the generation of the NAS layer keys (K_{NASenc}) and (K_{NASint})) as well as, the radio access network key (K_{gNb}), which is shared between the gNb and the UE. The latter key K_{gNb} is used to calculate a series of keys, namely the K_{RRCint}, the K_{RRCenc}, the K_{UPint} and the K_{UPenc}. In contrast to the previous generations, 5G supports integrity protection in user plane messages [18].

E. LEGISLATION AND DIRECTIVES IN TELECOMMUNICATIONS

The EU General Data Protection Regulation (GDPR) [6], which came into effect in 2018, mandates companies and individuals handling or processing personal data that belong to EU citizens to adopt measures to protect the privacy of the data subject. As personal data, GDPR has considered all

information that may be linked to a natural person. GDPR is considered ''one of the strictest and most accurate privacy laws worldwide'' [20], therefore it comprises of the main legislative ground for this work used as a reference point to estimate the impact of an attack. The Privacy and Electronic Communications Regulations (PECR), also known as ePrivacy directive, is complementary to the GDPR and focuses on the privacy of the data subject on electronic communications [8]. Apart from user data mentioned in GDPR, the PECR covers traffic and location data as well.

Cellular networks have fortified their infrastructure through the techniques mentioned in the previous subsections. Nevertheless, even with the proposed solutions there is a residual risk due to the continuous technological progress and the simultaneous support of older generations. In 5G the user's permanent identity is recommended to be concealed while temporary identifier should be refreshed after each usage. Furthermore, the specifications suggest that both user and signaling data are encrypted and integrity protected to ensure personal data from accidental, unauthorized or unlawful access, use, modification, disclosure, loss, destruction or damage (EU GDPR Article 5) [20]. Previous generations did not focus neither on the concealment of the user permanent identity nor on the frequent update of the temporary identity, while the user data were not integrity protected.

The European Electronic Communications Code (EECC), will replace the current EU telecommunications framework as of December 2020. EECC supports the notion of confidentiality and privacy of users by design as well as the integrity and availability of the network while it urges the need for risk assessment (Articles 40 and 41) [21]. EECC further introduces definitions on the security of services apart from network, as well as a toolbox of risk mitigating measures for 5G networks [22]. Another relevant EU legislation is the NIS Directive (Directive on Security of Network and Information Systems) addressed to Operators of Essential Services (OES) and Digital Service Providers (DSP) whose infrastructure is labeled as critical. The expected outcome of the NIS directive is the successful governance and monitoring of critical infrastructures from the responsible authorities of the EU member states [23].

IV. BACKGROUND WORK

The background work is discussed with focus on two categories, namely i) the security of cellular networks, the threats, attacks and vulnerabilities, identified by the research community and ii) the risk management methods used to estimate the overall risk of cellular networks.

A. CELLULAR NETWORKS ATTACKS, THREATS AND VULNERABILITIES

There are many research works related to cellular networks' vulnerabilities. Both the 3rd Generation Partnership Project (3GPP) and NIST have released technical reports and specifications explaining the possible threats [12], [24]–[27], while the most extensive literature reviews are presented in [28]–[30]. In particular, [28] provides a thorough analysis of all possible threats and vulnerabilities that could lead to serious attacks against GSM, UMTS and LTE. This survey classifies and categorises the security issues focusing on the network's architecture, by identifying the three attack entry points: the mobile device, the access and the core network. Some of the attacks included were IP-based, signaling or jamming attacks. Mitigation techniques for 4G were also included, in accordance with the employed technology, the type and the category of the attack. Moreover, [29] presented an analysis on cellular network attacks and vulnerabilities for all network generations with the intent to identify the security implications for the newest generation, 5G. This work differentiated from others as it introduced a systematic methodology for attacks and defenses. Specifically, it categorized the attacks by their aim, the proposed defenses and the causes, separating the ones related to the specifications from those related to implementation. The causes included were pre-authentication traffic, lack of mutual authentication, weak cryptography, insecure inter-network protocols, resource usage asymmetry, insecure or leaky implementation, cross-layer information loss and accounting policy inconsistency. In [30] a thorough study and a categorisation of the possible threats in LTE/LTE-A, is included, focusing on the IP-based architecture. The paper is proposing evaluation criteria for data collection and data analysis to achieve attack detection through machine learning techniques. More specifically, the authors managed to detect jamming and signaling attacks, Session Initiation Protocol (SIP) abnormal messages, Voice over LTE (VoLTE) and Sort Message Service (SMS) spamming as well as, mobile botnets.

Moreover, in [31] the authors proposed two tools (*"LTEInspector"* and *"LTEFuzz"*) to examine the security of 4G LTE during the attachment and the mobility control plane procedures. The *"LTEInspector"* was dedicated to NAS messages while the latter included RRC messages as well. The tool managed to identify ten (10) novel attacks and nine (9) already existed in the literature. The authors further observed that paging messages, which maintain the connection between the network and the UE when the latter is in idle mode, do not have any cryptographic protection. *"LTEFuzz"* identified new vulnerabilities both in the design and the implementation of LTE. Some of the mentioned attacks are related to the security mechanisms employed on the MME and the baseband chipset of the UE. The authors suggested countermeasures to diminish the security risk. Similarly, *"5GReasoner"* [32] followed *"LTEInspector"* rationale to attest the security of the 5G network control plane communications in the radio channel, meaning both NAS and RRC messages. *"5GReasoner"* managed to identify eleven design weaknesses, resulting in attacks against the integrity of the user messages, the availability of both the UE and the network as well as privacy of the user. Five inherited vulnerabilities from 4G were also discovered.

On the other hand, [33] followed a different approach for the detection of novel attacks. While most studies are

focused on the security of the physical and network layer, they chose to explore the security of the data link layer. The findings included three new types of cellular network attacks against LTE: identity mapping, website fingerprinting and user data manipulation by exploiting the AES-CTR (Advanced Encryption Standard in counter mode) encryption mode in user data messages. The work in [34]–[37] perform an evaluation of the security mechanisms employed by different MNOs. Particularly, authors in [34] examined the radio access technology in commercial 4G and future 5G networks and provided metrics for the paging and TMSI allocation procedure frequency. In [35] the *"GSMMap"* provides a publicly available comparison of the implemented protection features between different operators. The threat scenarios included intercept (active or passive), impersonation and tracking while the security features examined were the encryption algorithms used, the randomness of the keys, the frequency of the authentication and TMSI allocation and the protection of IMSI. According to the report, Greek MNOs have lately adopted some of the recommended measurements thus, they are moving towards safer communications. The work in [36] presented a tool, which captured and analyzed the security policy of MNOs. More specifically, *"(U)SimMonitor"* inspected the traffic to estimate the usage of each technology (2G or 3G), the employed algorithms for encryption, as well as, the frequency of AKA, TMSI and IMSI allocation. [37] investigated the security configurations of 12 MNOs across Europe (Austria, Czech Republic, Germany, Spain, and France), giving emphasis to the authentication procedure and the algorithms used for encryption. The results are rather unsatisfactory due to the support of EEA0 algorithm which does not offer any cryptographic protection hence could lead to an impersonation attack. The authors concluded that four out of the twelve MNOs suffered from severe misconfigurations while they successfully demonstrated an impersonation attack.

B. RISK ANALYSIS IN CELLULAR NETWORKS

The research work on the risk management for cellular networks is rather limited. In a work closely related to this one is [38] where the authors presented attack jungles as a method to define which attacks are most likely to happen thus identify which attack has the minimum cost for an adversary. Attack jungles, in contrast to attack trees, allow cycles and re-usability of resources which may pose an additional complexity both in the representation and the analysis of the attacks. Furthermore, in [39] the authors proposed the use of attack trees to identify the primary security requirements, thus the possible threats and their impact for automotive on-board networks, meaning vehicle to everything (V2X) communications. The presented analysis can be used in combination with the vehicle manufacturer's security policy, in order to decide whether to accept, transfer or take measures to reduce the identified security risks. The estimation of the attack potential though does not consider real-life measurements. The authors of [40] presented a qualitative risk analysis for GPRS technology. This study evaluated the risk in a scale of five classes, by estimating the impact and the likelihood of the plausible attacks against the network. The analysis concluded that the attacks that threaten the integrity and confidentiality of both network and user data presented a high-risk level. Nevertheless, since the analysis is qualitative, the results cannot be validated with real metrics. Furthermore, the methodology is not applicable in the latest mobile network generations.

3GPP specifications [41] introduced a risk analysis methodology for 2G and 3G, nevertheless it is not extensible and cannot be adapted to the contemporary standards. Thus, the numbers used for the probability of an attack are not based on real metrics that rely on the MNO's security configurations. Moreover, NIS Cooperation Group released in late 2019 a risk assessment report [2] for the security of 5G networks, in which it presents an overview of the threats, the threat actors, the assets and the vulnerabilities, while providing some qualitative assessment criteria and risk scenarios. This report, despite its generic nature, paves the way for more specific methodologies to assess the risks of 5G infrastructures.

Building and extending the the NIS approach, this paper proposes a methodology that evaluates the risk of MNOs network infrastructure quantitatively, considering the vulnerabilities and threats of all heterogeneous wireless access and core network technologies and protocols that coexist in current cellular systems. This paper focuses on the definition of a solid, yet, simple methodology, which considers all threats identified by the existing literature, in the radio access network of the cellular technologies 2G (GSM), 3G (UMTS), 4G (LTE) and 5G. The probability of an attack is quantitatively estimated for each MNO, considering its security configuration while using real metrics that can be deduced by open-source tools. The proposed methodology for estimating the probability of an attack from the existing network vulnerabilities is based on attack trees that are easier to understand as they do not include cycles. Each recognised threat is studied individually therefore no complex inter-dependencies exist. This work recommends also a method for evaluating the impact of an attack with regards to the GDPR framework, in order to quantitatively estimate the risk, which depends on the impact of the attack as very probable attacks may have a lesser or greater significance on the performance and reliability of the network. Finally, the proposed model is expandable since it can extend the attack trees to accommodate additional vulnerabilities, should these be discovered in the future.

V. VULNERABILITIES AND MISCONFIGURATIONS OF CELLULAR NETWORKS

The vulnerabilities of cellular networks can be grouped into two main categories, i) the technological vulnerabilities due to the architecture design (Class A) and ii) the vulnerabilities triggered by MNO's misconfiguration (Class B). We argue that the vulnerabilities included in the first category cannot

be easily amended by the MNO, while the vulnerabilities enlisted in the second category can be mitigated with the appropriate measures by the MNO.

A. TECHNOLOGICAL VULNERABILITIES (CLASS A)

(a) Authentication and Key Agreement (AV1): The lack of mutual authentication concerns only the 2G networks. In later generations such as 3G, 4G and 5G, the authentication between the UE and the network is mutual, following a challenge-response scheme. Table 1 summarizes the security vulnerabilities of every commercially deployed network generation. 5G, provides a unified authentication framework supporting, apart from the 5G AKA, the Extensible Authentication Protocol (EAP-AKA), which supports different types of credentials such as, certificates or username and password as well a,s the EAP Transport Layer Security (EAP-TLS). This flexibility allows 5G networks to cover the numerous needs and vertical services. In this paper the focus is on mobile devices, therefore only the security of 5G-AKA is considered.

(b) Confidentiality (AV2): In terms of confidentiality there are two different types of messages that need to be reviewed: i) the signaling messages (control plane) and ii) the user data (user plane). The 3GPP specifications recommend, but not mandate, that user data should be confidentially-protected in all network generations (i.e., 2G, 3G, 4G, 5G). Protection mechanisms are also provisioned by the specifications for signaling messages (i.e., RRC and NAS), although there are some exceptions (i.e., the pre-authentication traffic such as Attach Request, RRC Connection and Paging messages). Ciphering in RRC and NAS is recommended by the 3GPP specifications but it remains an operator option. It has to be underlined that among the pre-authentication traffic, information such as the RAND and the AUTN is included. To this extend, some signaling messages in all network generations are always send unciphered, by design. The literature [31]–[33] has already covered some of the LTE as well as, 5G vulnerabilities associated with unprotected messages (i.e., RRC connection, paging and auth. reject messages).

(c) Integrity (AV3): In terms of integrity 2G did not provide protection mechanisms neither for signaling messages nor for user data, until recently where in [17] and [42] integrity protection is introduced for the enhanced General Packet Radio Service (GPRS) in relation to Cellular Internet of Things (CIoT). Even though the latest 3GPP specifications [42] have included integrity protection mechanisms for 2G, it is doubtful that MNOs have implemented this recommendation, allocating financial resources in an outdated technology to reconfigure the infrastructure. 3G and 4G include integrity protection techniques for signaling messages (both NAS and RRC). Nonetheless, similar to confidentiality, there are some exceptions (i.e., RRC Connection messages, sent prior to authentication during attachment, or Paging messages [19], [31]–[33], [43]). The latest 3GPP specification on LTE (Release 15), which was released in 2019, suggest that user data could also be integrity protected [44]. Although it seems unlikely for MNOs to have already applied this recommendation, as 4G is commercially deployed since 2009, it could however prepare the ground for more secure 5G implementations as it seems to be the case according to [18].

B. MNO MISCONFIGURATIONS (CLASS B)

(a) Key Generation Algorithms (BV1): Although 3GPP states that *"the operation of the key generation functions falls within the domain of the MNO"*, there are some examples of key generation algorithms specified for the MNOs that do not wish to design their own. The first proposed algorithm COMP128 was vulnerable. The latest specifications propose two algorithms: MILENAGE and Tuak [45]. MILENAGE is based on AES (Rijndael), while Tuak is based on *Keccak* permutation. Tuak allows lengthier keys than MILENAGE for future flexibility. The literature refers to some vulnerabilities but practical attacks against the aforementioned algorithms have not been demonstrated up till now.

(b) Encryption Algorithms (BV2): Apart from the security features included in the 3GPP specifications, cellular network security depends on the chosen configurations of the MNO. In order to assess the security level of an MNO, the encryption algorithms that the MNO supports must be reviewed. Algorithms such as, A5/0, UEA0, EEA0 and NEA0 do not provide any cryptographic protection. Specifically, A5/1 and A5/2 stream encryption algorithms, which are used for voice encryption have been characterized as breakable due to cryptographic vulnerabilities of the Linear Feedback Shift Register (LFSR) [46]. For the these algorithms open source decryption tools have been released [47], [48]. Due to the vulnerabilities found in A5/1 algorithm, which can lead to known plaintext attacks, GSM specifications [42] have proposed the use of random values for padding the packets as a countermeasure. MNOs that deploy the A5/1 algorithm to further harden the encryption scheme have included the International Mobile Equipment Identity (IMEI) that is different for each user, in the cipher mode complete message [36]. GEA1 and GEA2, which are used for data encryption are also using LSFR, thus they are subjected to the same attacks as A5/1 and A5/0 [46], [49]. The algorithms A5/3 and GEA3, which use KASUMI, have been proven vulnerable but only in theory, while there are no known attacks for A5/4, GEA4 and UEA1, which also use KASUMI. The UEA2 and EEA1 algorithms use SNOW 3G, while EEA2 and EEA3 use AES in CTR mode and ZUC respectively [29]. The authors in [33] achieved a chosen-ciphertext attack by exploiting the fact that user data in 4G are not integrity protected while AES in CTR mode is used

TABLE 1. Summary of cellular network's technological vulnerabilities (by design).

Technological vulnerability		2G	3G	4G	5G	Remarks
Lack of mutual authentication		●	○	◔	◔	
Lack of encryption	Signaling messages	◑	◑	◑	◑	Signaling messages are recommended to be encrypted. Nonetheless, there are some exceptions [19], [43] (i.e., pre-authentication traffic and paging). 3GPP recommends, but not mandates, that user plane messages should be encrypted.
Lack of integrity	Signaling messages	●	◑	◑	◑	Signaling messages are recommended to be integrity protected although there are some exceptions [19] (i.e., pre-authentication traffic, *RRC Connection Reject, RRC Connection Release* and *Paging*). *Latest 3GPP specifications suggest that 2G could also be integrity protected nevertheless it seems highly improbable for MNOs to change their configurations [42].
	User data	●	●	●	○	User data is recommended to be integrity protected only in the latest 3GPP release [18] referring to 5G.

● complete lack of security, ◑ partial lack of security, ○ presence of security

for encryption, which is vulnerable. The 5th generation algorithms, NEA1, NEA2 and NEA3 equivalent to 4G's EEA1, EEA2 and EEA3 respectively, may use 128 bits keys, but they shall support the transport of 256 bit keys, as well [18]. In this work we have consider that NEA2 is also unsafe, suffering from the same vulnerabilities as EEA2, as discussed in [33].

(c) Integrity Protection Algorithms (BV3): Another important indicator is the algorithm used for integrity protection. Integrity protection in 2G was not originally supported, the latest 3GPP's releases [42] propose GIA algorithm if the MNO decide to reinforce the security of their 2G infrastructure. In 3G, algorithms such as UIA1 and UIA2 are being proposed, based in KASUMI and SNOW 3G respectively. It should be mentioned that according to [50] and [51], there are concerns on the randomness of a 256-bit *IK* key size on UIA2 due to SNOW [49]. Nevertheless the 3GPP specifications on SNOW 3G already propose a 128-bit key. In 4G, EIA1, EIA2 and EIA3 are recommended which are based on SNOW 3G, AES in CMAC mode and ZUC. The 5th generation algorithms, NIA1, NIA2 and NIA3 equivalent to 4G's EIA1, EIA2 and EIA3 respectively, may use 128 bits keys but they shall support the transport of 256 bit keys as well [18].

(d) Frequency of AKA (rekeying) and key refresh (BV4): The AKA procedure can take place during the attachment of the ME to the network or during the mobility. In an earlier study we have argued that the best configuration is to perform AKA in every data request, call and SMS [36]. The frequency of AKA reallocation procedure can distinguish different MNO's, as a short period between two consecutive executions indicates that the keys change regularly. The AKA frequency may also affect other security parameters, such as the TMSI, as a fresh key is necessary to encrypt them. Although AKA is one of the most important procedures for security, the specifications neither oblige nor recommend a specific period for the AKA procedure. During AKA the MSC/VLR or SGSN contacts the HLR/AuC for fresh authentication vectors. A frequent AKA procedure may cause delays to the network, hence some operators may considered performance over security. In 4G the AKA procedure differentiates as the K_{NAS} and the K_{eNb} keys are not the same. Both keys are derived from the K_{ASME} but the K_{eNb} keys include a freshness parameter. As mentioned in the specifications there is a difference between the K_{eNb} re-keying and K_{eNb} refresh procedure, since *"the key hierarchy does not allow direct update to RRC and UP keys, but fresh RRC and UP keys are derived based on a fresh K_{eNb}"*. Evidently, the re-keying procedure is initiated by the MME after a successful AKA and affects all keys (i.e., both K_{NAS} and K_{eNb}), while the key refresh procedure only affects the K_{eNb} and takes place during intra-cell handovers. Therefore, in 4G besides the AKA, the key refresh procedure needs to be examined as well in order to assess the vulnerability caused by the rare key renewal. Similarly, in 5G the keys between the gNb and the UE can be changed without initiating an AKA procedure. Therefore, the frequency of the key refresh must be examined together with the frequency of the AKA (rekeying).

(e) Frequency of TMSI and GUTI (re)allocation (BV5): The TMSI or GUTI is sent from the ME to the network during the attachment, the mobility procedure and the paging procedure. It is temporary identifier in 2G, 3G and 4G networks, which should change on a regular basis otherwise they are equivalent to a permanent identifiers. A frequent TMSI reallocation can distinguish different MNO's, as a short period between two consecutive executions indicates that the temporary identifier (TMSI/GUTI) change regularly, thus identity mapping cannot be achieved. In [36] we have established that the TMSI should change at the end of every communication. The TMSI/GUTI reallocation procedure is usually performed in ciphered mode during the attach or tracking area update procedures to avoid mapping the old TMSI/GUTI to the new one [43]. There is a strict provision in 5G networks regarding the TMSI/GUTI refresh that must be executed after the *"initial registration"*, the *"mobility registration update"* and the network triggered Service Request. This feature makes identifying

or tracing subscribers, based on 5G-GUTI, impractical [52]. If adversaries manage to gain access to the temporary identity, then they could use this information to track a subscriber's location by checking its presence in a specific area and reveal hers/his past or future movements [53]. Another type of attack demonstrated in [54], is mapping a mobile phone number to its TMSI. According to [55], even when TMSI and GUTI change often the identity can be revealed, when the pattern is predictable.

(f) Usage of IMSI (BV6): The IMSI is sent from the ME to the network during the first attachment, or whenever the TMSI/GUTI cannot be retrieved. Regardless the 3GPP recommendations to avoid the use of IMSI since it is a permanent identity, some operators may still use the IMSI more often than recommended, which could lead to identity leakage. *Piercer* attack [54] managed to expose several MNO's that due to flawed paging deployment, the attacker can map the victim's phone number to its IMSI and subsequently identify user's location in a specific area. Furthermore, in the same research IMSI-Cracking attack is demonstrated and the authors identify that some digits of the IMSI can be predicted, while the rest of them can be guessed through brute-force. Based on the extensive research on the security issues caused by the unencrypted exchange of the IMSI between the ME and the network, the 5th generation of mobile networks introduced the SUPI, which contains the IMSI but should not be transferred in clear text over the next generation RAN except the part that contains the routing information, (i.e., Mobile Country Code - MCC [18]). The Subscription Concealed Identifier (SUCI) constitutes an encrypted SUPI, freshly generated each time by the UE using Elliptic Curve Integrated Encryption Scheme (ECIES) along with the MNO's key. In addition to the cryptographic protection of SUPI using the SUCI, the 5G specifications decouple its use during the paging process. The support of long-term identifiers as a paging identifier is currently replaced by the TMSI and the Radio Network Temporary Identifier (RNTI).

(g) MNO's noncompliance with 3GPP recommendations (BV7): Lastly, in order to assess the total risk of an MNO's radio access infrastructure, its level of compliance with the 3GPP recommendations as presented in the ''class A'' category of our model, should be investigated. For instance the MNO might choose not to follow the suggestions on encryption and integrity protection mechanisms (Table 1), as they are not mandatory. Additionally, as discovered in [31], it is possible for MNO's to partially apply the 3GPP suggestions, leaving some important messages unprotected (i.e., ''security mode command''). The same research recognized that at least one US MNO used EEA0 which does not provide protection.

The above miconfigurations are summarised in Table 2.

VI. PROBABILITY ESTIMATION LINKED TO VULNERABILITIES

We assume that the attacker has the technical ability and the appropriate equipment, if needed, to launch an attack thus gain access to the wireless part of the communication. Moreover, we consider the attacker equally motivated in exploiting all recognised vulnerabilities. The vulnerability related to the lack of mutual authentication ($AV1$) is defined as:

$$P_i(\text{exploit } AV1) = n_i \cdot x_i \quad \text{with } n_i = \begin{cases} 1, & \text{if } i = 2G \\ 0, & \text{if } i = 3G, 4G \text{ or } 5G \end{cases} \tag{1}$$

where, x_i is the percentage of the employed technology and defined as the $1 \times i$ size vector $x_i = [\%2G, \%3G, \%4G, \%5G]$.

Observation: It is evident that for (1), both the support of a mutual authentication scheme and the percentage of the employed technology, x_i are considered in order to calculate the probability. For 2G we consider that a skilled attacker can certainly exploit this vulnerability therefore the probability equals the usage of the 2G technology.

The probability of a successful attack caused by the lack of encryption ($AV2$) and the lack of integrity protection ($AV3$) is calculated as follows:

$$P_i(\text{exploit } AV2) = \frac{u_i^{AV2}}{T_i} \cdot x_i \tag{2}$$

$$P_i(\text{exploit } AV3) = \frac{u_i^{AV3}}{T_i} \cdot x_i \tag{3}$$

where, u_i^{AV2} and u_i^{AV3} denote the number of unprotected messages per network generation i, related to vulnerabilities $AV2$ and $AV3$, respectively. The total number of messages per network generation is T_i.

Observation: If the employed generation (2)(3) does not protect any of the messages then the probability of the attack is equal to the percentage of the employed technology.

Observation: The number of the unprotected messages (2)(3) may vary per technological generation and vulnerability (i.e., confidentiality or integrity).

The probability of an attack triggered by vulnerabilities in the key generation ($BV1$), the encryption ($BV2$) or the integrity protection ($BV3$) algorithms is estimated as follows:

$$P_i(\text{exploit } BV1, BV2, BV3) = r \cdot x_i \quad \text{with r} = \begin{cases} 1, & \textit{if the algorithm is vulnerable} \\ 0, & \textit{if the algorithm is considered safe} \end{cases} \tag{4}$$

For the vulnerability related to rekeying / key refresh ($BV4$), we assume that the encounter has the knowledge and the resources to learn the key size that MNO is using. The attacker may learn the size of the key for a specific MNO either by impersonating a legitimate user or by intercepting the signaling messages that contain this type of information. The time period during which the key size is unchanged by the MNO is t, while k is the key size that MNO is using and $E_k(t)$

TABLE 2. Summary of the authentication and key generation, encryption and integrity algorithms used in cellular networks.

Security Algorithms	Technology	Algorithm	Type	Key size (bits)	Attackable	Reference
Authentication and key generation	2G	COMP128	COMP128	128 input,96 output	●	[46]
	2G/3G/4G/5G	Milenage	AES (Rijndael)	128 input/output	○	[42] [45]
	3G/4G/5G	Tuak	Keccak	128 or 256 input/output	○	[45]
Confidentiality	2G/3G voice	A5/0	-	-	○	[29]
		A5/1	LFSR	64	●	[29]
		A5/2	LFSR	64	●	[29] [46]
		A5/3	KASUMI	64	◑	[29]
		A5/4	KASUMI	128	○	[29]
	2G data	GEA0	-	-	●	[42]
		GEA1	LFSR	64	●	[29]
		GEA2	LFSR	64	●	[29]
		GEA3	KASUMI	64	◑	[29]
		GEA4	KASUMI	128	○	[29]
		GEA5	SNOW 3G	128	○	[56]
	3G data	UEA0	-	-	●	[29]
		UEA1	KASUMI	128	○	[29]
		UEA2	SNOW 3G	128	○	[29]
	4G data	EEA0	-	-	●	[29]
		EEA1	SNOW 3G	128	○	[29]
		EEA2	AES in CTR	128	●	[29]
		EEA3	ZUC	128	○	[33]
	5G data	NEA0	-	-	●	[18]
		NEA1	SNOW 3G	128	○	[18]
		NEA2	AES in CTR	128	●	[18] [33]
		NEA3	ZUC	128	○	[18]
Integrity	2G	GIA4	KASUMI	128	○	[42] [56]
		GIA5	SNOW 3G	128	○	[42] [17] [57]
	3G	UIA0	-	-	●	-
		UIA1	KASUMI	128	○	[19]
		UIA2	SNOW 3G	128	○	[19]
	4G	EIA0	-	-	●	[16]
		EIA1	SNOW 3G	128	○	[16]
		EIA2	AES in CMAC	128	○	[16]
		EIA3	ZUC	128	○	[16]
	5G	NIA0	-	-	●	[18]
		NIA1	SNOW 3G	128	○	[18]
		NIA2	AES in CMAC	128	○	[18]
		NIA3	ZUC	128	○	[18]

● practical attacks have been discovered, ◑ attacks have been discovered but only in theory, ○ no attacks have been found

as the number of different keys of length k that the encounter can generate and try in time t.

$$P_i(\text{exploit } BV4) = \begin{cases} 1, & for\ k = 0 \\ \dfrac{E_k(t)}{k} \cdot x_i, & for\ k \neq 0 \end{cases} \quad (5)$$

Observation: For every pair t_1, t_2, where $t_2 \geq t_1$, we have $E_k(t_2) \geq E_k(t_1)$. Thus, in order to reduce the probability of a successful attack (5), the MNO has to decrease the time t, where the key remains unchanged.

Observation: The time t may vary between different generations i due to the different key size k. Therefore, the mixing of different cellular network generations x_i is also considered in (5). **Observation:** When $k = 0$, the employed algorithm does not provide any cryptographic protection (i.e., EEA0), consequently the probability of a successful attack is 1.

The most frequent attacks related to the frequency of TMSI (re)allocation ($BV5$) are tracking the subscriber or identifying the user. Therefore, a less frequent TMSI update could allow an adversary to correlate different messages thus extract information. The 5G standards propose an update after TMSI usage to avoid this vulnerability nevertheless previous generations have discovered to be vulnerable. The probability

of an intruder to exploit this vector is defined as follows:

$$P_i(\text{exploit } BV5) \begin{cases} (1 - \frac{1}{m_t}) \cdot x_i, & for\ m \neq 0 \\ 0, & for\ m = 0 \end{cases} \quad (6)$$

where, m denotes the total number of the exchanged messages, that include the same TMSI, measured in a time frame t.

Observation: If $m_t = 1$ it indicates that the TMSI is updated in each message exchange therefore, the probability that an attacker might extract information by linking different messages is 0 (6).

Observation: The $\frac{1}{m_t}$ may vary between different generations i. Therefore, the usage of the generation x_i is also considered in (6).

Observation: If the TMSI is not included in the messages m for the observed time frame t, then the probability to exploit this threat is equal to 0 (6).

For the vulnerability connected with the usage of the IMSI ($BV6$), we consider that for every message that contains the IMSI, the probability of an attack is estimated as follows:

$$P_i(\text{exploit } BV6) = \begin{cases} 1 \cdot x_i, & for\ i\text{=2G,3G,4G,5G(SUPI)} \\ (1 - \frac{1}{m_t}) \cdot x_i, & for\ i\text{=5G(SUCI) and } m \neq 0 \\ 0, & for\ i\text{=5G(SUCI) and } m = 0 \end{cases} \quad (7)$$

Observation: The probability of an attack is independent of the number of messages that contain the IMSI due to the fact that one message is enough to leak identity information (7).

Observation: For 5G, the probability (7) to take advantage of a permanent identifier is dependant to the operators deployment. If the MNO sends the SUPI, then the probability connected to the usage of an identifier follows IMSI's rationale. If however the MNO uses a key to conceal the identifier, then the vulnerability is calculated by the number of messages that contain the same SUCI. Similar to the TMSI, if the SUCI remains unchanged between many messages, the adversary could deduce information.

Finally, the probability of exploiting an MNO's inclompliance to 3GPP specifications P_i(exploit BV7)(8) depends to vulnerabilities $AV1$, $AV2$ and $AV3$. Therefore, if the MNO does not follow the recommendations, then the (1),(2) and (3) may alter. The most common case is that u_v is not the same as described in the 3GPP specifications.

VII. PROPOSED COUNTERMEASURES BASED ON CURRENT RESEARCH

A. TECHNOLOGICAL VULNERABILITIES (CLASS A)

a) *Authentication and Key Agreement (AV1):* MNOs must stop supporting 2G technology as it has effects on the overall security level. Nonetheless, there are some research works that propose mitigation techniques concerning the absence of mutual authentication in 2G technology [58]. In parallel, [28] advocates both a control traffic detection system and a certificate authority.

b) *Confidentiality (AV2):* Authors in [59] support that the capabilities of the UE should not be sent prior to the authentication, while [58] recommends authenticated paging responses and [60] encrypted paging requests using an unlikability key. The use of a PKI infrastructure according to [31] is not a feasible solution as it is not in accordance with the performance requirements of the standards.

c) *Integrity (AV3):* In 2G the integrity protection mechanisms did not exist until recently, which is a severe drawback. 3GPP released documents defining GIA algorithm for 2G integrity protection. Due to the introduction of integrity protection in 3G, frequent authentication is less needed [41] however, user data are still not protected. In [33] it is suggested to utilise authenticated encryption for the user plane. The latest release of 3GPP specifications include integrity key for user data, as well. In other research works, the use of a digital signature scheme is proposed, according to which, each BTS and UE owns a certificate [61]. Fianlly, in [28] a control traffic detection system is advocated.

B. MNO MISCONFIGURATION (CLASS B)

a) *Encryption Algorithms (BV2):* MNOs should not support A5/1, A5/2 [49], GEA1 and GEA2, as they are already broken. Furthermore, algorithms such as: UEA0 and EEA0 are introduced only in emergencies, in which case the BTS selection is random, otherwise these algorithms should never be used due to their lack of any cryptographic protection. In case that the MNO supports A5/1, then in order to verify its vulnerability level, the use of padding randomization and inclusion of IMEI should also be examined. In [36] has been proved that only one MNO in Greece supported such measurement. Additionally, in [29] describes the use of passive behavioral analysis of control traffic in order to detect downgrade attacks against the cryptographic algorithms.

b) *Integrity Protection Algorithms (BV3):* Integrity protection was introduced later that the rest security mechanisms; hence, there are no known attacks against the suggested algorithms.

c) *Frequency of AKA (rekeying) and key refresh (BV4):* AKA should be executed as frequent as possible without deteriorating the usability. A frequent AKA execution can protect from persistent attacks.

d) *Frequency of TMSI and GUTI (re)allocation (BV5):* Similarly to AKA, the TMSI/GUTI allocation should be executed as frequent as possible without deteriorating the usability, to prevent targeted DoS. The results retrieved from [36] indicate that these actions are not as regular as they should, thus affecting the security of the MNO. As additional countermeasures, pseudo TMSIs could be used instead of the real ones [62] or a PKI to encrypt the TMSI [29].

e) *Usage of IMSI (BV6):* Opposite to AKA/TMSI/GUTI, the IMSI execution should be avoided. However, since this measurement seems unfeasible, the use of a Pseudo-IMSI [63] or a PKI to encrypt the IMSI [29] is proposed. The latest specifications on 5G define a SUPI that can indicate the IMSI and a Subscription Concealed Identifier (SUCI) that contains the concealed SUPI [64]. An IMSI Catcher Catcher is proposed in [65] for protection against IMSI Catchers from adversaries. Alternatively, public key encryption mechanisms could be used for the protection of the IMSI during the initial registration [61]. The work in [29] describes the use passive behavioral analysis of control traffic aiming at discovering unauthenticated IMSI requests.

f) *MNO's compliance with 3GPP recommendations (BV7):* MNOs should follow the 3GPP policies concerning the messages that should be encrypted.

VIII. THREAT MODELING FOR CELLULAR NETWORKS USING ATTACK TREES

Threat modeling is a common and effective process to identify and prioritize risks. One approach to achieve threat modeling is attack trees, which provide a simple yet methodical way to describe the security of a system as they present every step of a possible attack [66]. The root node of the attack tree is the goal of the attacker, while its children are the ways to accomplish the goal. The relationship between the nodes may be conjunctive (AND) or disjunctive (OR) [67].

A. THREAT MODEL

The basic security requirements, known as the CIA triadare, are:

(i) Confidentiality,
(ii) Integrity,
(iii) Availability

For the purposes of this paper the threats with regards to the CIA triad will be examined, with the addition of a fourth category:

(iv) Privacy,

due to its direct implications with GDPR compliance. Furthermore, the paper is examining the attackers' capabilities against these four security requirements. The proposed categorization carefully examines the different goals of the attacker (i.e., access/tamper a message or compromise the network). In this approach, the adversary could be either an authorized subscriber of the network or manage to gain unauthorized access in the radio communication. The attacker, therefore, may be able to capture radio transmissions passively or even participate actively by injecting messages, either control or user data, on the radio channel. The study is focusing on attacks and threats associated with the protocol's architectural vulnerabilities or the chosen configurations, particularly in the radio access part, meaning the messages exchanged through the air. For the purposes of this study, physical attacks, malicious MNOs/insiders/manufacturers, malware and software bugs, are not considered. Moreover, jamming attacks and attacks due to the internet traffic (i.e., TCP/UDP packets), are nor taken into consideration due to the inability to estimate accurately the probability of their occurrence.Finally, for the remain of the analysis, the probability of a downgrade attack is regarded as the probability to use the 2G network.

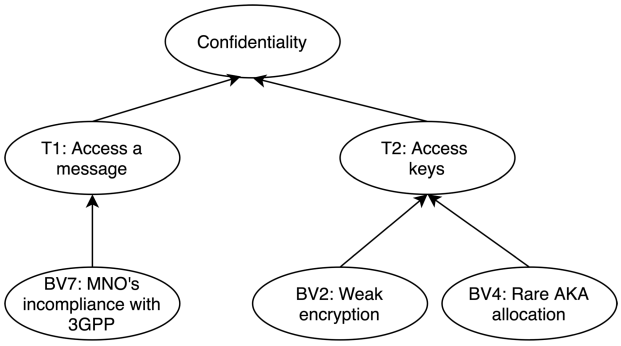


FIGURE 2. Attack tree for Confidentiality.

B. ATTACK TREE DESIGN: IDENTIFICATION OF ATTACKS, THREATS AND VULNERABILITIES

The threats and the vulnerabilities against cellular networks, have been identified, based on the research in [28], [29], [33]. Each of these threats is based on a different set of vulnerabilities while their impact value varies. The identified vulnerabilities related to the threats are divided in two categories, namely (i) technological vulnerabilities (class A) and (ii) configuration mistakes (class B).

1) CONFIDENTIALITY

The threats against the confidentiality of the system are separated into distinct categories [49], as shown in Fig. 2. During such threats the attacker may manage to either access a message or access a key. Evidently, the attacks considered in this category are passive attacks, since the attacker does not interfere with the communication, which would also affect the integrity of the system.

T1:Access a message

Threat: An adversary may manage to eavesdrop the communication and subsequently read a message (SMS or packet) or listen to a call.

Vulnerabilities:

- *BV7*: incompliance to 3GPP specifications by lack of encryption in *"SecurityModeCommand"* signaling message (4G)

Attack surface/Method to accomplish the attack: Both user data and signaling messages are encrypted in every generation hence there is no need to specify the type of the message. In 2G since the network is not authenticated to the user, illegal access to messages is possible by impersonating the network, which is an active attack for our model (T4: Modify/create/delete messages originated from the network). In later generations 3G and 4G, the authentication is mutual,

thus there are no acknowledged methods for an attacker to read the contents of an encrypted message without initially retrieving the key (which is another threat category in our approach, T2: Access keys). The only alternative is to either trick the UE into not using encryption (i.e., by exploiting *SecurityModeCommand* message) as described in [31] or access the non-encrypted messages (i.e., RRC connection, paging and *AuthReject* messages) [31], [33]. The useful information that can be retrieved from the unencrypted messages (*RRCConnection*, paging and *AuthReject*) is privacy-related, which is a different category in the proposed methodology [49] (as will be discussed in the following ***T7: Determine subscriber's id and location, T8: Discover ME's information*** and ***T9: Map information to another information***).

Requirements: malicious eNb, victim's IMSI or GUTI.

Threat Probability Estimation (vulnerabilities): Described in Section V

Impact Evaluation: It is a serious attack for both EECC and GDPR legislation, as unauthorized parties may gain access to sensitive information nevertheless we consider that it has a limited applicability therefore it will not severely impact the MNO's operations or reputation.

Proposed Countermeasures: Described in Section VII.

T2: Access keys

Threat: An adversary may manage to eavesdrop the communication and access the keys or break the encryption scheme.

Vulnerabilities:

- *BV2*: weak encryption algorithms (i.e., A5/1) and lack of additional countermeasures (padding randomization and inclusion of IMEI).
- *BV4*: rare AKA allocation (comparing to the proposed frequency for AKA allocation).

Attack surface/Method to accomplish the attack: This attack may be achieved by performing cryptanalysis and consequently manage to disclose the keys (K_i, K_c, *IK* or *CK*) [41].

Threat Probability Estimation (vulnerabilities): Described in Section V.

Impact Evaluation: This threat affects the overall security of the network thus it's not compliant with both EECC and GDPR. It will impact all communications and consequently severely damage the reputation of the MNO.

Proposed Countermeasures: Described in Section VII.

2) INTEGRITY

The threats against the integrity of the system were separated into two distinct categories, as depicted in Fig. 3, where an intruder may have the ability to (i) modify messages originated from the user or (ii) modify messages originated from the network. In the category of threats associated with the integrity of the system the following active attacks have been considered.

T3: Inject or Modify messages originated from the user

Threat: Redirect, drop or inject calls or messages (SMS or packets). This form of threat can be linked to user's impersonation and over-billing attacks. The adversary could create fake messages (i.e., empty paging messages) pretending to be a legitimate UE.

Vulnerabilities:

- *AV3*: lack of integrity in user data messages (2G, 3G, 4G) and lack of integrity in certain signaling messages (3G, 4G, 5G).
- *BV2*: weak encryption algorithms (i.e., A5/1) and lack of additional countermeasures to weak encryption. algorithms (i.e., padding randomization and inclusion of IMEI).
- *BV4*: rare AKA allocation (comparing to the proposed frequency for AKA allocation).

Attack surface/Method to accomplish the attack: Integrity protection is nonexistent in 2G while in 3G and 4G technology, only signaling messages are integrity protected. The absence of integrity protection mechanisms combined with the fact that some messages are, either by default (i.e., RRC Connection message) [31] or by erroneous configuration (i.e., Security Mode Command) [33], not encrypted, permits to modify user messages [31], [67]. To this extend, even a fake attach procedure, on behalf of a legitimate user, can be accomplished. A malicious UE can impersonate a user and perform unauthorized actions or even alter location information in the case of a fugitive in order to avoid tracking from the authorities as described in (authentication relay attack) [31]. Another interesting attack vector are the emergency messages. An attacker could send a fake emergency request to the network and gain access to services [29]. User impersonation could be also attained if the attacker manages first to "***T2 Access keys***". In 5G user plane messages are protected therefore only the control plane messages excluded from the integrity protection mechanisms are vulnerable (6). Authors in [32] discovered that even in the latest generation messages such as, *"RRC establish request"*, *"RRC resume request"*, or *"NAS registration request"*, which do not employ neither integrity protection mechanisms nor ciphering, could be used by adversaries to impersonate the user. Man-In-The-Middle attacks are though less plausible since it is mandatory to integrity protect radio control messages that redirect devices. This feature makes it infeasible for false base stations to perform rogue redirections.

Requirements: malicious UE, victim's IMSI (or GUTI), or IMEI, or C-RNTI [32].

Threat Probability Estimation (vulnerabilities): Described in Section V.

Impact Evaluation: Similarly to ***T1***, this threat is considered to be a targeted attack, against a specific subscriber, as the attacker needs some information about the victim (i.e., IMSI or MSISDN), therefore we consider this attack limited to only the targeted subscribers.

Proposed Countermeasures: Described in Section VII.

T4: Modify (create/delete) messages originated from the network

Threat: Redirect, drop or create calls or messages (either SMS or packets) or even authentication vectors. This form of

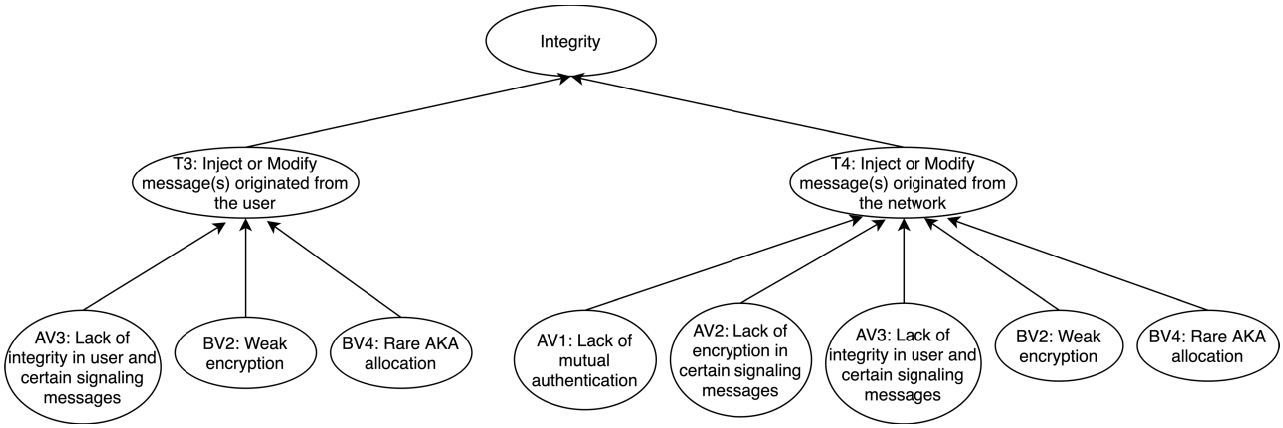


FIGURE 3. Attack tree for Integrity.

threat can be linked to network's impersonation by creating either a fake BTS/eNb or by replaying an already known challenge (RAND) as part of mobility signaling.

Vulnerabilities:

- *AV1*: lack of mutual authentication (2G).
- *AV2*: lack of encryption in certain signaling messages (2G, 3G, 4G, 5G) (i.e., RRC Connection message).
- *AV3*: lack of integrity in signaling messages (2G), lack of integrity in certain signaling messages (3G, 4G, 5G).
- *BV2*: weak encryption algorithms (i.e., A5/1) and lack of additional countermeasures to weak encryption algorithms (i.e., padding randomization and inclusion of IMEI).
- *BV4*: rare AKA allocation (comparing to the proposed frequency for AKA allocation).

Attack surface/Method to accomplish the attack: In 2G, there are no integrity mechanisms while only the UE authenticates to the network and not vice versa. Therefore, it is easy for an adversary to modify the identity of the network hence, create a fake base station and access all user messages [28]. Even in later generations, due to the backwards compatibility, an adversary might create a fake base station and bypass the improved security features. Nevertheless, 5G describes a framework for detecting false base stations in the MNO's network in order to inform the subscribers thus take legal actions. Moreover, later generations such as 3G, 4G and 5G, make use of integrity protection mechanisms for signaling data. It should be denoted though, that some signaling messages do not employ the integrity protection mechanisms (i.e., paging, auth reject, detach request or emergency messages). Hence, an adversary may exploit these messages to impersonate a legitimate network. The network impersonation could lead to accessing non-encrypted messages, disconnecting the UE [32] or creating a fake emergency alarm [31]. Last but not least, the pre-authentication traffic in all generations (2G, 3G, 4G, 5G) is neither encrypted not integrity protected.

Requirements: malicious eNb, victim's IMSI (or GUTI), already known RAND, C-RNTI [32].

Threat Probability Estimation (vulnerabilities): Described in Section V.

Impact Evaluation: This threat is not compliant with EECC legislation thus it could affect the overall security of the network.

Proposed Countermeasures: Described in Section VII.

3) AVAILABILITY

As depicted in Fig. 4, the threats against the availability of the system were separated into [49] distinct categories: i) those that concern the mobile equipment (ME) of the user and ii) those that concern the network infrastructure.

T5: Disable/Detach ME

Threat: An adversary may manage to disable or detach the UE from the network.

Vulnerabilities:

- *AV1*: lack of mutual authentication (2G).
- *AV2*: lack of encryption in certain signaling messages (2G, 3G, 4G, 5G) (i.e., RRC Connection message).
- *AV3*: lack of integrity (2G), lack of integrity in certain signaling messages (3G, 4G, 5G).
- *BV2*: weak encryption algorithms (i.e., A5/1) and lack of additional countermeasures to weak encryption algorithms (i.e., padding randomization and inclusion of IMEI).
- *BV4*: rare AKA allocation (comparing to the proposed frequency for AKA allocation).

Attack surface/Method to accomplish the attack: This attack can be successfully completed by impersonating a legitimate BTS or eNb and subsequently disconnecting the UE by sending the messages that are not integrity protected as discussed in ***T4: Modify (create/delete) messages originated from the network*** (auth reject, detach req or paging messages). Additionally, the attach messages (i.e., RRC connection messages) could be exploited to achieve blind DoS attack since they do not apply either encryption or integrity mechanisms [31], while too many paging requests to the UE could further achieve battery drain. Disconnecting the UE can be also achieved by changing the RAND or RES to invalid values during the authentication procedure [41]. This attack is realizable as both encryption and integrity protection is applied after the authentication.

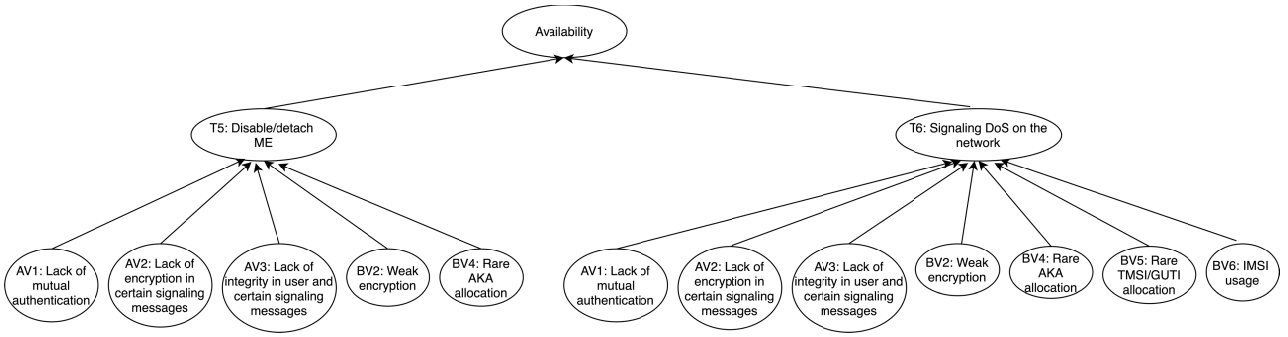


FIGURE 4. Attack tree for availability.

Requirements: malicious eNb, IMSI (or GUTI), C-RNTI [32]

Threat Probability Estimation (vulnerabilities): Described in Section V.

Impact Evaluation: It is a serious attack though it could be restricted within the boundaries of a specific geographical area or subscriber. It is probable to harm human life in case of emergency.

Proposed Countermeasures: Described in Section VII.

T6: Signaling DoS on the network

Threat: An adversary may successfully accomplish a DoS attack against the network by impersonating a legitimate user.

Vulnerabilities:

- *AV1*: lack of mutual authentication (2G)
- *AV2*: lack of encryption in certain signaling messages (2G, 3G, 4G, 5G) (i.e., RRC Connection message).
- *AV3*: lack of integrity (2G), lack of integrity in certain signaling messages (3G, 4G, 5G).
- *BV2*: weak encryption algorithms (i.e., A5/1) and lack of additional countermeasures to weak encryption algorithms (i.e., padding randomization and inclusion of IMEI).
- *BV4*: rare AKA allocation (comparing to the proposed frequency for AKA allocation).
- *BV5*: rare TMSI/GUTI allocation (comparing to the proposed frequency for TMSI/GUTI allocation).
- *BV6*: IMSI allocation (instead of TMSI).

Attack surface/Method to accomplish the attack: This kind of attack may be achieved by exhausting user traffic capacity over the air interface (i.e., in 4G, too many RRC connection requests to the eNb), since these types of messages do not require prior authentication [49]. Another method is by sending different security capabilities in *"NAS attach requests"* to disrupt the authentication synchronization [31]. Traffic analysis could also lead to the same results.

Requirements: malicious UE

Threat Probability Estimation (vulnerabilities): Described in Section V.

Impact Evaluation: This treat affects the overall security of the network as well as, the reputation of the MNO; hence, it may prove extremely disruptive for mission critical and emergency services. It violates EECC and optionally NIS legislation.

Proposed Countermeasures: Described in Section VII.

4) PRIVACY

The threats against system's Privacy are separated into four categories, i) subscriber's location, ii) mobile equipment (ME) information and iii) information mapping, as illustrated in Fig. 5.

T7: Determine subscriber's id and location (tracking)

Threat: An adversary may retrieve the location of the subscriber trough the IMSI, TMSI/GUTI and optionally the Tracking Area ID (TAI).

Vulnerabilities:

- *AV2*: lack of encryption in certain signaling messages (2G, 3G, 4G, 5G) (i.e., RRC Connection message, Paging messages).
- *BV2*: weak encryption algorithms (i.e., A5/1) and lack of additional countermeasures to weak encryption algorithms (i.e., padding randomization and inclusion of IMEI).
- *BV5*: rare TMSI/GUTI allocation (comparing to the proposed frequency for TMSI/GUTI allocation).
- *BV6*: IMSI allocation (instead of TMSI).
- *BV7*: incompliance to 3GPP specifications by lack of encryption in *"security mode command"* messages.

Attack surface/Method to accomplish the attack: The lack of protection mechanisms on particular signaling messages, exchanged either prior to the authentication or during paging, in all cellular network technologies (2G, 3G, 4G, 5G) may permit attackers to access important information. Identifiers such as IMSI, TMSI/GUTI, IMEI and MSIN as part of the IMSI, were heavily included in older generations signaling messages, many of which were sent unencrypted, regardless of the fact that they contain valuable data whose exposure could lead to subscriber's tracking [31]. Even in the cases where the TMSI/GUTI is used instead of the IMSI, attackers can easily deduce location information either due to the lack of frequent updates which is an operator option or by following the TMSI/GUTI updates in the radio communication [31]. An attacker could also learn the Mobile Station International Subscriber Number (MSISDN) hence the IMSI, by sending fake identity requests to which the UE will respond.

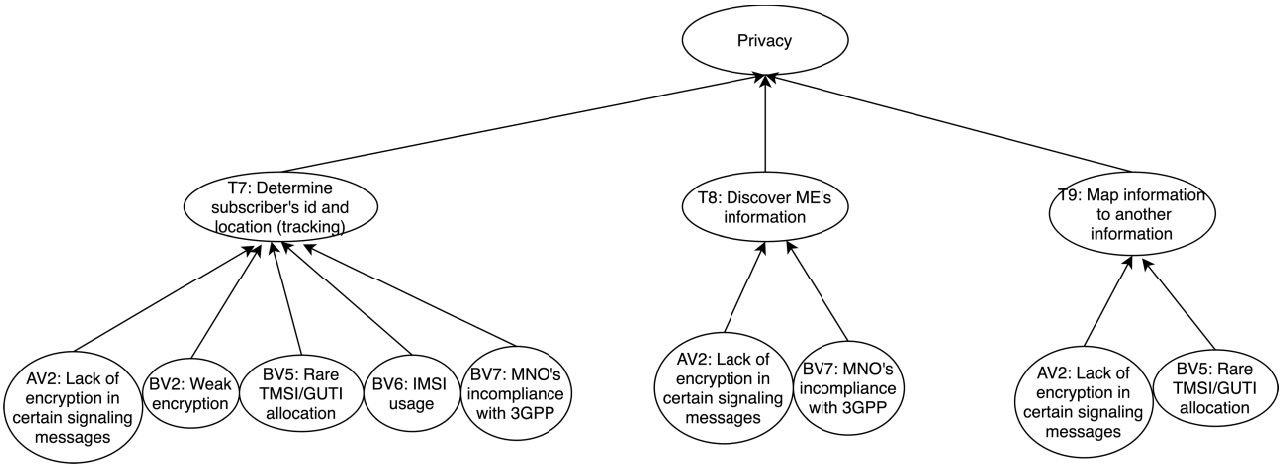


FIGURE 5. Attack tree for privacy.

5G technology has tried to overcome the vulnerabilities related to the exchange of the IMSI in plaintext, which was a major issue in the previous technologies, by introducing the SUCI. The SUCI conceals the identity of the subscription (including the MSIN). As a result, instead of the IMSI, the UE sends either the GUTI or the SUCI for identification [18]. The IMEI in specific, in GSM and UMTS is securely stored within the UE but sent without any cryptographic protection in the radio channel. In LTE, the IMEI is securely stored while it is recommended to be confidentiality protected in the radio channel. Nevertheless, it could be included before the NAS security [16]. In 5G, Permanent Equipment Identifier (PEI) substitutes for the IMEI and is sent after NAS security context is established, unless during emergency registration when no NAS security context can be established [18].

Nevertheless, there are still vulnerabilities that could be exploited by malicious parties, either related to the lack of privacy provisioning by the MNO or the unauthenticated emergency call option, where the privacy protection for SUPI is not required [18]. *Paging*, *RRC Request* and *Attach Request* (3G, 4G) messages contain both info on the identity of the subscriber either IMSI or TMSI-GUTI and tracking are information (i.e., TAI). A *Tracking Area Update* Request message contains the old GUTI as well as the last TAI (3G, 4G). TMSI/GUTI or generally UE information may be available in other messages as well namely: i) *Registration Request* (GUTI)(5G), ii) *N1 NAS Signalling Connection*, (TMSI)(5G), iii) *RRC Connection Request* (TMSI) (3G, 4G), iv) *RRC Connection Setup Complete* (TMSI) (4G), v) *RRC Connection Setup* (3G), vi) *RRC Early Data Request* (TMSI) (4G) and vii) *RRC Connection Reject* (3G). In addition, authors in [31] demonstrated that an attacker can check the presence or absence of a certain UE in an area by retrieving and replaying a *Security Mode Command* message and observing the UE's response. A different way to learn the subscriber's location history is by performing the authentication relay attack [33] by taking advantage of the lack of encryption (by erroneous configuration) in *Security Mode Command* message. However, this attack requires to impersonate the user first.

Threat Probability Estimation (vulnerabilities): Described in Section V.

Impact Evaluation: According to Article 5 of the GDPR, location information is considered personal. Inevitably, unless the processing of this information is legitimate as described in Article 9 of the GDPR, the attacks related to location leakage pose a great threat against the subscriber's privacy. PECR and EECC legislations are also violated.

Proposed Countermeasures: Described in Section VII.

T8: Discover ME's information

Threat: An adversary may manage to eavesdrop the communication and collect information on UE, the capabilities of the UE (i.e., supported encryption algorithms) or the subscription. [59].

Vulnerabilities:

- *AV2*: lack of encryption in certain signaling messages (2G, 3G, 4G) (i.e., *RRC Connection message*).
- *BV7*: lack of encryption in "security mode command" messages.

Attack surface/Method to accomplish the attack: The victim's profiling is also achievable when the MNO does not secure messages such as, *"security mode command"* as recommended in [31]. Moreover, due to the by default unencrypted nature of some specific signaling messages, an attacker could deduce information, such as the UE capabilities, chosen security algorithms or the UE identity from specific messages, namely i) *Security Mode Command* (security algorithms)(3G, 4G, 5G), ii) *UE Capability Enquiry*, iii) *UE Capability Enquiry Information* (4G, 5G), iv) *Registration Request* (UE security capabilities)(5G), v) *Attach Request* (UE network capabilities), vi) *Tracking Area Update Request* (UE network capability) (4G), vii) *RRC Connection Reestablishment Request* (UE identity, MAC)(4G), viii) *RRC Connection Request* (UE identity, IMEI)(4G)(3G),

ix) *RRC Connection Resume Request* (UE identity)(4G), x) *RRC Connection Setup* (IMEI) (3G),xi) *RRC Connection Setup Complete* (UE system specific capability) (3G) and xii) *RRC Connection Reject* (IMEI) (3G).

Threat Probability Estimation (vulnerabilities): Described in Section V.

Impact Evaluation: This attack has an effect on the privacy of the subscriber as it exposes its identity. In this case, GDPR, PECR and EECC legislative frameworks apply.

Proposed Countermeasures: Described in Section VII.

T9: Map an information to another information (i.e., identity mapping)

Threat: Map an information to another information.

Vulnerabilities:

- *AV2*: lack of encryption in certain signaling messages (2G, 3G, 4G) (i.e., *RRC Connection message*, pre-authentication traffic).
- *BV5*: rare TMSI/GUTI allocation (comparing to the proposed frequency for TMSI/GUTI allocation).

Attack surface/Method to accomplish the attack: A possible attack is to map user's TMSI to a public identity (i.e., phone number) [68] and consequently, identify the user. Alternatively, TMSI could be mapped to the Radio Network Temporary Identity (RNTI) in layer [33], [49]. Another type of attack presented in [32], is profiling the service usage and user's activity by observing the NAS sequence number hence, the AKA sessions. It should also be mentioned that routing information is not encrypted, as such attackers may take advantage of the RNTI and try to map it to another information aiming at identifying the user within the network [33]. The RNTI is included in several signaling messages some of which are send unencrypted in the radio access channel namely: i) *Paging* (3G, 4G, 5G), ii) *RCC Reestablishment Request* (4G, 5G), iii) *RRC Resume Request* (4G, 5G), iv) *RRC Reconfiguration* (5G), v) *SIB1* (5G), vi) *RRC Connection Release* (3G, 4G), vii) *PUSCH Capacity Request* (3G), viii) *Physical Shared Channel Allocation* (3G) and the ix) *RRC connection Setup* (3G). Additionally the AKA frequency could be discovered by the *RRC Connection Resume* (key change for 5G).

Threat Probability Estimation (vulnerabilities): Described in Section V.

Impact Evaluation: This attack has an effect on the privacy of the subscriber, but it is a minor type of attack at this stage. The affected legislation include GDPR, PECR and EECC.

Proposed Countermeasures: Described in Section VII.

IX. RISK ASSESSMENT METHODOLOGY

A. CALCULATION OF THREAT PROBABILITY

The calculation of the cybersecurity risk for MNOs, that one or more vulnerabilities exposed, is based on the attack trees defined in the last section. Since each vulnerability can be exploited independently, without loss of generality the vulnerabilities $v = \{AV1, AV2, AV3, BV1, BV2, BV3, BV4, BV5, BV6, BV7\}$ are consider as statistical independent, hence a single OR-gate suffices for linking the vulnerabilities (leaves in the attack trees) to the threat T_i (root of the attack trees), where i denotes the network generation for all different categories of threats (i.e., confidentiality, integrity, availability and privacy). Considering the probability $P_i(v)$ of any vulnerability v being exposed in any given time, as defined in (1) - (7), the probability of a threat $P_i(T)$, is defined as follows:

$$\text{AND: } P_i(T) = \prod_v P_i(v) \tag{8a}$$

$$\text{OR: } P_i(T) = 1 - \prod_v (1 - P_i(v)) \tag{8b}$$

where $T = \{T1, T2, T3, T4, T5, T6, T7, T8, T9\}$, are the threats per cellular network generation, as defined in VIII-B.

B. IMPACT LEVELS

Following the definition of the vulnerabilities and misconfigurations of cellular wireless protocols and network architectures in Section V and the identification of the resulted threats that rises as consequence of assets being compromised according to the attack trees of Section VIII-B, the next step is to map the identified consequences to a discrete set of impact levels (e.g., between *Low* (1) and *Highly Critical* (5)), in accordance to [41] and [13]. This information will be used, along with the probability of threat occurrence $P_{T(i)}$ to calculate the overall risk level for an assessment.

In an effort to tailor the set of impact levels for the consequences relevant to the vulnerabilities and misconfigurations of MNOs as accurately as possible, a broad range of heterogeneous technological, operational and business objectives of MNOs have been considered. In Table 3 the set of consequences and impact levels, are shown. From this table, for example, it can be determined that ***T1:Access a message***, which has a limited applicability and it should not impact the MNO's operations or reputation severely, is considered to have a low impact on the MNO. In contrast, ***T6: Signaling DoS on the network***, which has the potential to affect the overall security of the network and harm the MNO's reputation, is considered to have high impact on the operator. The exploitation of vulnerabilities and misconfigurations that lead to such attacks, could also lead to regulatory penalties (GDPR financial sanctions), as shown in the table. In the proposed mapping of impact levels to the consequences, the experience of just one, out of the set of all the identified consequences associated with a particular threat, suffices for characterising the impact as *Low, High, Critical* or *Highly Critical*.

Threats, consequences and severity form a tuple that can be ranked based on the impact level, the resulting consequence or the type of threat and be considered for the calculation of the risk associated with the the threat and its severity on MNO's operational, business and marketing aspects. Based on the discrete impact levels and the probability of a threat as defined in (8b), the risk of a threat T for each cellular network

TABLE 3. Map of impact levels and consequences to MNOs operational and business aspects due to confidentiality, integrity, availability and privacy related threats.

Impact level	Scale	Consequence	Threats
Low	1	Minor injuries <10% of the subscribers of the MNO Limited to blogs press coverage No or unimportant information leakage **OR** No or unimportant modified information Rural, sparsely populated area or small neighbourhood service unavailability No Implications to critical services and operations, public safety and public order No service disruption	T1, T3, T5, T9
High	2	Minor Injuries to >10% subscribers of the MNO Local press coverage Information leaked with negligible consequences (only few subscribers affected) **OR** Modified information with negligible consequences (only few subscribers affected) City unavailability Negligible implications to critical services and operations, public safety and public order The service and normal operations will need <2 hours in order to return back to normal	T1, T3, T5, T9
Critical	3	Life threatening or severe consequences for one subscriber of the MNO Regional press coverage Information leaked with moderate consequences **OR** Modified information with moderate consequences Town area service unavailability Moderate implications to critical services and operations, public safety and public order The service and normal operations will need 2<h<24 hours in order to return back to normal 500K€financial sanctions, due to legislative noncompliance	T2, T3, T4, T5, T6, T7, T8
Critical	4	Life threatening or severe consequences for multiple subscribers of the MNO National press coverage Information leaked with serious consequences (i.e., national relations, terrorist attacks, etc.) **OR** Modified information with serious consequences (i.e., international affairs, terrorist attacks, etc.) Region area service unavailability Severe implications to critical services and operations, public safety and public order The service and normal operations will need 24<h<48 hours in order to return back to normal 10M€, or up to 2% of the operator's entire global turnover of the preceding fiscal year, whichever is higher, due to sanctions for noncompliance	T2, T3, T4, T6, T7, T8
Highly Critical	5	Life threatening or fatal consequences for one or multiple subscribers of the MNO International press coverage Information leaked with major consequences nation-wide (i.e., international affairs, terrorist attacks etc.) **OR** Modified information with major consequences nation-wide (i.e., international affairs, terrorist attacks etc.) International service unavailability Catastrophic implications to critical services and operations, public safety and public order The service and normal operations will need >48hours in order to return back to normal 20M€, or up to 4% of the operator's entire global turnover of the preceding fiscal year, whichever is higher, due to sanctions for noncompliance	T2, T3, T4, T6

technology i is defined as follows:

$$R_{T,i} = P_{T,i} \cdot \widetilde{I_T} \tag{9}$$

The risk is an expression of the probability of a threat $P_{T,i}$ occurring due to the exploitation of a threat T under any network generation i, multiplied by the severity of the threat's impact I_T, represented as discrete number and defined in Table 3. Since the threat's impact depends on the actual event, and the same threat can have different impact severity as can been seen from 3, the risk assessment $R_{T,i}$ is propotional to the average impact level of the threat $\widetilde{I_T}$, which is calculated as:

$$\widetilde{I_T} = \frac{\sum_{j=1}^{J} I_{T,j}}{j} \tag{10}$$

where, j denotes the total occurrences of the desired threat on Table 3. Evidently, the risk is proportionally affected by both the probability of a treat and the severity of its impact, thus a low probability threat that can cause a major destruction in the MNOs access network or loss of sensitive data, would be assessed as a high risk.

X. RISK ASSESSMENT EVALUATION

To evaluate the proposed risk assessment methodology, three scenarios describing three distinct vertical scenarios have been selected, namely: (a) an emergency call (112), (b) a high speed train commute and (c) a massive public event. All three scenarios include characteristics that classify them to all three quality of service categories (eMBB-enhanced

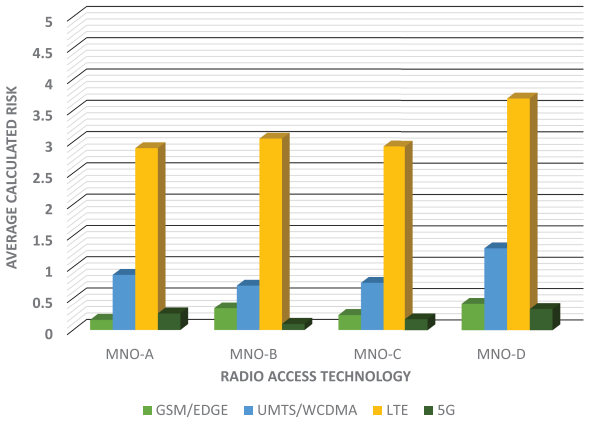
Mobile Broadband, mMTC-massive Machine-Type Communications and URLLC-Ultra-Reliable, Low-Latency Communications), as defined by [69].

Furthermore, in order to expand the statistical significance of the risk assessment methodology, we define four different MNO profiles (MNO-A, MNO-B, MNO-C and MNO-D), each of which has deployed and operates an amalgam of cellular network technologies and distinct security strategies. Based on recent reports on the average mobile subscriptions per cellular technology in Western Europe [70], the four MNOs' profiles have been defined in terms of subscriber coverage as in Table 4. The four MNO profiles pose unique characteristics that span a broad range of potentially real-world MNO deployments across Europe. The defined profiles also allow for the validation of as many threats as possible, resulting in a more comprehensive evaluation of the risk assessment model. In details, MNO-A and MNO-B are defined as operators that have selected a different blend of access technologies with MNO-A adapting quicker towards 5G and MNO-B selecting to keep legacy technologies deployed in an effort to support user equipment with lower capabilities and to minimise the cost of migrating to new technologies. Whereas, MNO-C and MNO-D are defined as operators that follow the same strategy in terms of deployed RATs, however MNO-C poses as more security aware than MNO-D, which has chosen to minimise the authentication transactions per connection in an effort to minimise signalling overheads and computational complexity. Moreover, MNO-D has avoided the use of SUCI, which would require a new USIM card, thus is not considered as practical. The details of the algorithms adopted by the four MNOs, which differentiate their approach towards security are summarised in Table 5.

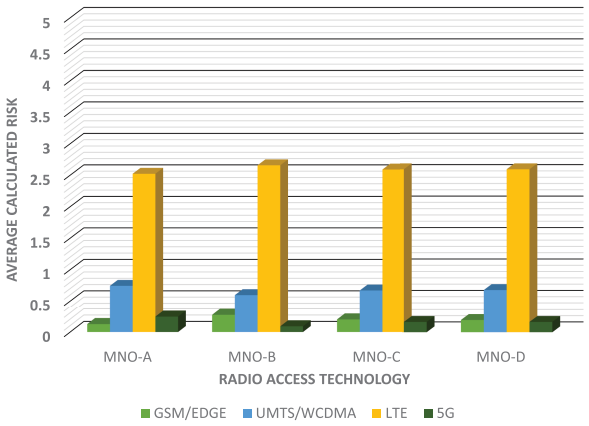
A. RISK EVALUATION DURING AN EMERGENCY CALL (112)

The pan-European emergency call number 112 has been (or is in the process of being) adopted by every member state. Currently 112 is based on legacy technologies and as part of the GSM standard it supports voice communication along with limited data from all GSM compatible mobile phones even when locked or with no SIM card present. In the verge of the 5G deployment, telecommunication providers are switching rapidly towards an All-IP infrastructure leaving behind the Public Switched Telephone Networks (PSTN). Therefore, next generation emergency services are bound to be provided over IP networks as well, with larger data sets for delivering real-time sensing data, accurate geodesic location and rich multimedia content to first responders [71], [72]. This scenario, provides the complexity of coexisting legacy and future cellular networks that are required to support GSM-based emergency calls (CS) in remote rural areas, or even next generation rich-content emergency services over high bandwidth 4G or 5G networks.

In particular, during an emergency situation, a user places a call to 112 through whatever network is available in the area. The emergency call could be routed through the user's own operator, or through a third operator, according to the network coverage in the area. In any case, the user will be able to make an emergency call even without a valid TMSI and without having to be authenticated. During the initial *Attach Request* message, the UE will send the IMSI (for 2G, 3G and 4G), or the SUPI (for 5G) or the IMEI (for a UE that does not possess a valid SIM). In case the emergency call is routed over a third operator, the MME will not communicate with the HSS to obtain the subscriber's data, as it does not belong in the operator's database. Nevertheless, it will use the MME Emergency Configuration [44]. The operator will allow the UE to call 112 without offering encryption or integrity protection in the voice channel. Similarly, in case of a next generation, data rich emergency call that would require a 4G and beyond RAT technology, the MME produces a K_{ASME}



(a) ***T2: Access a key***



(b) ***T8: Discover ME's information***

FIGURE 6. Assessment of Risk for each MNO profile in the Emergency Call scenario, across all Radio Access Technologies.

TABLE 4. Percentage of Radio Access Technology deployed by the four indicative MNO profiles.

Access Technology	MNO-A	MNO-B	MNO-C	MNO-D
GSM/EDGE	3.4%	7.4%	5.4%	5.4%
WCDMA/HSPA	19.92%	15.92%	17.92%	17.92%
LTE	70.36%	74.36%	72.36%	72.36%
5G	6.32	2.32	4.32%	4.32%

TABLE 5. Summary of the security strategy selected by the four MNOs.

Algorithm	2G			3G			4G			5G		
	MNO-A & B	MNO-C	MNO-D	MNO-A& B	MNO-C	MNO-D	MNO-A& B	MNO-C	MNO-D	MNO-A& B	MNO-C	MNO-D
Authentication Algorithm	COMP128	COMP128	COMP128	COMP128	Milenage	COMP128	Milenage	Tuak	COMP128	Milenage	Tuak	COMP128
Encryption Algorithm	A5/3&GEA3	A5/4&GEA4	A5/0&GEA0	A5/3&UEA1	A5/4&UEA2	A5/0&UEA0	EEA2	EEA1	EEA0	NEA2	NEA1	NEA0
Integrity Algorithm	-	GIA4	-	UIA1	UIA2	UIA0	EIA2	EIA1	EIA0	NIA2	NIA1	NIA0
AKA rekey/refresh	0.15	0.07	1	0.12	0.05	1	0.1	0.04	1	0.01	0.01	1
TMSI Allocation	0.55	0	0.76	0.32	0	0.75	0.14	0	0.57	0	0	0.1
IMSI Allocation	1	1	1	1	1	1	1	0	1	0.8	0.66	1

which is used to offer a multimedia connection with the responder nevertheless, no encryption or integrity protection is offered, to achieve a faster set up. Algorithms such as EEA0 and EIA0, that do not offer either confidentiality or integrity protection, are employed for the data channel.

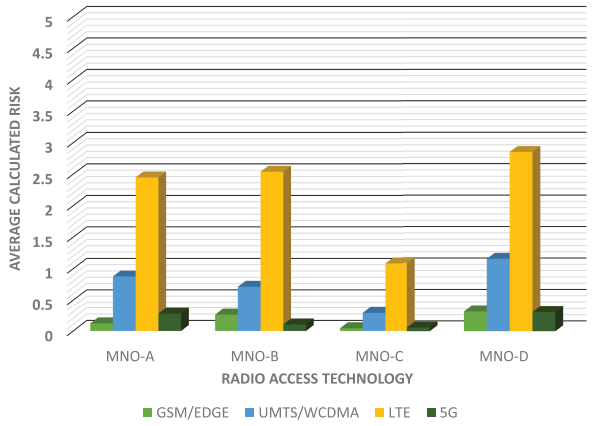
In the emergency call scenario the four MNOs are being examined against the threats ***T2: Access a key*** and ***T8: Discover ME's information***, which given the analysis provided in section VIII seem highly feasible while their impact according to Table 3 is evaluated as *Critical*. Figures 6a and 6b illustrate the calculated Risk of threats ***T2*** and ***T8*** respectively, for all MNOs involved in the scenario. Although the impact of both threats is similar, the risk assessment reveals that ***T2*** involves on average a higher risk for MNOs than that of ***T8***, due to the higher probability associated with the vulnerability *AV2: Weak or no encryption*. The rationale behind this result is that even thought ***T8*** is linked to more vulnerabilies, the number of messages that include information related to the identity of the subscriber and/or the location of the UE is limited. Hence, an adversary is more likely to exploit ***T2***, since it affects all of the exchanged messages in the case of an emergency. As expected, this is more evident in the case of MNO-D. In this scenario, the calculated risk is similar for all MNOs, with a noticeable exception in the case of the LTE network of MNO-D, which is due to the fact that the weaker security strategy of MNO-D will affect the most predominant cellular technology.

B. RISK EVALUATION DURING A HIGH SPEED TRAIN COMMUTE

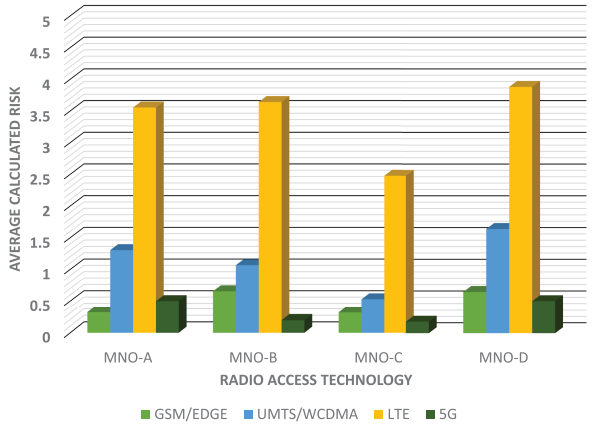
The railway vertical communication requirements have a significant complexity due to the mixture of heterogeneous wireless communication technologies that it requires to satisfy the needs for operational signalling and passenger communication needs, over high speeds. In this scenario, a passenger train provides long-distance intercity commuter trips over a mixture of urban and suburban environments. In such a scenario the train is assumed to travel with average speeds of 100Km/h and reaching a maximum speed of 150Km/h over suburban areas. The communication networks that are involved in this scenario are GSM for operational voice and signalling messages (i.e., train operation specific communications), while overlapping 3G, 4G and 5G coverage (the latter offered only in city centres or in selected train stations) support voice and data communication needs of commuters on board.

The scenario is characterised by the highly mobility of the users, which results in frequent horizontal and vertical handovers. Depending on the percentage of RAT deployment and the security profile of the MNOs, the frequent handovers would be associated with equally frequent rekeying rates and TMSI allocation. Evidently, MNO-C will adopt such a behaviour, opposite to MNO-D, which tries to minimise such overhead. Due the characteristics of the scenario, all MNOs will be considered susceptible to integrity (***T3: Inject or Modify messages originated from the user***, ***T4: Modify (create/delete) messages originated from the network***) and privacy threats (***T7: Determine subscriber's id and location (tracking)***), associated with the heterogeneity of the networking environment and the highly user mobility. Particularly for ***T7)***, the *NAS* and *RRC* messages considered for the calculation of the threat probability, are those containing information specifically related to the subscriber's identity or location. In the XI of the paper, Table 6 lists the number of *NAS* and *RRC* messages considered in this scenario, while Table 9 includes the number of messages considered for the Privacy related threat [19], [73]–[76].

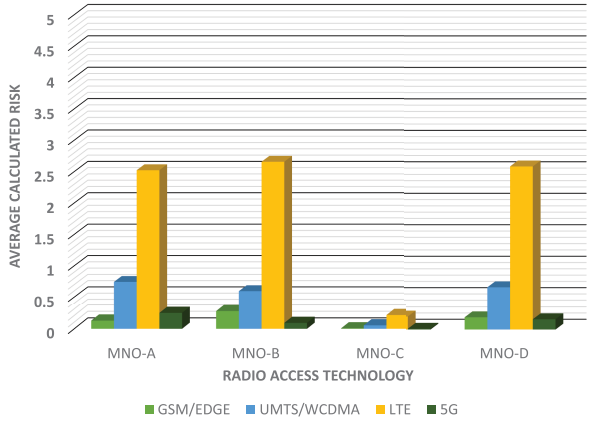
In the scenario of a high speed train commute, the MNOs are required to provide uninterrupted services to highly mobile users, utilising all deployed RATs over a typically large geographical areas. Hence, the impact of the probable attacks would have an impact over large areas and number of subscribers. Table 3 reveals a highly disperse of impact levels, particularly for ***T3*** and ***T4***, which reveals a wide range of consequences affecting technical, financial and business aspects of the MNO's operation. Figures 7a, 7b and 7c, illustrate the quantified risk. As speculated, MNO-C having adopted the most secure strategy, faces on average, a minimised risk compared to the rest of the MNOs. MNO-A and MNO-B, which have ratified a common security strategy, demonstrate a similar behavior dependant to the different technology mixture. The divergence of the probability, thus risk, between MNO-A and MNO-B is greater in ***T4*** than in ***T3*** and ***T7***, as this threat is related to more vulnerabilities that depend to the employed technology. MNO-D demonstrates the higher probability thus risk, as expected. Nonetheless, the risk of MNO-A and MNO-B appears to be closer to the risk value of MNO-D than the one of MNO-C. Even though MNO-A and MNO-B refresh their keys more frequently, both operators have not chosen secure algorithms like MNO-D. The comparison of the average calculated risk due to the three threats of this scenario reveals a slightly higher risk for ***T4***.



(a) ***T3: Inject or Modify messages originated from the user***



(b) ***T4: Modify (create/delete) messages originated from the network***



(c) ***T7: Determine subscriber's id and location (tracking)***

FIGURE 7. Assessment of Risk for each MNO profile in the High speed train commute scenario, across all Radio Access Technologies.

This outcome is justified both by the fact that ***T4*** emerges as a result of several vulnerabilities, which result in an augmented value for the probability and the fact that its impact ranges from *Critical* to *Highly Critical*.

C. RISK EVALUATION DURING MASSIVE PUBLIC EVENTS

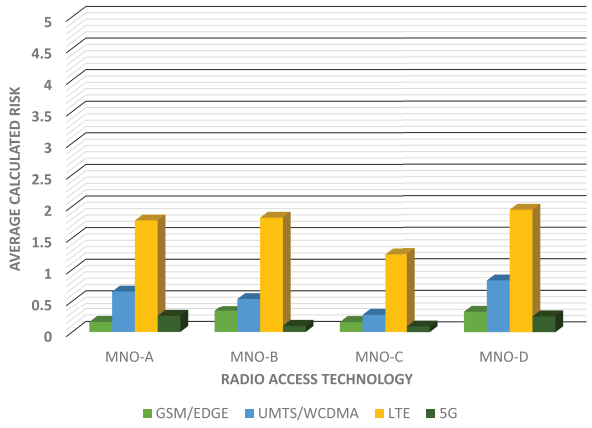
The massive public event scenario is characterised by extremely high traffic and service demands with highly irregular, seasonal spikes at massively dense hot-spots such as stadiums, concert halls, parks, etc. Therefore, MNOs need to ensure sufficient coverage and bandwidth provisioning for supporting efficiently an amalgam of telecommunication services. Such heterogeneous applications and services (i.e., over-the-top, on-demand, etc.) require ultra-high channel capacity at specific time windows (i.e., during a match, or concert), often with guaranteed QoS levels. Moreover, this networking environment poses unique security challenges to MNOs, due to the massive number of heterogeneous devices concurrently competing for resources, as well as, the need for additional hybrid RATs femto cells, often required for capacity provisioning, which may result in tilting off balance the security strategy of MNOs.

During a massive public event high capacity eMBB, mMTC and URLLC services need to be offered over heterogeneous RATs, which already provide coverage in the area or are being deployed specifically for the increased capacity needs of the event. In particular, fans/spectators will often compete for resources in order to upload high and ultra-high definition (UHD) videos to private clouds of social media, or use their mobiles devices UHD video streaming previous scenes, doubtful incidents (in case of sport events), etc. The provision of high-speed wireless data networks also provides the opportunity for live TV broadcast (IPTV) from media companies to fans at home. All these services are offered on top of regular operational related services of the venues (e.g., remote controlled high definition CCTV, wireless remote security cameras, sensors, etc.), which in turn compete over the same wireless resources. In addition, mMTC services would include push notification over large number of spectators/fans for advertisements, online contests, as well as IoT services over massively dense sensor networks across the venues. Finally, location-based services and other interactive services need to be provider to attendees and venue employees.

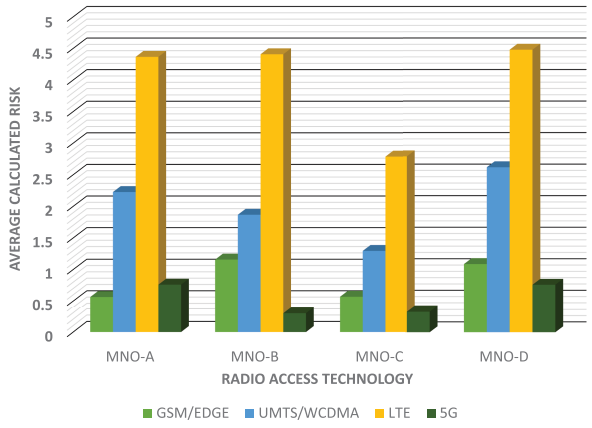
In this scenario, MNOs need to compensate for the scarce radio resources with deploying additional femto cells of different radio access technologies in the area. Moreover, the scenario assumes that MNOs will handle voice calls differently than data communications, in an effort to preserve capacity for demanding video services, or high priority traffic. Therefore, MNOs are interested to estimate the risk caused by the different threats affecting the availability and potentially the privacy. Figs. 8a, 8b and 8c illustrate the calculated risk associated with threats ***T5: Disable/Detach ME***, ***T6: Signaling DoS on the network*** and ***T9: Map an***

TABLE 6. Unprotected messages per generation according to [19], [73]–[76].

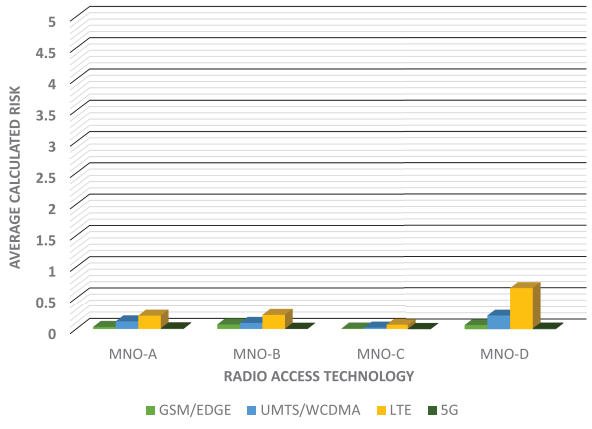
Protocol	Vulnerability	2G	3G	4G	5G
NAS	No encryption	-	3/59	3/59	4/49
RRC	No encryption	12/64	12/64	33/65	25/47
NAS	No integrity	-	17/59	17/59	14/49
RRC	No integrity	64/64 or 12/64	12/64	12/65	7/47



(a) ***T5: Disable/Detach ME***



(b) ***T6: Signaling DoS on the network***



(c) ***T9: Map an information to another information (i.e., identity mapping)***

FIGURE 8. Assessment of Risk for each MNO profile in the Massive public event scenario, across all Radio Access Technologies.

information to another information (i.e., identity mapping), respectively. As speculated, the probability value for ***T6*** is greater than the probability value for ***T5*** as ***T6*** is linked to more vulnerabilities. Interestingly, in a secure 5G integration (such as the one of MNO-A, MNO-B and MNO-C), the probability value of T5 is almost equal to the probability value of T6. The massive number of subscribers concentrated in a small area, in addition to the heterogeneity of the provided services, often associated with different security requirements that favor DoS attacks; hence ***T6*** pose a significantly greater risk to MNOs with an impact reaching to *Highly Critical* levels. The risk due to ***T9*** appears to be minor due to the limited number of unencrypted messages that include the RNTI, thus could lead to information mapping, in addition to the low impact of this threat. MNO-D divulge a greater risk value that the rest of the operators since the TMSI allocation is less frequent.

TABLE 7. Unencrypted messages for T7 per generation according to [19], [73]–[76].

Generation	Protocol	Message
3G	NAS	Attach Request (IMSI/TMSI, last visited TAI) Tracking Area Update Request (old GUTI, last TAI)
	RRC	Paging (IMSI or UE identity for later generations that do not support IMSI) RRC Connection Request (UE identity/TMSI) RRC Connection Setup (TMSI) RRC Connection Reject (TMSI)
4G	NAS	Attach Request (IMSI/TMSI, last visited TAI) Tracking Area Update Request (old GUTI, last TAI)
	RRC	Paging (IMSI or UE identity) RRC Connection Request (UE identity/TMSI) RRC Connection Setup Complete (TMSI) RRC Early Data Request (TMSI) RRC Connection Reestablishment Request (UE identity) RRC Connection Resume Request (UE identity)
5G	NAS	Registration Request (GUTI) N1 NAS signalling connection (TMSI)
	RRC	Paging (TAI) RRC Request (TMSI or TAI) RRC Setup Complete (TMSI)

XI. CONCLUSION

The area of cellular networks has been broadly investigated throughout the years, nevertheless there is limited research on procedures to calculate the risk of the MNO's, caused by the discovered vulnerabilities. This work presents a systematic, comprehensive and extensible methodology to estimate the risks associated with the access radio technologies currently deployed by MNOs. The analysis considers the vulnerabilities caused by the 3GPP specifications and the configurations of the MNO across all currently deployed network generations (2G, 3G, 4G) while can be also used in 5G. In addition to identifying the vulnerabilities and the associated threats, using attack trees, the paper proposes a number of countermeasures to mitigate the risks and minimise the impact of confidentiality, integrity, availability and privacy related threats. The risk assessment methodology involved an innovative mapping of the threats' impact severity with specific consequences spanning over both technical and business aspects of MNOs. The risk was assessed using three distinct scenarios (emergency call 112, high speed train commute, massive public event) that involved multiple MNOs with different security strategies and deployed RATs. The analysis of the results showcased the importance of the security strategy adopted by MNOs, particularly those that still support legacy RAT systems (GSM and UMTS based access). The security inefficiencies of such RATs do not only affect the specific networks and their subscribers, but propagate to RATs of later generations, despite the improved security levels of the latter.

TABLE 8. Unencrypted messages for T8 per generation according to [19], [73]–[76].

Generation	Protocol	Message
3G	NAS	Attach Request (UE network capability) Tracking Area Update Request (UE network capability) Security Mode Command (chosen ciphering/integrity algorithms)
	RRC	RRC Connection Setup (Capability update requirement) RRC Connection Setup Complete (UE system specific capability)
4G	NAS	Attach Request (UE network capability) Tracking Area Update Request (UE network capability) Security Mode Command (chosen ciphering/integrity algorithms)
	RRC	UE Capability Enquiry (UE capabilities) UE Capability Information (UE capabilities)
5G	NAS	Registration Request (UE security capability) Security Mode Command (algorithms)
	RRC	UECapabilityEnquiry (capabilities) UECapabilityInformation

TABLE 9. Unencrypted messages for T9 per generation according to [19], [73]–[76].

Generation	Protocol	Message
3G	RRC	Paging Type 1 PUSCH Capacity Request Physical Shared Channel Allocation) RRC connection Setup RRC connection Release (CCCH only)
4G	RRC	Paging RRC Connection Reestablishment Request RRC Connection Release RRC Connection Resume Request
5G	RRC	Paging RRC Reconfiguration RRC Reestablishment Request RRC Resume Request SIB1

The research outcomes of this research are not exhausted with considering heterogeneous RATs and the threats associated with these. This is an ongoing work that currently involves a systematic study of vulnerabilities and the risk they impose to 5G networks, specifically focusing on massive MIMO small cell and cell-free architectures. Such superfluidity-like networking and service provisioning cloud based architectures, pose security risks yet unknown to the research community, due to the varying spatial and temporal characteristics of novel cloud-native applications and cell-free ultra massive MIMO wireless access networks. Therefore, novel cybersecurity insurance strategies need to be introduced to cover for the emerging risks MNOs will face in the era of 5G and Beyond.

APPENDIX

See Tables 6–9.

REFERENCES

[1] P. Cerwall. (2020). *Adapting to New Realities*. https://www.ericsson.com/49da93/assets/local/mobility-report/documents/%2020/june2020-ericsson-mobility-report.pdf

[2] NIS Cooperation Group. (2019). *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*. Accessed: Aug. 25, 2020. [Online]. Available: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

[3] B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor, and K. R. B. Butler, "Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways," in *Proc. IEEE Symp. Secur. Privacy (SP)*, 2016, pp. 339–356.

[4] C. S. Yu Chuan and C. Zhiping, "LTE phone number catcher: A practical attack against mobile privacy," *Secur. Commun. Netw.*, vol. 2019, pp. 1–10, May 2019.

[5] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.

[6] (2016). *Regulation EU 2016/679 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (GDPR)*. Accessed: Aug. 25, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R06%79&from=EN

[7] (2002). *Directive 2002/21/ec on a Common Regulatory Framework for Electronic Communications Networks and Services(Framework Directive)*. Accessed: Aug. 25, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L00%21&from=en

[8] (2002). *Directive 2002/58/ec Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)*. Accessed: Aug. 25, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L00%58&from=EN

[9] (2016). *Directive EU 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*. Accessed: Aug. 25, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L11%48&from=EN

[10] (2019). *Cybersecurity of 5G Networks*. Accessed: Aug. 25, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019H05%34&from=EN

[11] Federal Communications Commission. (2016). *Fifth Generation Wireless Network and Device Security*. Accessed: Aug. 25, 2020. [Online]. Available: https://docs.fcc.gov/public/attachments/DA-16-1282A1.pdf

[12] *Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements (Release 4)*, document (TS) 21.133, version 4.1.0, 3rd Generation Partnership Project, 2001. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/21_series/21.133/21133-410.zip

[13] G. Stoneburner, A. Y. Goguen, and A. Feringa. (2002). *NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems*. Accessed: Aug. 25, 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01

[14] (2012). *NIST Special Publication 800-30 Revision 1 Guide for conducting Risk Assessments*. Accessed: Aug. 25, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-3%0r1.pdf

[15] *Ericsson Network Slicing*. Accessed: Aug. 25, 2020. [Online]. Available: https://www.ericsson.com/en/digital-services/trending/network-slicing

[16] *Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 8)*, document (TS) 33.401, 3rd Generation Partnership Project, Mar. 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/33_series/33.401/33401-831.zip

[17] *Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol Specification (Release 8)*, document TS 36.331, (3GPP), Jan. 2007. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/36_series/36.331/36331-100.zip

[18] *Security Architecture and Procedures for 5G System (Release 16)*, document TS 33.501, version 16.1.0, (3GPP), Dec. 2019. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/33_series/33.501/33501-g10.zip

[19] *Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 15)*, document TS 33.102, 3rd Generation Partnership Project, Dec. 2018, version 15.1.0. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/33_series/33.102/33102-f10.zip

[20] S. Rizou, E. Alexandropoulou-Egyptiadou, and K. E. Psannis, "GDPR interference with next generation 5G and IoT networks," *IEEE Access*, vol. 8, pp. 108052–108061, 2020.

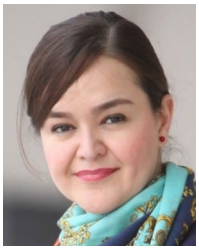
[21] Council of European Union. (2018). *Directive 2018/1972 Establishing the European Electronic Communications Code*. Accessed: Aug. 25, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L197%2&from=EN

[22] NIS Cooperation Group. (2020). *Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures*. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-net%works-eu-toolbox-risk-mitigating-measures
[23] ETSI. (Dec. 2017). *Cyber; Implementation of the Network and Information Security (NIS) Directive*. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/t%r_103456v010101p.pdf
[24] *Technical Specification Group Service and System Aspects; Security of H(e)NB; (Release 8)*, document TR 33.820 version 8.3.0, (3GPP), Dec. 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/33_series/33.820/33820-830.zip
[25] *Technical Specification Group Services and System Aspects; Study on the Security Aspects of the Next Generation System (Release 14)*, document TR 33.820 version 1.3.0, (3GPP), Aug. 2017. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/33_series/33.899/33899-130.zip
[26] *Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 9)*, document TS 33.102, 12 2009 version 9.1.0, 3rd Generation Partnership Project, Dec. 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/33_series/33.102/33102-910.zip
[27] J. J. Cichonski and M. Bartock. (Dec. 2017). *Guide to LTE Security*. Accessed: Aug. 25, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.p%dfp
[28] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.
[29] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and C. Pöpper, "On security research towards future mobile network generations," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2518–2542, 3rd Quart., 2018.
[30] L. He, Z. Yan, and M. Atiquzzaman, "LTE/LTE-a network security data collection and analysis for security measurement: A survey," *IEEE Access*, vol. 6, pp. 4220–4242, 2018.
[31] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A systematic approach for adversarial testing of 4G LTE," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2018, pp. 1–8.
[32] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2019, pp. 669–684.
[33] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking LTE on layer two," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1–5.
[34] T. Byrd, V. Marojevic, and R. P. Jover, "CSAI: Open-source cellular radio access network security analysis instrument," in *Proc. 91st Veh. Technol. Conf.*, May 2020, pp. 1–5.
[35] GSM security country report: Greece. (2012). *Security Research Labs Berlin*. Accessed: Aug. 25, 2020. [Online]. Available: https://gsmmap.org/assets/pdfs/gsmmap.org-country_report-Greece-2012-03%.pdf
[36] C. Xenakis, C. Ntantogian, and O. Panos, "(U)SimMonitor: A mobile application for security evaluation of cellular networks," *Comput. Secur.*, vol. 60, pp. 62–78, Dec. 2016.
[37] M. Chlosta, D. Rupprecht, T. Holz, and C. Pöpper, "LTE security disabled-misconfiguration in commercial networks," in *Proc. Conf. Secur. Privacy Wireless Mobile Netw.*, 2019, pp. 261–266.
[38] P. A. Abdulla, J. Cederberg, and L. Kaati, "Analyzing the security in the GSM radio network using attack jungles," in *Proc. Int. Symp. On Leveraging Appl. Formal Methods, Verification Validation*, 2010, pp. 60–74.
[39] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl, "Security requirements for automotive on-board networks," in *Proc. 9th Int. Conf. Intell. Transp. Syst. Telecommun. (ITST)*, 2009, pp. 64–641.
[40] C. Xenakis, D. Apostolopoulou, A. Panou, and I. Stavrakakis, "A qualitative risk analysis for the gprs technology," in *Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput.*, vol. 2, 2008, pp. 61–68.
[41] *Technical Specification Group Service and System Aspects; Access Security Review (Release 7)*, document TR 33.801 version 1.0.0, (3GPP), May 2012. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/33_series/33.801/33801-100.zip
[42] *Technical Specification Group Services and system Aspects; Security related network functions (Release 15)*, document TS 43.020, version 15.0.0, (3GPP), Jun. 2018. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDeta%ils.aspx?specificationId=2663
[43] *Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)*, document TS 24.301, version 12.9.0, (3GPP), Jun. 2015. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/24_series/24.301/24301-c90.zip
[44] *Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 15)*, document TS 33.401 version 15.7, (3GPP), Mar. 2019. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/33_series/33.401/33401-f70.zip
[45] *Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification (Release 15)*, document TS 35.206, version 15.0.0, (3GPP), Nov. 2018. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/35_series/35.206/35206-f00.zip
[46] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of gsm encrypted communication," in *Proc. 23rd Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, vol. 2729, Aug. 2003, pp. 600–616. [Online]. Available: https://iacr.org/archive/crypto2003/27290598/27290598.pdf
[47] *A5/1 Decryption Tool, SRLabs*. Accessed: Aug. 25, 2020. [Online]. Available: https://opensource.srlabs.de/projects/a51-decrypt
[48] N. Paglieri and O. Benjamin. (Jun. 2011). *Implementation and Performance Analysis of Barkan, Biham and Keller's Attack on A5/2*. Accessed: Aug. 25, 2020. [Online]. Available: https://www.npag.fr/project-a52hacktool
[49] H. Kim, J. Lee, E. Lee, and Y. Kim, "Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane," in *Proc. IEEE Symp. Secur. Privacy (SP)*, 2019, pp. 1153–1168.
[50] *Technical Specification Group Services and system Aspects; Security related network functions (Release 4)*, document TS 43.020, version 4.0.0, (3GPP), Nov. 2000. [Online]. Available: https://web.3gpp.org/tsg_sa/WG3_Security/_Specs/Old_Vsns/43020-400.pdf
[51] *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 5: Design and Evaluation Report*, document TR 33.401, (ETSI), Feb. 2006. [Online]. Available: https://www.academia.edu/7970944/ETSI_SAGE_Technical_report_Version_1_0%_Date_6_th_February_2006_Specification_of_the_3GPP_Confidentiality_and_Integri%ty_Algorithms_UEA2_and_UIA2_Document_5_Design_and_Evaluation_Report
[52] *Ericsson 3GPP Release 15: An End to the Battle Against False Base Stations*. Accessed: Aug. 25, 2020. [Online]. Available: https://www.ericsson.com/en/blog/2019/1/3gpp-release15
[53] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J. Seifert, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2016, pp. 1–5.
[54] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2019, pp. 24–27
[55] B. Hong, S. Bae, and Y. Kim, "GUTI reallocation demystified: Cellular location tracking with changing temporary identifier," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2018, pp. 1–5
[56] *Technical Specification Group Services and System Aspects; Specification of the GIA4 integrity algorithm for General Packet Radio Service (GPRS); Design conformance test data Release 15*, document TS 55.243, version 15.0.0, (3GPP), Jun. 2018. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/55_series/55.243/55243-f00.zip
[57] *Technical Specification Group Services and System Aspects; Specification of the GEA5 and GIA5 encryption algorithms for General Packet Radio Service (GPRS); GEA5 and GIA5 algorithm specification (Release 15)*, document TS 55.251, version 15.0.0, (3GPP), Jun. 2018. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/55_series/55.251/55251-f00.zip
[58] M. Ramadan, F. Li, C. X. Xu, A. Abdalla, and H. Abdalla, "An efficient end-to-end mutual authentication scheme for 2g-gsm system," in *Proc. IEEE Int. Conf. Big Data Anal. (ICBDA)*, Dec. 2016, pp. 1–6.
[59] A. Shaik, R. Borgaonkar, S. Park, and J. P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: Exposing device capabilities," in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw.*, 2019, p. 221–231.
[60] N. Golde, K. Redon, and J. P. Seifert, "Let me answer that for you: Exploiting broadcast information in cellular networks," in *Proc. 22nd USENIX Secur. Symp.*, 2013, pp. 33–48.
[61] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on LTE," in *Proc. 28th Secur. Symp.*, 2019, pp. 55–72.
[62] E. R. M. Arapinis, L. I. Mancini, and M. Ryan, "Privacy through pseudonymity in mobile telephony systems," in *Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2014, pp. 1–8.

[63] M. Khan and C. J. Mitchell, "Trashing IMSI catchers in mobile networks," in *Proc. 10th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2017, pp. 207–218.
[64] *Technical Specification Group Core Network and Terminals; Numbering, addressing and identification (Release 15)*, document TS 23.003, version 15.7.0, (3GPP), Jun. 2019. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/23_series/23.003/23003-f70.zip
[65] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, 2014, p. 246–255.
[66] V. Saini, Q. Duan, and V. Paruchuri, "Threat modeling using attack trees," *J. Comput. Sci. Colleges*, vol. 23, no. 4, pp. 124–131, 2008.
[67] B. Schneier, "Attack trees," *Dr. Dobb's J.*, vol. 24, no. 12, pp. 21–29, 1999.
[68] D. F. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, "Location leaks on the GSM air interface," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2012, pp. 1–8.
[69] *IMT Vision Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond*, document ITU-Recommendation M 2083, Int. Telecommun. Union, Geneva, Switzerland, 2015.
[70] Ericsson. (2020). *Ericsson Mobility Visualizer*. [Online]. Available: https://www.ericsson.com/en/mobility-report/mobility-visualizer?f=1&ft%=2&r=5&t=1,2,3,4&s=4&u=1&y=2018,2022&c=1
[71] E. K. Markakis, I. Politis, A. Lykourgiotis, Y. Rebahi, G. Mastorakis, and C. X. Mavromo, "Efficient next generation emergency communications over multi-access edge computing," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 92–97, Nov. 2017.
[72] I. Politis, A. Lykourgiotis, C. Tselios, and T. Orfanoudakis, "On measuring the efficiency of next generation emergency communications: The emynos paradigm," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dec. 2018, pp. 1–6.
[73] *Technical Specification Group Radio Access Network; NR; Radio Resource Control (RRC) Protocol Specification (Release 16)*, document TS 38.331, version 16.0.0, (3GPP), Mar. 2020. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDeta%ils.aspx?specificationId=3197
[74] *Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3; (Release 16)*, document TS 24.501, 3 2020, version 16.4.1, (3GPP), May 2002. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDeta%ils.aspx?specificationId=3370
[75] *Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (Release 16)*, document TS 36.331, version 16.0.0, (3GPP), Mar. 2020. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDeta%ils.aspx?specificationId=2440
[76] *Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 16)*, document TS 24.301, version 16.4.0, (3GPP), Mar. 2020. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDeta%ils.aspx?specificationId=1072

ANNA ANGELOGIANNI (Graduate Student Member, IEEE) received the B.Sc. degree in digital systems and the M.Sc. degree in digital systems security from the University of Piraeus, Greece, in 2016 and 2018, respectively. She was an Exchange Student with the Department of Computer and System Sciences (DSV), Stockholm University, in 2015. She is currently a Ph.D. Researcher with the Systems Security Lab (SSL), Department of Digital Systems under the supervision of Prof. C. Xenakis and a member of the Systems Security Laboratory. She has been involved in several EU H2020 and Greek state funded projects. Her research interests include network and systems security, privacy, and forensics.

ILIAS POLITIS (Member, IEEE) received the B.Sc. degree in electronic engineering from Queen Marry College, London, U.K., in 2000, the M.Sc. degree in mobile and personal communications from King's College London, U.K., in 2001, and the Ph.D. degree in multimedia communications from the University of Patras, Greece, in 2009. He is currently a Senior Researcher with the Department of Digital Systems, University of Piraeus, and a member of the Systems Security Laboratory. His previous positions include the Senior Researcher at the Wireless Telecommunications Laboratory of the Electrical and Computer Engineering, University of Patras, and the School of Science and Technology, Hellenic Open University. He has been actively involved in all phases of several H2020 and FP7 framework projects. His research interests include future internet and next generation networks (5G and beyond), contextual awareness, and network security, where he has published more than 90 journals and conferences.



FARNAZ MOHAMMADI (Student Member, IEEE) studied computer software engineering and received the master's degree in computer science intelligent systems from the Amirkabir University of Technology (Tehran Polytechnic). She gained over ten years of experience later in Security and Access Control systems development, maintenance, and deployment while she worked as a Technical Team Member in an Iranian-Swedish company. In addition to her technical skills, she was later promoted to the Technical Team Manager and assisted the technical support as a Security System Consultant. She was a Junior Researcher with the System Security Laboratory, Department of Digital Systems, University of Piraeus, Greece, from 2017 to 2020, under the supervision of Prof. C. Xenakis. She is currently a Ph.D. Research Assistant with the Passau Institute of Digital Security, University of Passau, and she works under the Chair of IT-Security Prof. J. Posegga in Germany. Her research interests include network security, IoT-security, and AI.

CHRISTOS XENAKIS (Member, IEEE) received the B.Sc. degree in computer science, the M.Sc. degree in telecommunication and computer networks, and the Ph.D. degree from the Department of Informatics and Telecommunications, University of Athens, Greece, in 1993, 1996, and 2004, respectively. From 1998 to 2001, he was with a Greek Telecoms System Development Firm, where he was involved in the design and development of advanced telecommunications subsystems. From 1996 to 2007, he was a member of the Communication Networks Laboratory, University of Athens. Since 2007, he has been a Faculty Member of the Department of Digital Systems, University of Piraeus, Greece, where he is currently a Professor, a member of the Systems Security Laboratory, and the Director of the Postgraduate Degree Programme on "Digital Systems Security". He has participated in numerous projects realized in the context of EU Programs (ACTS, ESPRIT, IST, AAL, DGHOME, Marie Curie, and Horizon2020) as well as National Programs (Greek). He is also the Project Manager the CUREX, SECONDO, INCOGNITO, and SealedGRID projects, funded by Horizon2020, while he was the Project Manager of the ReCRED project funded by Horizon 2020 and the Technical Manager of the UINFC2 project funded by DGHOME/ISEC. He is also a Steering Committee member of the European Cyber Security Challenge (ECSC) and the Leader of the Hellenic Cyber Security Team. He is also a member of the editorial board of three Thomson Reuters indexed journals: *Computers & Security* journal (Elsevier), *Computer Communications* journal (Elsevier), and *IET Information Security* (Institute of Engineering and Technology). He has authored more than 100 papers in peer-reviewed journals and international conferences. His research interests include systems, networks, and applications security.