Review

Challenges and Opportunities in Mobile Network Security for Vertical Applications: A Survey

Álvaro Sobrinho * , Matheus Vilarim , Amanda Barbosa , Edmar Candeia Gurjão , Danilo F. S. Santos , Dalton Valadares , Leandro Dias da Silva

Posted Date: 22 December 2023

doi: 10.20944/preprints202312.1703.v1

Keywords: &nbsp;5G; security; privacy; vertical applications&nbsp;

Article

Challenges and Opportunities in Mobile Network Security for Vertical Applications: A Survey

Álvaro Sobrinho [1,*], Matheus Vilarim [2], Amanda Barbosa [2], Edmar Candeia Gurjão [2], Danilo F. S. Santos [2], Dalton Valadares [3] and Leandro Dias da Silva [4]

[1] Federal University of the Agreste of Pernambuco, Av. Bom Pastor, Garanhuns 55292-270, Pernambuco, Brazil
[2] Federal University of Campina Grande, R. Aprígio Veloso, Campina Grande, Brazil; matheus.vilarim@ee.ufcg.edu.br; amanda.silva@ee.ufcg.edu.br; edmar.gurjao@embedded.ufcg.edu.br; danilo.santos@dee.ufcg.edu.br
[3] Federal Institute of Pernambuco, Estrada do Alto do Moura, Caruaru, Brazil; dalton.valadares@caruaru.ifpe.edu.br
[4] Federal University of Alagoas, Campus A. C. Simões, Maceió, Brazil; leandrodias@ic.ufal.br
* Correspondence: alvaro.alvares@ufape.edu.br

Abstract: Ensuring the security of vertical applications in fifth-generation (5G) mobile communication systems and previous generations is crucial. These systems must prioritize maintaining the confidentiality, integrity, and availability of services and data. Examples of vertical applications include smart cities, smart transportation, public services, Industry 4.0, smart grids, smart health, and smart agriculture. Each vertical application has specific security requirements and faces unique threats within the mobile network environment. Thus, it is essential to implement comprehensive and robust security measures. This approach helps minimize the attack surface and effectively manage risks. This survey thoroughly examines mobile networks and their security challenges in vertical applications, shedding light on associated threats and potential solutions. Our study considers the interplay between security considerations in 5G, legacy networks, and vertical applications. We emphasize the challenges, opportunities, and promising directions for future research in this field and the importance of securing vertical applications in the evolving landscape of mobile technology.

Keywords: 5G; security; privacy; vertical applications

1. Introduction

Ensuring the Confidentiality, Integrity, and Availability (CIA) triad is pivotal for strengthening the reliability of fifth-generation (5G) mobile communication systems and previous generations. However, safeguarding the CIA triad within mobile networks introduces challenges [1]. These challenges are further compounded by the diverse range of vertical applications, each requiring specific security and privacy measures [2]. Various verticals, including smart cities, smart transportation, public services, Industry 4.0, smart grids, smart health, and smart agriculture, showcase the extensive application domains facilitated by 5G and previous generations [3].

Moreover, numerous technologies, including massive Multiple-Input/Multiple-Output (MIMO), Multi-Access Edge Computing (MEC), Software Defined Networks (SDN), Network Function Virtualization (NFV), and Network Slicing (NS), are relevant when incorporated into the architectural framework of the latest generation of mobile networks [4]. These technologies offer essential attributes for various applications, such as low latency, high reliability, extensive connectivity, and high-capacity broadband capabilities. Understanding these systems' potential threats and vulnerabilities becomes essential as these technological infrastructures and components integrate with vertical applications. Furthermore, it is crucial to apply new security paradigms to address the specific security challenges in each scenario.

Security concerns in 5G are heightened due to the software-based nature of many components, significantly expanding attack surfaces and necessitating robust cybersecurity measures. The dynamic nature of networks, facilitated by virtualization, enhances their flexibility and introduces potential vulnerabilities. Attacks targeting these virtualized components can compromise the integrity of the network. Consequently, cybersecurity has emerged as a critical priority for the successful and secure implementation of 5G. Nevertheless, legacy network infrastructures will coexist with 5G network infrastructure for many years [5], given the high costs of upgrading and replacing devices. Vulnerabilities of legacy networks can be used as a backdoor to attack 5G networks [6].

1.1. Related Works

Research focusing on security and privacy is essential for instilling confidence in mobile networks among various stakeholders, including industries, governments, and scientific communities. Khan et al. [4] addressed general security and privacy concerns, emphasizing key 5G technologies such as SDN, NFV, and NS. Sullivan et al. [7] provided a comprehensive overview of 5G security and the technologies designed to ensure its robustness. Tanveer et al. [8] conducted an in-depth exploration of the 5G network architecture, emphasizing crucial performance indicators compared to previous and upcoming generations of cellular networks. Tang et al. [9] conducted a comprehensive review of the novel features of 5G technology. Additionally, Khan and Martin [10] undertook a thorough examination of the current state of sign-up/subscription privacy in 5G networks.

Varga et al. [11] addressed challenges and proposed solutions concerning integrating 5G with industrial Internet of Things (IoT) applications. Wijethilaka and Liyanage [12] conducted a comprehensive analysis of NS implementation in the context of IoT. Wazid et al. [13] provided an in-depth exposition on the essential network and threat models required for the communication environment in IoT-enabled systems. Sanchez-Gomez et al. [14] conducted a detailed analysis of critical aspects of low-power wide area network security, emphasizing network access and the intersection of 5G and IoT.

Sharma et al. [15] conducted an extensive review focusing on securing industrial IoT devices and contributing to developing security methods employed in 5G and blockchain environments. Zhang et al. [16] presented a comprehensive summary of current end-to-end secure communication scenarios and fundamental techniques. Liu et al. [17] conducted an extensive survey covering various aspects of the security of 5G-IoT in the context of smart agriculture. Ahad et al. [18] discussed technology trends and security considerations for 5G-IoT-based smart health applications. Hui et al. [19] provided a review of the applications of 5G-IoT in the context of smart grids, with a specific focus on security and privacy.

Ogbodo et al. [20] analyzed the security aspects of 5G-enabled smart cities, specifically within the context of 5G, low-power wide-area networks, and IoT. Hakak et al. [21] conducted a study on smart vehicles in the context of 5G technology and security. Qiu et al. [22] briefly highlighted the security requirements of 5G vertical applications such as smart manufacturing, smart traffic, smart grid, and smart campus. Their primary focus, however, was on the three main 5G pillars, namely Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communications (URLLC), and massive Machine Type Communications (mMTC), along with a use case related to Industry 4.0. These studies contribute valuable insights into the security considerations of 5G-enabled smart cities, smart vehicles, and various vertical applications.

1.2. Contributions

The current literature does not provide a thorough survey that addresses the security and privacy concerns associated with 5G, legacy mobile networks, and vertical applications. Current surveys concentrate on individual technologies or a vertical rather than comprehensively analyzing the broader security and privacy landscape.

Furthermore, our research builds upon and extends the discussions presented in prior studies, notably the surveys conducted by Khan et al. [4] and Qiu et al. [22]. Consequently, the contributions of our article can be summarized: (1) we explore the security aspects of legacy networks and vertical applications; (2) we explore the security aspects of 5G networks; (3) we fill a gap in the literature by reviewing security aspects regarding various technologies and vertical applications; and (4) based on our findings, we present attack scenarios and attack-defense trees for 5G vertical applications.

1.3. Outline of the Article

The remainder of this article is structured as follows. Section 2 discusses the security aspects of legacy mobile networks, specifically in the context of vertical applications. Section 3 examines the security aspects of 5G in vertical applications. Section 4 presents the challenges and potential solutions concerning privacy in vertical applications. Section 5 outlines discussions and prospects for future research. Finally, Section 6 offers a conclusive summary of the paper's findings and contributions.

2. Security of Legacy Mobile Networks in Vertical Applications

2.1. Security of Vertical Applications in 2G

2G networks are based on Global System for Mobile Communications (GSM) technology and are used in applications requiring broad signal coverage, low cost, and low data transmission. Some usage scenarios of GSM networks include electronic security systems [23], remote monitoring of small dynamic quantities [24], agriculture [25], healthcare [26,27], industry [28], and tracking [29].

The absence of security measures during the connection to fixed networks is an example of a problem that makes communication and signaling traffic vulnerable. Moreover, the technology cannot effectively detect and neutralize active attacks, such as identity theft, establishing fake base transceiver stations, and eavesdropping [30].

Therefore, 2G network vulnerabilities put vertical applications at risk. Table 1 presents some threats to 2G networks. For instance, attackers can exploit a relatively non-complex form of unilateral authentication. The GSM network can enable operators to employ algorithms such as A3 and A8 [31]. However, extensive analysis has exposed numerous security vulnerabilities within the algorithm's design or implementation, compromising the confidentiality and integrity of the authentication process [32].

Table 1. Some threats related to 2G networks.

Threats	Description	Vulnerabilities
Espionage and collection	An attacker can eavesdrop on communication and collect information about the user's equipment, equipment capabilities (supported encryption algorithms), or signature.	Lack of encryption in certain signaling messages.
Redirection, discarding, and creation	An attacker can redirect, discard, or create calls/messages/authentication vectors.	Lack of mutual authentication in the context of 2G; lack of encryption in certain signaling messages; lack of integrity in signaling messages in the context of 2G; weak encryption algorithms (e.g., A5/1); lack of additional countermeasures for weak encryption algorithms.
Disabling or detaching user equipment	An attacker can disable or detach user equipment from the network.	Lack of mutual authentication; lack of encryption in certain signaling messages; lack of integrity; weak encryption algorithms (e.g., A5/1); lack of additional countermeasures for weak encryption algorithms.
Eavesdropping with access or listening	An attacker can eavesdrop on communication and subsequently access a message (SMS or packet) or listen to a call.	Weak encryption algorithms (e.g., A5/1); lack of network authentication by the user.

These weaknesses can allow attackers to gain unauthorized access or manipulate authentication mechanisms. Other examples of vulnerabilities include [33]: SIM card cloning, over-the-air cracking, flaws in cryptographic algorithms, short-range protection, lack of client perceptibility, user anonymity leakage, absence of integrity protection, and increased redundancy due to coding preference.

2.2. Security of Vertical Applications in 3G

Wideband Code Division Multiple Access (WCDMA), High-Speed Packet Access (HSPA), and Evolved High-Speed Packet Access (HSPA+) are technologies that emerged in the 3G architecture. Consequently, they provide enhanced data transmission capabilities [34]. Examples of applications include smart home security [35], intelligent image monitoring system [36], water resource monitoring system [37], telemedicine systems [38], remote control system for aerial vehicles [39], vehicle monitoring system [40], bridge monitoring system [41], intelligent electrical workplace security monitoring [42], video service [43], and streaming applications [44].

The growth of 3G networks has enabled a wide range of services, making security-related issues more evident. With the transition to Internet Protocol (IP)-based services, a broader field of applications emerged. However, security challenges also increased as using IP-based networks introduces threats such as viruses and user information theft.

The Authentication and Key Agreement (AKA) protocol has been adopted for access security in 3G networks. However, the techniques used in 3G networks have not been able to authenticate securely, presenting several vulnerabilities. Table 2 presents examples of threats that can be observed in 3G networks. For instance, mobile users are not authenticating in the Serving Network (SN) and not authenticating between the SN and the home network in the wired network. This allows authentication messages to be easily captured and modified during Man-in-the-Middle (MitM) attacks [45].

Table 2. Some threats to 3G networks.

Threats	Description	Vulnerabilities
Redirection, dropping, and injection	An attacker can redirect, drop, or inject calls or messages (SMS or packets).	Lack of integrity in user data messages and certain signaling messages.
Location retrieval	An attacker can retrieve the subscriber's location using the IMSI, TMSI/GUTI, and optionally, the TAI.	Lack of encryption in certain signaling messages, i.e., RRC connection and paging messages; infrequent TMSI/GUTI allocation; and allocation of IMSI instead of TMSI.
Inference mapping	An attacker can inferentially map information between different sources.	There is a lack of encryption in certain RRC signaling messages, pre-authentication traffic, and infrequent TMSI/GUTI allocation.
Denial of Service and QoS degradation attacks	An attacker can successfully perform a DoS attack against the network by impersonating a legitimate user. This attack makes a network resource unavailable, interfering or temporarily/definitively disrupting the service.	Lack of encryption in certain RRC signaling messages; lack of integrity in certain signaling messages; weak encryption algorithms (e.g., A5/1 or A5/2); infrequent AKA allocation; and infrequent TMSI/GUTI allocation.

2.3. Security of Vertical Applications in 4G

Long Term Evolution (LTE) technology has transformed mobile communications with its capability to support multimedia content, nearly real-time communication, and internet connectivity. Applications include remote system control [46], communication systems for drones [47,48], augmented reality [49], high-definition live video streaming [50], telemedicine [51], and smart grid communications [52].

The fully IP-based architecture of 4G networks and the new features introduced in this generation have brought new security challenges. Table 3 presents some threats to 4G networks. Some vulnerabilities from previous generations have been inherited by 4G networks. Attacks on data integrity, Denial of Service (DoS) attacks, unauthorized access, and location tracking are some of the issues identified in networks based on LTE [53].

Table 3. Some threats to 4G networks.

Threats	Description	Vulnerabilities
DoS and QoS degradation attacks	An attacker can successfully launch a DoS attack on the network by impersonating a legitimate user.	Lack of encryption in certain RRC signaling messages; lack of integrity in certain signaling messages; rare allocation of AKA; and rare allocation of TMSI/GUTI.
UE or base station impersonation	The 5G NR specifications also use an RRC and NAS protocol architecture very similar to LTE, and therefore, an attacker can impersonate UE or a base station, collect all broadcast information, such as EARFCN, PCI, ECGI of neighboring cells, and thus impersonate authentic network elements.	Traditional IMS servers designed for VoIP do not validate the subscriber identifier in received call setup requests, allowing an attacker to impersonate other subscribers; IP address and SIP header can be falsified due to lack of protection mechanisms; lack of sufficient control to authorize X2 interface establishment.
Forced network technology downgrading for the user	An attacker can force the UE to use a communication technology older than 5G, downgrading the communication security level.	Absence of protection mechanisms in handover between different generation networks; the possibility of requesting UE radio access capabilities before RRC security configuration; the *Attach Request* message is sent unencrypted by the UE to the network; UE registration process is not interrupted even if integrity verification fails at the MME.

3. Security of 5G Networks in Vertical Applications

3.1. 5G General Threats

Categorizing threats to 5G networks using the CIA triad can offer an overview of the general challenges involved. We identified various threats during our survey, and the upcoming sections highlight some of them.

3.1.1. Confidentiality

Table 4 presents some examples of confidentiality threats. For instance, relevant information can be obtained passively by accessing and analyzing data transmitted in plaintext over the network. If credentials or access keys are stolen, encryption algorithms are compromised, privilege escalation is executed, lateral movement occurs, or an insider facilitates unauthorized access, confidential information can be obtained actively.

Table 4. Examples of threats to confidentiality in 5G networks.

Threats	Architectural Part Affected	Risks
Perform Unauthorized Access to Confidential Data [54,55]	RAN, MEC, NG-CORE	Extortion, Data Privacy Violation Through Misuse and Disclosure
Analyze Air Interface Traffic [56,57]	RAN	Theft of Access Credentials, User Identifiers, and Location Parameters
Perform Data Leakage [58]	MEC	Personal, Corporate or Financial Damages
Extract Private Information of Other Users Using a Shared Service in an Unauthorized Manner [58]	MEC, NG-CORE	Information Disclosure
Eavesdrop Messages to Legitimize Users [59]	RAN	Identity Forgery
Sniffing the Physical Broadcast Channel (PBCH) [60]	RAN	Collection of Base Station and User Equipment Information
Unauthorized Access to Home Subscriber Server to Steal User Parameters [61]	NG-CORE	Identity Forgery
Use Software to Compromise Encryption Algorithms (ex. compromise the advanced encryption standard) [61]	RAN, MEC, NG-CORE	Exposure of Critical Information
Use Application Instance to Intercept Traffic Flows or Perform Black Holes [62]	MEC	Leakage or Loss of Information
Intercept a Key [63]	RAN, NG-CORE	Exposure of Critical Information
Identify a Subscriber's Identity [63]	RAN, NG-CORE	Identity Forgery
Track a Subscriber's Location [63]	RAN, NG-CORE	Information Disclosure

3.1.2. Integrity

Table 5 presents some examples of integrity threats. For instance, false synchronization signal transmissions threaten the 5G Radio Access Network (RAN), which is used to gather critical information and disrupt the proper functioning of communication services. The Quality of Service *(QoS) in 5G networks can be degraded, and harmful actions can be carried out on the systems, altering traffic, data, or controller functions.

Table 5. Examples of threats to integrity in 5G networks.

Threats	Architectural Part Affected	Risks
Maliciously Use Legitimate Access to the Orchestrator [58]	RAN, MEC, NG-CORE	Manipulate the Configuration and Run a Compromised Network Function
Tampering of Data [54]	RAN, MEC, NG-CORE	Create Network Congestion for Performance Degradation
Modify Traffic [64]	RAN, MEC, NG-CORE	Create Network Congestion for Performance Degradation
Change Network Elements Configuration Using the Management Interface [58]	RAN	Route Switching, Packet Dropping, and Data Inteception
Transmit False Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS) [60]	RAN	Getting UEs Information and Network Configuration Parameters
Spoofing the Physical Broadcast Channel (PBCH) [60]	RAN	Misconfiguration of Parameters for Establishing Communication on the Channel
Spoof the Physical Random Access Channel (PRACH) [60]	RAN	Pejudicate the Transport of Random Access Preamble from the UE to the gNB
Reprogram or Attack Controller Functions [61]	RAN, MEC, NG-CORE	Malfunctioning or Unavailability of Services
Send Forged or Spoofed Traffic Streams [65]	UE, MEC	Overloading of Services, Interruption or Malfunctioning of Applications
Calculate Valid session Keys to Reproduce the Same Message [66]	NG-CORE	Breach of confidentiality, Forgery or Impersonation
Take Advantage of a Fake or Unauthorized MEC Gateway [67]	MEC	Packet hijacking, Information theft, Application Malfunctioning
Spoof DNS Servers and IP Addresses to Spread Viruses [68]	UE, RAN, MEC, NG-CORE	Malicious Code Installation, Host Hijacking, Network Device Infection

3.1.3. Availability

Table 6 presents some examples of availability threats. For instance, an attacker may choose one or several architectural components to form their network exploitation strategy. Malicious actions, whether known or unknown, may be carried out with the intent to conduct DoS, function degradation or interruption, and hijacking applications or devices to alter configurations and introduce malicious code.

Table 6. Examples of threats to availability in 5G networks.

Threats	Architectural Part Affected	Risks
Take Advantage of Malicious Insiders Attacks [58]	RAN, MEC, NG-CORE	Inject Malicious Code, Infect Devices with Malware, and Intentional Misconfigurations of Devices
Perform Resource Exhaustion [13]	RAN	Generate Destructive Interference
Make Services Unavailable [67]	RAN, NG-CORE	Unavailability of Critical Parts of the System Can Interrupt the Entire Service of a Coverage Area
Perform Attacks for Resource Shortages [58]	RAN	Unavailable or Scarce Resources for Legitimate Applications or Devices
Use North and South Boundary Interfaces to Attack the SDN Controller [58]	RAN, MEC, NG-CORE	Misconfigurations, Malicious Code or Instance of Application
Communication Channels Attacks [59,60]	RAN	Block the Physical Broadcast Channel (PBCH), Block the Physical Downlink Control Channel (PDCCH), and Block Uplink or Downlink Signal (Data Plane)
Use Application Instance to Perform Black Holes [60]	MEC	Redirect or Interrupt Data Traffic
Attack Open Edge APIs [67]	MEC	Disable or Impair Services that Need Edge Processing for Low Latency
Disable IoT Device Power Saving Abilities [68]	UE	Reduced Battery Life, Shutdown of Devices with Only the Battery as Power Source, Overheating Can Lead to Poor Device Performance
Attack the Weakest Link of Heterogeneous 5G Networks [56]	RAN, MEC, NG-CORE	Partial or total interruption of the network, a Single Fragile Part in the Security of the System Can Impact the Rest of the Architecture that a Priori Would Be Well Protected

3.2. 5G Vertical Applications Threats

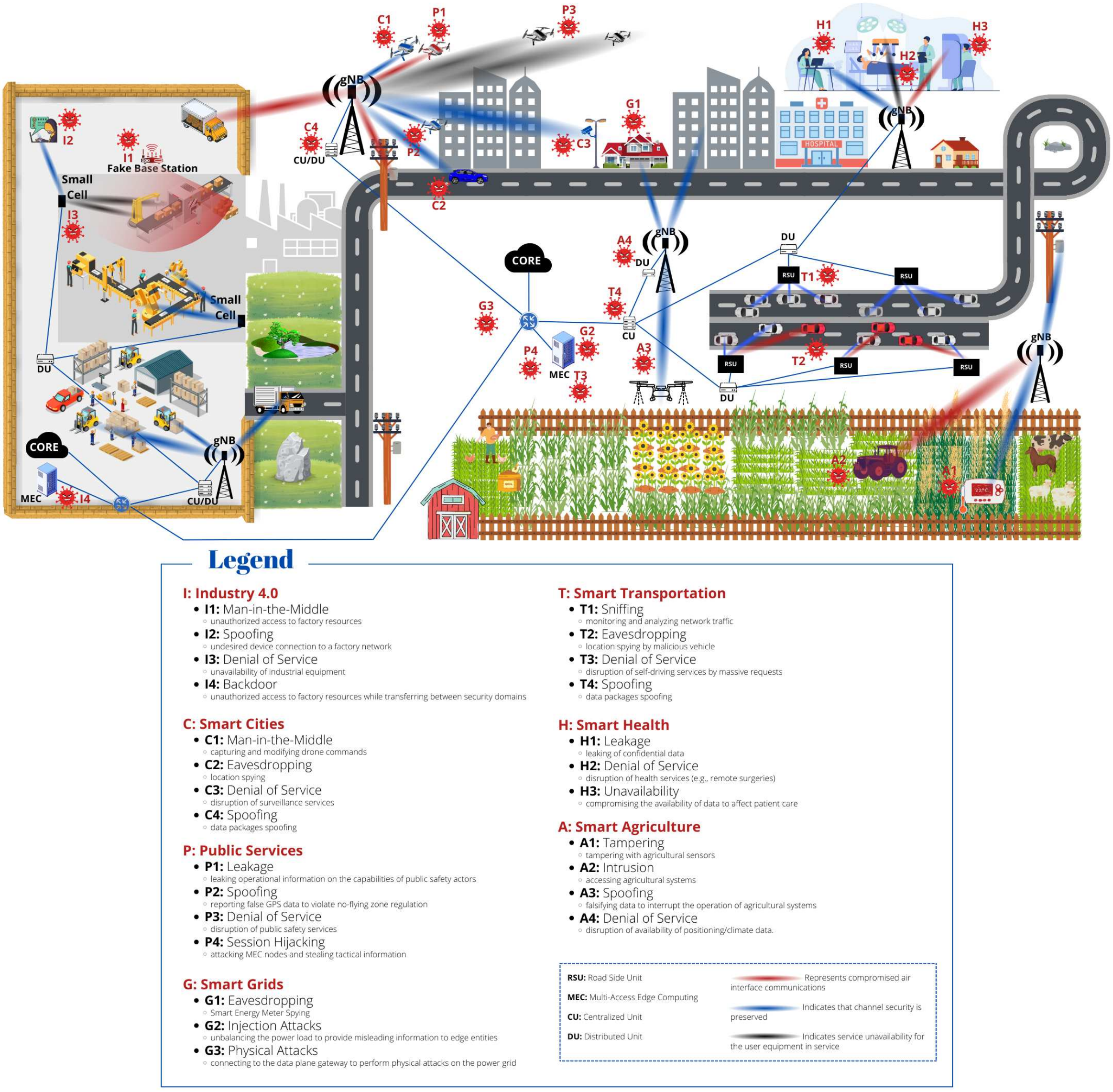
Any attack compromising the network's CIA can impact the vertical applications the network supports. Figure 1 synthesizes examples of threat scenarios in some vertical applications. The scenarios for Industry 4.0 (I), Smart Cities (C), Public Services (P), Smart Grids (G), Intelligent Transportation (T), Smart Health (H), and Smart Agriculture (A) depict potential threats (red image of the attacker) with their respective identifiers. The red light represents compromised air interface communications, active or passive, depending on the related threat. The gray light indicates service unavailability for the user equipment in service. The blue light indicates that channel security is preserved, but internal threats may still exist in the equipment or applications.

Concerning Figure 1, in the context of smart transportation, the Road Side Unit (RSU) is a device that collects, processes, and transmits traffic, safety, and vehicle management information [69]. Multi-Access Edge Computing (MEC), Centralized Unit (CU), and Distributed Unit (DU) refer to 5G network architecture elements.

3.3. Security in Smart Cities

In the context of smart cities [70–72], concepts such as smart homes and buildings and smart infrastructure and mobility are considered. Privacy is one of the most relevant challenges in smart cities, as devices constantly capture users' voices, locations, and behavior.

For instance, this vertical is subject to espionage, DoS, MiTM, side-channel attacks, phishing, and spoofing attacks. To mitigate these attacks, it is necessary to establish a secure environment for processing private data, using appropriate encryption models, and implementing suitable policies for access authentication and data transfer [73].



Legend

I: Industry 4.0
- **I1:** Man-in-the-Middle
  - unauthorized access to factory resources
- **I2:** Spoofing
  - undesired device connection to a factory network
- **I3:** Denial of Service
  - unavailability of industrial equipment
- **I4:** Backdoor
  - unauthorized access to factory resources while transferring between security domains

C: Smart Cities
- **C1:** Man-in-the-Middle
  - capturing and modifying drone commands
- **C2:** Eavesdropping
  - location spying
- **C3:** Denial of Service
  - disruption of surveillance services
- **C4:** Spoofing
  - data packages spoofing

P: Public Services
- **P1:** Leakage
  - leaking operational information on the capabilities of public safety actors
- **P2:** Spoofing
  - reporting false GPS data to violate no-flying zone regulation
- **P3:** Denial of Service
  - disruption of public safety services
- **P4:** Session Hijacking
  - attacking MEC nodes and stealing tactical information

G: Smart Grids
- **G1:** Eavesdropping
  - Smart Energy Meter Spying
- **G2:** Injection Attacks
  - unbalancing the power load to provide misleading information to edge entities
- **G3:** Physical Attacks
  - connecting to the data plane gateway to perform physical attacks on the power grid

T: Smart Transportation
- **T1:** Sniffing
  - monitoring and analyzing network traffic
- **T2:** Eavesdropping
  - location spying by malicious vehicle
- **T3:** Denial of Service
  - disruption of self-driving services by massive requests
- **T4:** Spoofing
  - data packages spoofing

H: Smart Health
- **H1:** Leakage
  - leaking of confidential data
- **H2:** Denial of Service
  - disruption of health services (e.g., remote surgeries)
- **H3:** Unavailability
  - compromising the availability of data to affect patient care

A: Smart Agriculture
- **A1:** Tampering
  - tampering with agricultural sensors
- **A2:** Intrusion
  - accessing agricultural systems
- **A3:** Spoofing
  - falsifying data to interrupt the operation of agricultural systems
- **A4:** Denial of Service
  - disruption of availability of positioning/climate data.

RSU: Road Side Unit

MEC: Multi-Access Edge Computing

CU: Centralized Unit

DU: Distributed Unit

🟥 Represents compromised air interface communications

🟦 Indicates that channel security is preserved

⬛ Indicates service unavailability for the user equipment in service

Figure 1. Examples of threat scenarios in 5G vertical applications.

3.3.1. Example of a Smart City Attack Scenario

An attacker can use a network of zombie devices or Software Defined Radio (SDR) to simulate many different devices and initiate mass Radio Resource Control (RRC) connection requests. These requests can overwhelm the radio resources of the base station, causing drones used for logistics to lose their communication channel and become adrift. Many infected drones or SDR devices are required to conduct these malicious actions.

Vulnerabilities can result from infected devices with malicious code or inherent system weaknesses, which may stem from the lack of periodic updates for the devices. Attackers can explore the lack of encryption in specific signaling messages (e.g., RRC connection message) and integrity in specific signaling messages in 3G, 4G, or 5G networks.

Figure 2 presents a sequence diagram depicting the interception, by an attacker, of message exchanges for the configuration of malicious devices. We can observe that by triggering a large volume of connection messages to the base station, the attacker exhausts the available radio resources on the channel, causing legitimate devices to be unable to communicate with the network.

For example, consider a fleet of logistics drones that carry out deliveries in a large metropolitan area. Another fleet from a different company got infected by a malicious update, introducing malicious code into the drones and turning them into zombie devices that form a network controlled by the attacker.

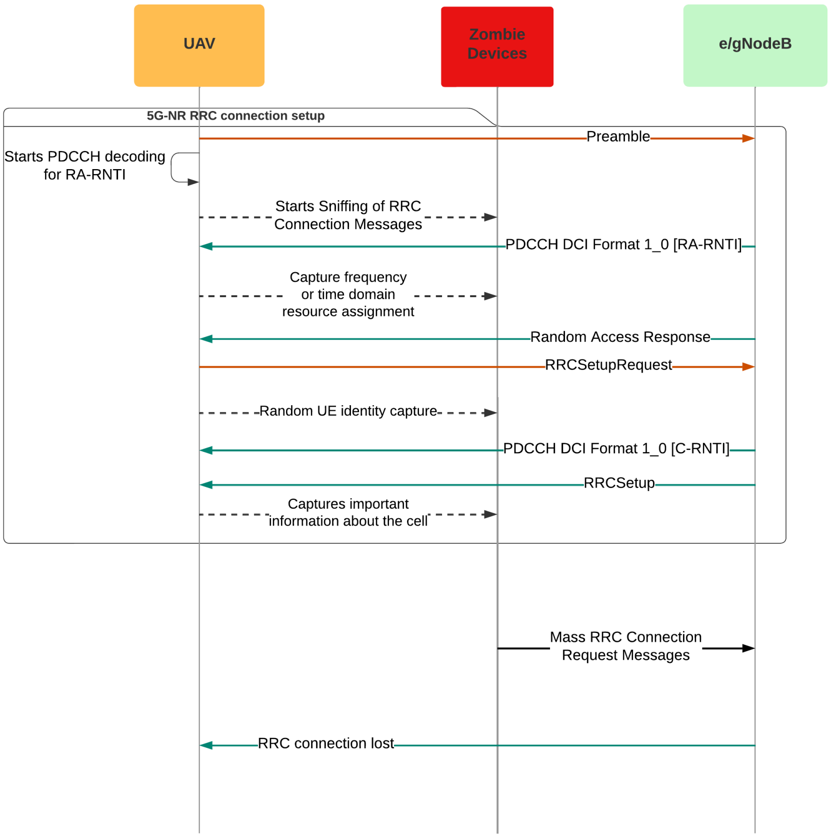

UAV
Zombie Devices
e/gNodeB
5G-NR RRC connection setup
Preamble
Starts PDCCH decoding for RA-RNTI
Starts Sniffing of RRC Connection Messages
PDCCH DCI Format 1_0 [RA-RNTI]
Capture frequency or time domain resource assignment
Random Access Response
RRCSetupRequest
Random UE identity capture
PDCCH DCI Format 1_0 [C-RNTI]
RRCSetup
Captures important information about the cell
Mass RRC Connection Request Messages
RRC connection lost

Figure 2. Sequence diagram related to denial of service attack scenario for drones in smart cities.

By intercepting the RRC connection parameters in the middle, the attacker triggers commands to their malicious network, altering device configurations and forcing them to send connection requests to the gNodeB continuously. The attacker may also utilize SDR equipment to ensure scarce radio resources. Once the gNodeB can no longer handle the many connection requests, legitimate drones may have their requests left unanswered, resulting in a DoS and system unavailability for delivery operations.

3.4. Security in Smart Transportation

The high mobility and rapid vehicular access make the communication environment in 5G networks complex [74]. The 5G vehicular network access control supports heterogeneous technology and, as a result, presents security risks, demanding a unified and real-time authentication scheme. The network is also vulnerable to DoS attacks due to massive access devices. The 5G vehicular network encounters challenges concerning confidentiality, integrity, availability, and authentication, making its protection a significant challenge [75–82].

As the components of autonomous vehicles are limited in computational capacity, the protection of vehicular networks demands an adaptable infrastructure to ensure passengers' safety and vehicle cybersecurity [83]. Since each vehicle type has distinct computational constraints, policy-based security provides enhanced security to match these differences, ensuring each vehicle has appropriate protection resources.

3.4.1. Example of a Smart Transportation Attack Scenario

An attacker can monitor and analyze network traffic and steal sensitive vehicle information (e.g., vehicle location and identity). The attacker monitors and analyzes network traffic on the air interface, capturing message exchanges between a vehicle and the gNodeB, and stealing sensitive vehicle information (e.g., vehicle location and identity). The location can be retrieved by obtaining parameters such as the International Mobile Subscriber Identity (IMSI), Temporary Mobile Subscriber Identity(TMSI)/Globally Unique Temporary Identity (GUTI), and Tracking Area Identity (TAI).

Vulnerabilities can result from incorrect equipment configuration, either accidental or malicious. The lack of encryption in specific signaling messages (2G, 3G, 4G, and 5G), such as RRC connection messages and Paging messages, can be exploited. Attackers can also explore weak encryption algorithms (e.g., A5/1) and the lack of additional security countermeasures (e.g., random padding and inclusion of International Mobile Equipment Identity (IMEI)). Other vulnerabilities include rare allocation of TMSI/GUTI, allocation of IMSI (instead of TMSI), and non-compliance with 3GPP specifications due to lack of encryption in "security mode command" messages.

Figure 3 shows a sequence diagram illustrating the interception, by an attacker, of the message exchange during the establishment of a 5G-New Radio (NR) RRC connection. By capturing the *RRCSetupComplete* message, we can observe that the attacker gains access to the parameters required to infer the user's location.

For instance, consider an autonomous vehicle transporting high-value cargo (a critical business system). If the network operator has incorrectly or insufficiently configured security settings in commissioning their gNodeB, the attacker could capture the signaling exchange between the vehicle and the gNodeB. By obtaining the relevant parameters, the attacker can infer the location of the cargo. Moreover, this scenario could be related to secure critical systems, as undesired behaviors may harm human beings (e.g., collisions).

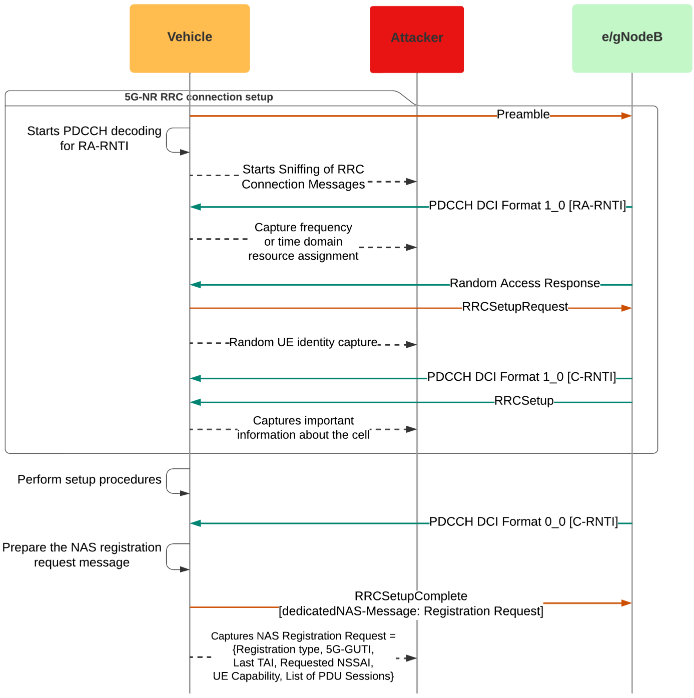

Vehicle
Attacker
e/gNodeB
5G-NR RRC connection setup
Preamble
Starts PDCCH decoding for RA-RNTI
Starts Sniffing of RRC Connection Messages
PDCCH DCI Format 1_0 [RA-RNTI]
Capture frequency or time domain resource assignment
Random Access Response
RRCSetupRequest
Random UE identity capture
PDCCH DCI Format 1_0 [C-RNTI]
RRCSetup
Captures important information about the cell
Perform setup procedures
PDCCH DCI Format 0_0 [C-RNTI]
Prepare the NAS registration request message
RRCSetupComplete [dedicatedNAS-Message: Registration Request]
Captures NAS Registration Request = {Registration type, 5G-GUTI, Last TAI, Requested NSSAI, UE Capability, List of PDU Sessions}

Figure 3. Sequence diagram for a vehicle sensitive information capture attack.

3.5. Security in Public Services

Public service systems are commonly interconnected through private networks and entail high maintenance costs. Public service networks must comply with 3GPP standards, utilizing tactical bubbles in a hybrid format with commercial networks. However, this exposes the network to challenges concerning availability, reliability, and integrity [84–86].

3.5.1. Example of a Public Service Attack Scenario

An attacker can capture sufficient information to tamper with remote commands sent to a surveillance drone, which may have weapons attached to its structure. This highly complex attack requires the attacker to capture security configuration parameters. Once the attackers obtain the keys and identifiers, they can conduct malicious actions to send false or altered commands to control the drone or any of its resources.

Vulnerabilities can also result from incorrect equipment configurations, either accidental or malicious. The lack of encryption in specific signaling messages (2G, 3G, 4G, and 5G), such as RRC connection messages and Paging messages, can be exploited. The attacker can also exploit the weak encryption algorithms (e.g., A5/1) and the lack of additional security countermeasures (e.g., random padding and IMEI inclusion). Other examples of vulnerabilities include rare TMSI/GUTI allocation, allocation of IMSI instead of TMSI, non-compliance with 3GPP specifications due to the lack of encryption in "security mode command" messages, and low control of information shared by individuals involved in the network configuration or operation process.

Figure 4 presents a sequence diagram to illustrate the interception by an attacker of the message exchange to perform the 5G RRC connection setup and Non-Access Stratum (NAS) authentication and security. We can observe that the attacker, in possession of network security information, can take actions to compromise data confidentiality and integrity that traverse the user plane, thereby tampering with the data flow by removing, adding, or altering packets in the network.

For instance, consider a fleet of armed drones patrolling conflict zones and high-risk areas. An attacker could capture airborne signalings to obtain connection setup parameters and, in conjunction with information (security keys) obtained through malicious insiders who might have infiltrated the operators or corporations responsible for network configuration and operation, gain access to the UPF in the core. Subsequently, the attacker could implement malicious code within the function to tamper with the data flow, enabling the transmission of adulterated commands to the drones. This could result in actions such as firing weapons to harm innocent civilians (critical mission system).

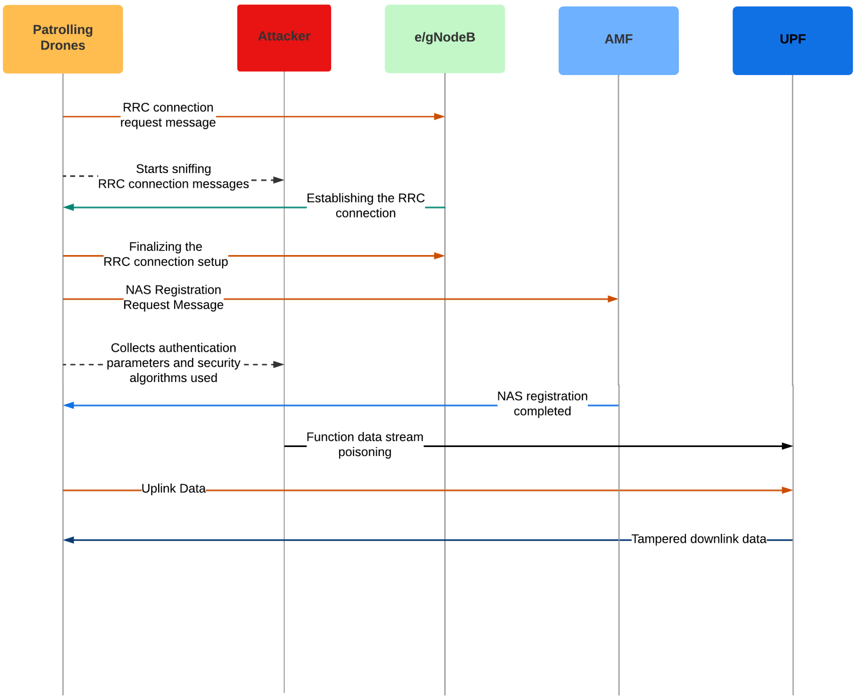

Patrolling Drones
Attacker
e/gNodeB
AMF
UPF
RRC connection request message
Starts sniffing RRC connection messages
Establishing the RRC connection
Finalizing the RRC connection setup
NAS Registration Request Message
Collects authentication parameters and security algorithms used
NAS registration completed
Function data stream poisoning
Uplink Data
Tampered downlink data

Figure 4. Sequence diagram related to the attack scenario of compromising and taking control of patrolling drones.

3.6. Security in Industry 4.0

Industry 4.0, evolving with IoT technologies, utilizes 5G networks in industrial IoT applications [87]. Moreover, Industry 4.0 is associated with security challenges in industrial cyber-physical systems, as an attacker can exploit known cellular network vulnerabilities to carry out cyber-attacks and cause damage to the industrial processes [88–90].

Industry 4.0 also leads to an increase in the use of private mobile networks [91]. This type of network is one of the most important connectivity technologies in this context and, therefore, should be among the services offered by Mobile Network Operators (MNOs). To ensure network availability, privacy, and integrity, companies and MNOs must prioritize cybersecurity. The private mobile network can be deployed in different architectures depending on corporate use cases, subject to different security risks. The company and the MNO must work together to mitigate them [92].

3.6.1. Example of an Industry 4.0 Attack Scenario

An attacker can capture information about the cell on the air interface and use it to configure a fake base station through which industrial equipment can be made unavailable by disabling or isolating them from the network. A malicious base station captured IMSI (or GUTI), and Cell Radio Network Temporary Identifier (C-RNTI) is required for devices to connect to the fake network.

Vulnerabilities can result from incorrect equipment configuration, whether accidental or malicious or the use of radio resources causing destructive interference, forcing the network to downgrade. It can exploit the lack of mutual authentication (2G), lack of encryption in specific signaling messages (2G, 3G, 4G, and 5G) (i.e., RRC connection messages), lack of integrity (2G), lack of integrity in specific signaling messages (3G, 4G, and 5G), weak encryption algorithms (i.e., A5/1), and lack of additional countermeasures for weak encryption algorithms (i.e., padding randomization and inclusion of IMEI), rare allocation of AKA (in comparison with the proposed frequency for AKA allocation).

Figure 5 presents a sequence diagram to represent the interception, by an attacker, of the message exchange for the configuration of a fake base station. We can observe that by capturing configuration information about the cell, such as the C-RNTI message, the attacker gains access to the necessary parameters for creating the fake base station.

For instance, consider a set of industrial equipment operating on a production line. An attacker could employ a fake base station and provide a signal with a higher power to the industrial devices. Since attackers can capture the cell configuration parameters, when correctly set up, the equipment can detect this fake base station as legitimate.

However, upon connecting to this higher-power signal, which is expected to deliver a better QoS, the devices become inaccessible, as they need access to the core network and, consequently, need a data plan. Therefore, the industry could not send new commands or collect crucial plant data for control actions, leading to paralysis or reduced production line performance and financial losses (given that these are critical business systems).

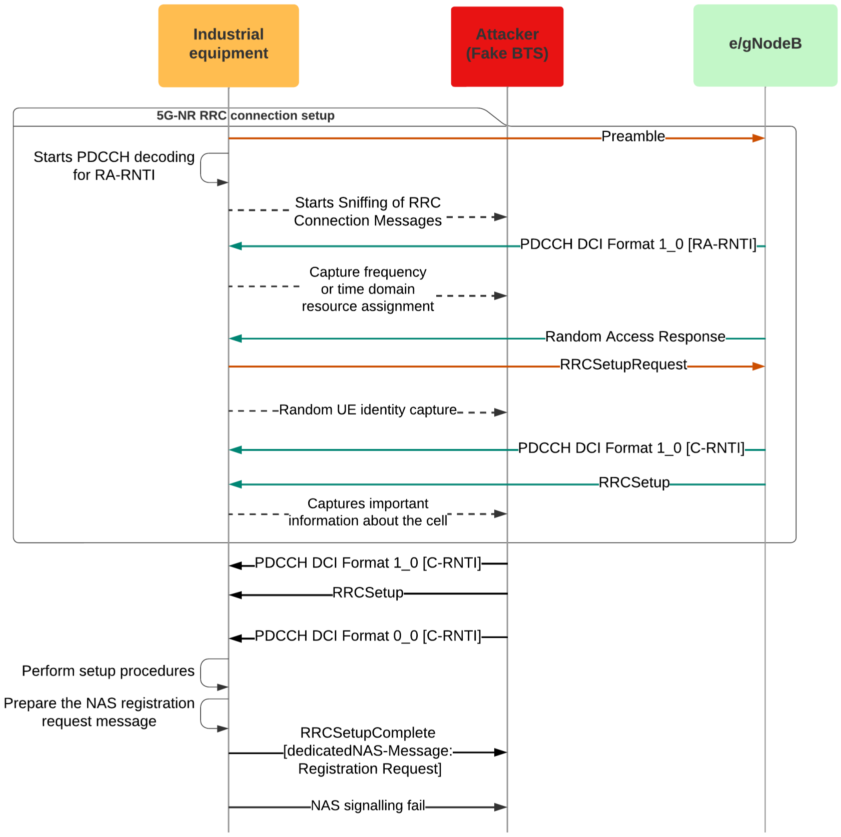

Industrial equipment
Attacker (Fake BTS)
e/gNodeB
5G-NR RRC connection setup
Preamble
Starts PDCCH decoding for RA-RNTI
Starts Sniffing of RRC Connection Messages
PDCCH DCI Format 1_0 [RA-RNTI]
Capture frequency or time domain resource assignment
Random Access Response
RRCSetupRequest
Random UE identity capture
PDCCH DCI Format 1_0 [C-RNTI]
RRCSetup
Captures important information about the cell
PDCCH DCI Format 1_0 [C-RNTI]
RRCSetup
PDCCH DCI Format 0_0 [C-RNTI]
Perform setup procedures
Prepare the NAS registration request message
RRCSetupComplete [dedicatedNAS-Message: Registration Request]
NAS signalling fail

Figure 5. Sequence diagram related to Industry 4.0 equipment unavailability attack scenario.

3.7. Security in Smart Grid

Using 5G networks can benefit the requirements present in the services of power grids [93]. However, many security challenges exist [94,95]. Applying 5G resources in power grids introduces new threats due to the integration of multiple heterogeneous wireless networks, more open network installations, and service providers with different levels of trust. Additionally, network devices have limited computational resources, making security protection difficult. In the case of an attack at the edge, for example, the attacker may gain access to the core and perform data leakage and DoS attacks [95].

3.7.1. Example of a Smart Grid Attack Scenario

An attacker can intercept uplink data from the smart energy meter and tamper with it, retransmitting it to provide the utility company with fake information about the load consumption. This is a highly complex attack, as the attacker needs to capture security configuration parameters. Once attackers obtain these keys and identifiers, they can conduct malicious actions to send false or tampered information to the electric system operator.

As for the previous scenarios, vulnerabilities can result from incorrect equipment configuration. Lack of encryption in specific signaling messages (2G, 3G, 4G, and 5G), such as RRC connection messages and Paging messages, can be exploited. Attackers can exploit weak encryption algorithms (e.g., A5/1) and the lack of additional security countermeasures (e.g., random padding and IMEI inclusion). Other examples of vulnerabilities include infrequent allocation of TMSI/GUTI, allocation of IMSI instead of TMSI, non-compliance with 3GPP specifications due to the lack of encryption in "security mode command" messages, and insufficient control over information shared by individuals involved in the network configuration or operation process.

Figure 6 depicts a sequence diagram to represent the interception, by an attacker, of the message exchange for the 5G RRC connection setup and NAS authentication and security configuration. We can observe that the attacker, possessing network security information, can perform actions to breach the confidentiality and integrity of data transmitted in the user plane, enabling the attacker to impersonate the legitimate user and manipulate the data flow by removing, adding, or tampering with packets in the network.

For example, consider a smart meter installed in a high-end residence. After capturing the parameters, the attacker, with the help of security keys from SIM cards purchased from employees with elevated access credentials within the service providers, can transmit tampered data to the energy utility company, indicating a consumption much lower than what the actual consumer unit is performing.

This attack can cause significant financial losses for the distributor if carried out in many residences (a critical business system). In another scenario, the attacker could infer the occupants' behavior with access to the household's consumption data, potentially mapping the moments when the property is most vulnerable to invasions and theft of targeted assets.

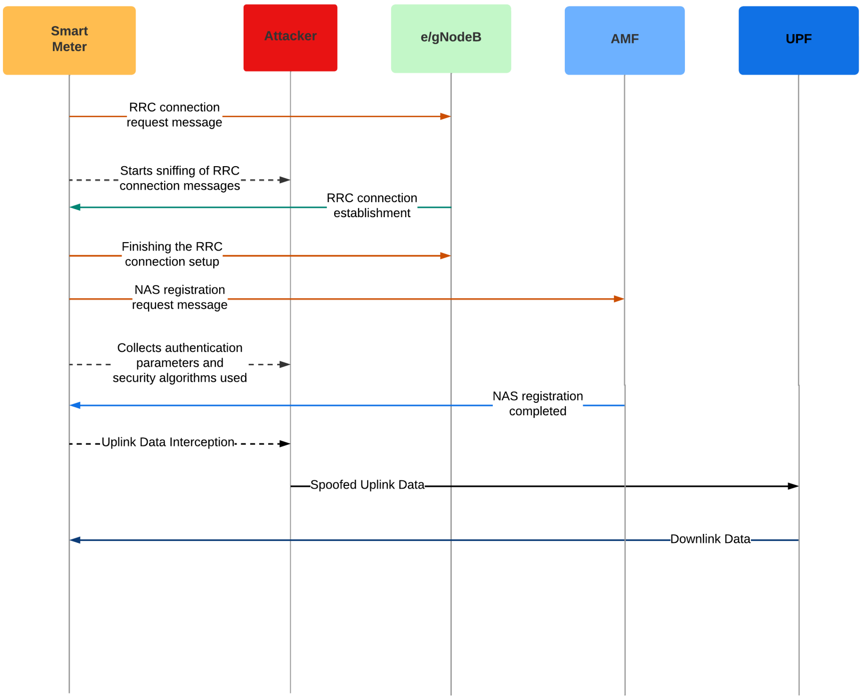

Smart Meter
Attacker
e/gNodeB
AMF
UPF
RRC connection request message
Starts sniffing of RRC connection messages
RRC connection establishment
Finishing the RRC connection setup
NAS registration request message
Collects authentication parameters and security algorithms used
NAS registration completed
Uplink Data Interception
Spoofed Uplink Data
Downlink Data

Figure 6. Sequence diagram related to the attack scenario of compromising smart meter reading data collection.

3.8. Security in Smart Health

The advent of 5G networks can support smart health in aspects such as hospital asset management, remote health data monitoring, and medication control [96]. The architecture of e-Health applications [97], for example, includes sensors on the human body, communication networks, and services associated with medical service providers. Therefore, sensitive data can be exposed to various attacks [98,99]. For instance, data breaches, interference, availability attacks, unauthorized access, DoS attacks, social engineering, phishing, and malware attacks can occur.

Therefore, ensuring the security and privacy of medical applications is essential [73,100]. To protect this type of application, solutions proposed in the literature address, for example, authentication and authorization, using encryption and redundancy to ensure availability and secure communication between hospitals, medical personnel, and patients [73].

3.8.1. Example of a Smart Health Attack Scenario

An attacker can emit a signal that causes destructive interference, disrupting or degrading the connection of a medical device during a hospital procedure. An attacker requires a jamming device to carry out this attack. The capture of information about the configuration of the 5G RRC connection can assist in adjusting the malicious equipment, making it no longer necessary to radiate the signal over a wide range and increasing the damage in the specific irradiated frequency band due to the provision of power in the equipment.

The vulnerability exploited in this attack is inherent to the communication channel used, as the air interface remains inevitably exposed and widely accessible. Figure 7 presents a sequence diagram to represent the interception, by an attacker, of the message exchange to capture parameters about the 5G RRC connection.

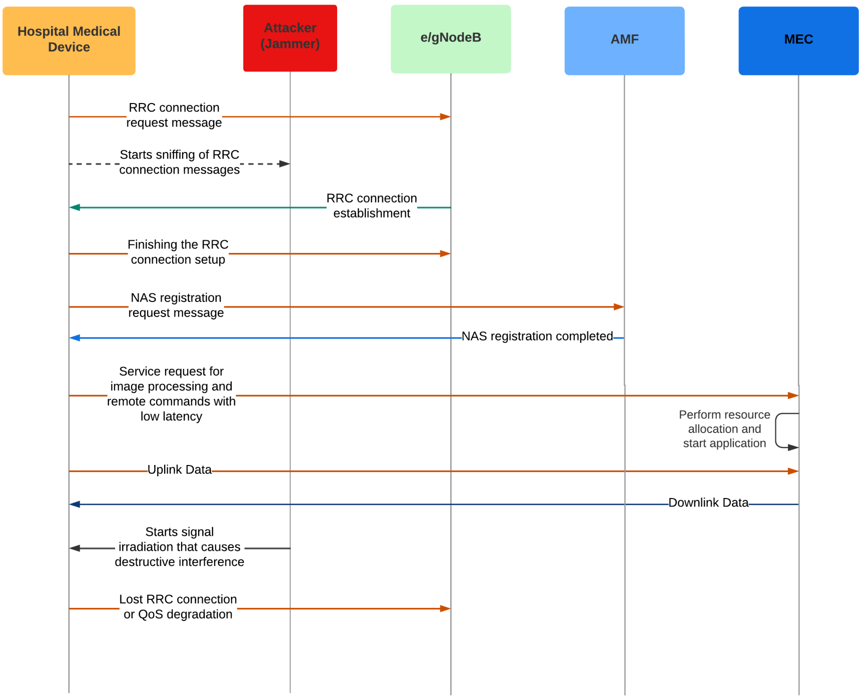

Hospital Medical Device
Attacker (Jammer)
e/gNodeB
AMF
MEC
RRC connection request message
Starts sniffing of RRC connection messages
RRC connection establishment
Finishing the RRC connection setup
NAS registration request message
NAS registration completed
Service request for image processing and remote commands with low latency
Perform resource allocation and start application
Uplink Data
Downlink Data
Starts signal irradiation that causes destructive interference
Lost RRC connection or QoS degradation

Figure 7. Sequence diagram related to the healthcare disruption attack scenario.

We can observe that the attacker, armed with the captured information, configures the jamming device and initiates signal radiation, causing connection loss or deterioration of service quality. To continue operating the device, it may seek a connection with a more distant gNodeB operating in a different frequency band from the degraded one. However, due to the greater distance between the equipment and the base station, attackers can use a modulation level with fewer symbols. This procedure will worsen service quality to levels that may render healthcare service provision impossible.

For example, one can envision a surgery scenario where a physician remotely controls a surgical robot. Upon capturing the RRC connection configuration parameters, the attacker adjusts the jamming equipment to the operating frequency band of the hospital device.

Subsequently, the attacker initiates the signal radiation that will cause destructive interference in the 5G network signal. The robot will lose communication with the network and may attempt to connect to another base station farther away, operating on a different channel. However, the increased distance will result in the use of a modulation level with fewer symbols, leading to a deterioration in service quality. Consequently, the quality of service may become insufficient for providing a service like surgery, which relies on low latency for the surgical equipment to respond quickly and for procedure images to reach the physician in near real-time (a safety-critical system).

3.9. Security in Smart Agriculture

The evolution of agricultural applications in the context of smart agriculture necessitates using technologies such as edge computing, augmented reality, and artificial intelligence [101]. Various network requirements are considered when considering the different types of applications, including latency, data processing, and transmission type. By supporting different types of radio connections, agricultural systems present vulnerabilities related to licensed radio spectrum standards (2G, LTE, and eMTC), as well as threats found in IoT devices when using unlicensed spectrums (Wi-Fi, LoRa, and SIGFOX).

Furthermore, attackers can conduct DoS attacks by infected devices or external devices attempting unauthorized access. In general, attacks threatening systems in this vertical are related to IoT system vulnerabilities and can be categorized into data attacks, network and equipment attacks, and supply chain attacks [73].

3.9.1. Example of a Smart Agriculture Attack Scenario

An attacker can capture enough information to tamper with remote commands sent to a fleet of autonomous harvesters, interrupting or delaying harvesting and damaging the machines or crops. This results in significant financial losses.

This is a highly complex attack, as the attacker needs to capture security configuration parameters. Once the attackers obtain these keys and identifiers, they can conduct malicious actions to send false or tampered commands to control the harvesting machines. For this type of attack to occur, specific vulnerabilities in the system are considered a premise. Vulnerabilities can result from incorrect equipment configuration, whether accidental or malicious. Lack of encryption in specific signaling messages (2G, 3G, 4G, and 5G), such as RRC connection messages and Paging messages, can be exploited.

Weak encryption algorithms (e.g., A5/1) and the lack of additional security countermeasures (e.g., random padding and IMEI inclusion) are vulnerabilities. Other examples of vulnerabilities include infrequent allocation of TMSI/GUTI, allocation of IMSI instead of TMSI, non-compliance with 3GPP specifications due to the lack of encryption in "security mode command" messages, and insufficient control over information shared by individuals involved in the network configuration or operation process.

Figure 8 presents a sequence diagram to represent the interception of the message exchange for the 5G RRC connection setup and NAS authentication and security configuration. We can observe that the attacker, armed with network security information, can carry out actions to breach the confidentiality and integrity of data transmitted in the user plane, allowing them to intercept, read, alter, and retransmit packets that will appear legitimate.

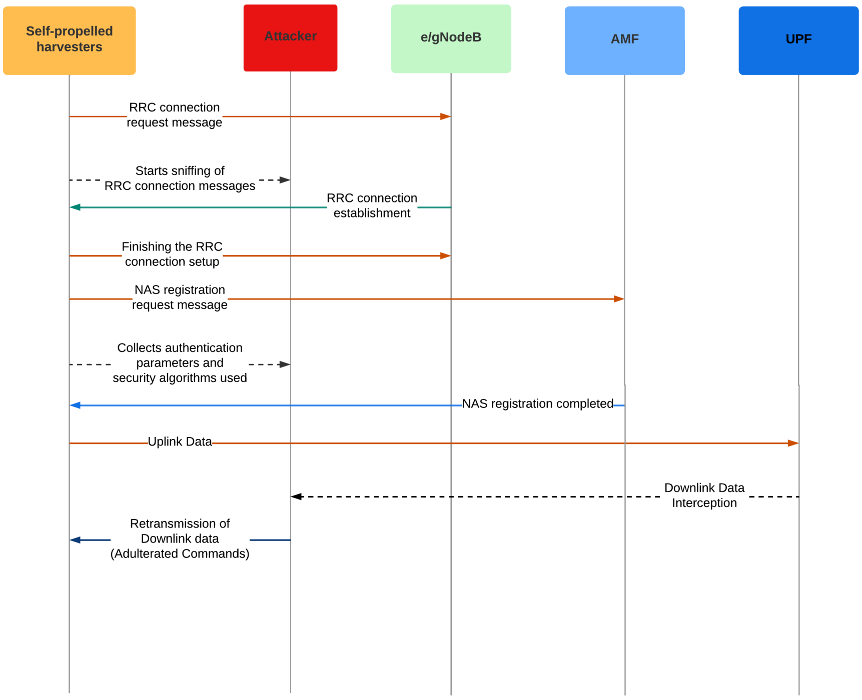

Self-propelled harvesters
Attacker
e/gNodeB
AMF
UPF
RRC connection request message
Starts sniffing of RRC connection messages
RRC connection establishment
Finishing the RRC connection setup
NAS registration request message
Collects authentication parameters and security algorithms used
NAS registration completed
Uplink Data
Downlink Data Interception
Retransmission of Downlink data (Adulterated Commands)

Figure 8. Sequence diagram related to the compromise and take control attack scenario for self-propelled harvesters.

For example, consider a fleet of autonomous harvesters operating in the field, monitored and operated remotely through the 5G network. With the collected information from the air interface and internal malicious actors within the network operators, an attacker can intercept the data sent to the machines and maliciously retransmit commands. The harvesters can then misbehave and damage vast areas of crops, resulting in losses for the harvest, which, depending on their magnitude, can influence the availability of that crop in the market and alter its prices (a critical business system).

3.10. Security in Other Verticals

The existing threats may extend to other verticals, such as education and retail [102]. Smart education is a relevant vertical for both the public and private sectors, which can positively impact student learning [103]. In the context of education, immersive technologies like Augmented Reality (AR) and Virtual Reality (VR) are also susceptible to attacks. For example, an attacker might gain unauthorized access to and manipulate video streams used in AR applications. Moreover, AR and VR applications are vulnerable to tampering, side-channel attacks, malicious code injections, and hardware Trojans [94].

3.11. Attack-Defense Trees

3.11.1. Attack-Defense Tree for the Smart City Scenario

Figure 9 presents an attack-defense tree for the DDoS scenario in smart cities. We can observe that there is a primary goal (Attack on the 5G Network) from which a primary sub-goal derives (DDoS Attack on the Smart Cities Vertical). The subsequent nodes are divided into secondary sub-goals (Logical Attack and Physical Attack). They are conjunctive refinements, implying that both conditions must be fulfilled. Also, security and privacy solutions in smart cities [104] and DDoS prevention strategies [105] are presented as countermeasures for the primary sub-goal. The logical attack must be done by infecting the drones, which can be achieved through malicious firmware updates. The countermeasure proposed is to verify the integrity and authenticity of updates.

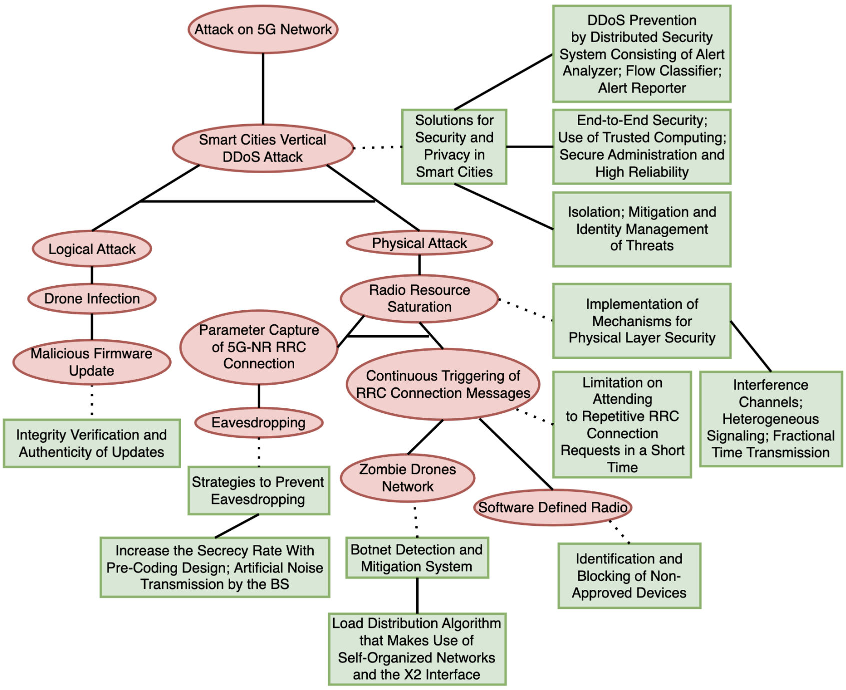

Attack on 5G Network
Smart Cities Vertical DDoS Attack
Solutions for Security and Privacy in Smart Cities
DDoS Prevention by Distributed Security System Consisting of Alert Analyzer; Flow Classifier; Alert Reporter
End-to-End Security; Use of Trusted Computing; Secure Administration and High Reliability
Isolation; Mitigation and Identity Management of Threats
Logical Attack
Physical Attack
Drone Infection
Radio Resource Saturation
Implementation of Mechanisms for Physical Layer Security
Malicious Firmware Update
Parameter Capture of 5G-NR RRC Connection
Continuous Triggering of RRC Connection Messages
Limitation on Attending to Repetitive RRC Connection Requests in a Short Time
Interference Channels; Heterogeneous Signaling; Fractional Time Transmission
Integrity Verification and Authenticity of Updates
Eavesdropping
Strategies to Prevent Eavesdropping
Zombie Drones Network
Software Defined Radio
Increase the Secrecy Rate With Pre-Coding Design; Artificial Noise Transmission by the BS
Botnet Detection and Mitigation System
Identification and Blocking of Non-Approved Devices
Load Distribution Algorithm that Makes Use of Self-Organized Networks and the X2 Interface

Figure 9. Attack-defense tree for the DDoS scenario in smart cities.

The physical attack will involve saturating the radio resources of the base station, which can be countered by implementing mechanisms for security at the physical layer [106]. In the lack of measures to mitigate vulnerabilities at the physical layer, two new conjunctive refinements can be valid: capturing 5G RRC connection parameters and continuously firing RRC connection messages. It is possible to address the second refinement by quickly limiting the responsiveness to repetitive RRC connection requests. To carry out the parameter capture, the attacker must employ eavesdropping techniques. It is possible to prevent this threat through specific security strategies [107], such as using encrypted signaling messages. With the lack of measures against the continuous firing of messages, the attacker may use a network of zombie drones or SDRs to flood the base station with RRC connection requests. Attackers can employ a botnet detection and mitigation system to address these actions [108]. In the case of SDR, unauthorized devices can be identified and blocked.

3.11.2. Attack-Defense Tree for the Smart Transportation Scenario

Figure 10 presents an attack-defense tree for capturing confidential information in smart transportation. This and the following trees use the same logic of Figure 9. A set of solutions for physical layer security relates to this scenario [59,106,109–111]. We can observe that the capture occurs through eavesdropping on the air interface. As a countermeasure to protect the air interface, increasing the secrecy rate with the design of pre-coding and artificial noise transmission by the base station is proposed [107].

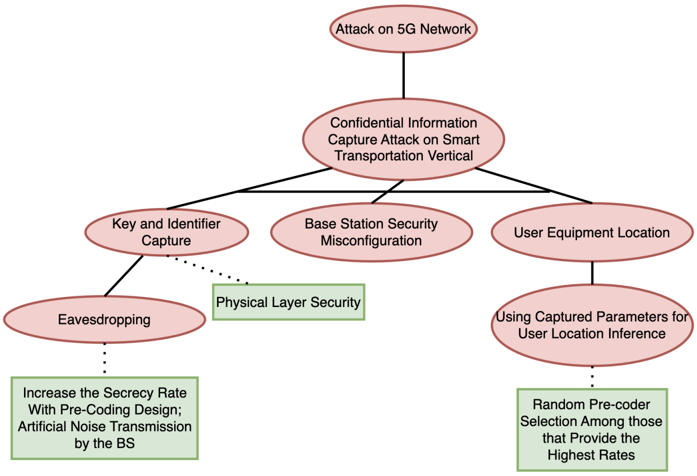

Attack on 5G Network
Confidential Information Capture Attack on Smart Transportation Vertical
Key and Identifier Capture
Base Station Security Misconfiguration
User Equipment Location
Physical Layer Security
Eavesdropping
Using Captured Parameters for User Location Inference
Increase the Secrecy Rate With Pre-Coding Design; Artificial Noise Transmission by the BS
Random Pre-coder Selection Among those that Provide the Highest Rates

Figure 10. Attack-defense tree for the smart transportation confidential information capture scenario.

We also observe that the successful progress of the attack depends on the Improper Security Configuration of the Base Station, enabling vulnerabilities such as transmitting permanent identifiers in clear text. On the other hand, the User Equipment Localization attack will involve using the captured parameters to infer the user's location. For instance, one possible countermeasure for this attack is the random selection of pre-coding schemes that provide the highest rates [112].

3.11.3. Attack-Defense Tree for the Public Service Scenario

Figure 11 presents an attack-defense tree for the scenario of compromising the control of patrolling drones in public services. A set of solutions is presented to combat the capture of identifiers and keys, replacing permanent identifiers with variable and temporary pseudonyms [113]. We can observe that the capture occurs through eavesdropping on the air interface and information leakage by malicious insiders within the network.

As a countermeasure to protect the air interface, increasing the secrecy rate with the design of pre-coding and artificial noise transmission by the base station can be used [107]. Against the exposure of confidential information, access control and action logging for non-repudiation, user behavior analysis, and user-level and time-based access policies can be implemented [114].

On the other hand, the attack of Malicious Access to User Plane Function (UPF) will involve using captured keys and identifiers to access the data flow and inject malicious code into the UPF. One possible countermeasure for this attack is using intelligent authentication through machine learning [115] and cross-layer authentication protocol [116]. With the lack of measures to mitigate the vulnerabilities mentioned above, data flow poisoning and takeover of patrolling drones may occur. However, there are possible countermeasures [117].

doi:10.20944/preprints202312.1703.v1

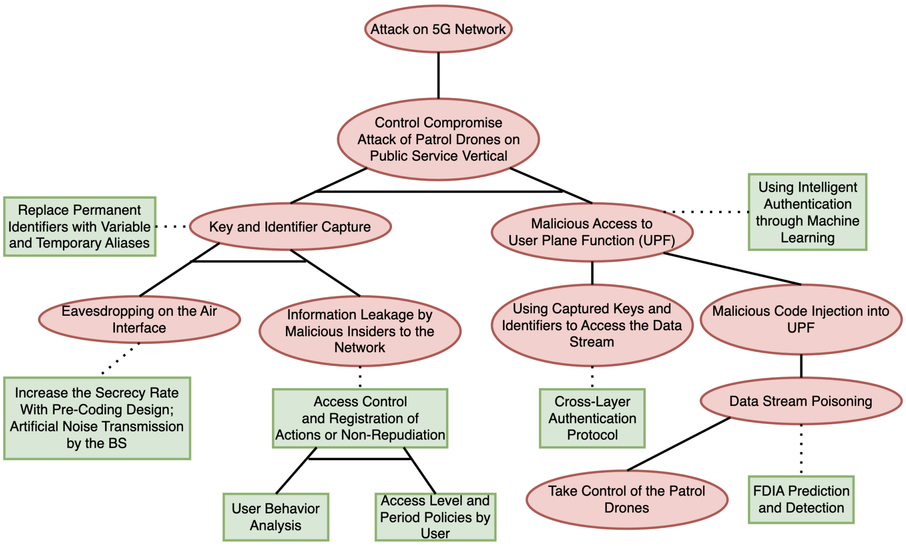

Attack on 5G Network
Control Compromise Attack of Patrol Drones on Public Service Vertical
Key and Identifier Capture
Replace Permanent Identifiers with Variable and Temporary Aliases
Malicious Access to User Plane Function (UPF)
Using Intelligent Authentication through Machine Learning
Eavesdropping on the Air Interface
Information Leakage by Malicious Insiders to the Network
Using Captured Keys and Identifiers to Access the Data Stream
Malicious Code Injection into UPF
Increase the Secrecy Rate With Pre-Coding Design; Artificial Noise Transmission by the BS
Access Control and Registration of Actions or Non-Repudiation
Cross-Layer Authentication Protocol
Data Stream Poisoning
User Behavior Analysis
Access Level and Period Policies by User
Take Control of the Patrol Drones
FDIA Prediction and Detection

Figure 11. Attack-defense tree for the patrolling drone control compromise scenario.

3.11.4. Attack-Defense Tree for the Industry 4.0 Scenario

Figure 12 presents an example of an attack-defense tree for the scenario of disruption in industrial service. We can observe the connection of the equipment to the fake base station. As an example of a countermeasure, the use of an algorithm that monitors the equipment and verifies if they are performing the expected function [118] is presented. With the lack of measures to mitigate the vulnerabilities mentioned above, the attacker may cause the equipment to disconnect from the legitimate network and halt the production line.

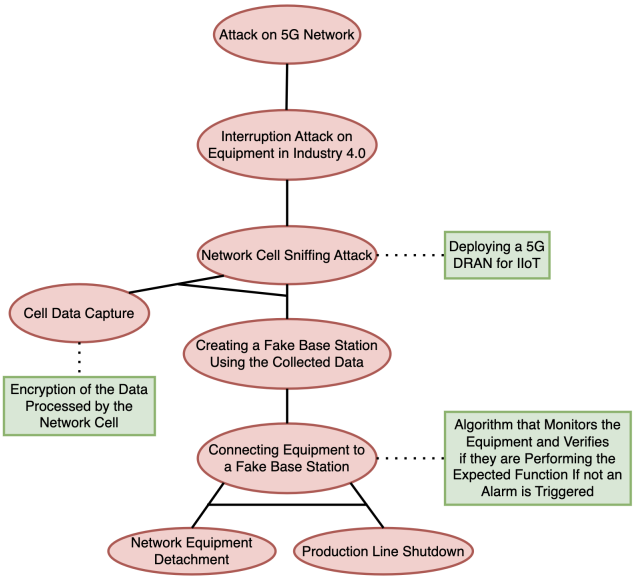

Attack on 5G Network
Interruption Attack on Equipment in Industry 4.0
Network Cell Sniffing Attack
Deploying a 5G DRAN for IIoT
Cell Data Capture
Creating a Fake Base Station Using the Collected Data
Encryption of the Data Processed by the Network Cell
Connecting Equipment to a Fake Base Station
Algorithm that Monitors the Equipment and Verifies if they are Performing the Expected Function If not an Alarm is Triggered
Network Equipment Detachment
Production Line Shutdown

Figure 12. Attack-defense tree for the industrial service outage scenario.

3.11.5. Attack-Defense Tree for the Smart Grid Scenario

Figure 13 presents an attack-defense tree for the scenario of data tampering in smart grids. A set of solutions is present in the literature to combat the capture of identifiers and keys, replacing permanent identifiers with variable and temporary pseudonyms [113]. Afterward, we can observe that the capture occurs through eavesdropping on the air interface and leakage of information by malicious insiders within the network.

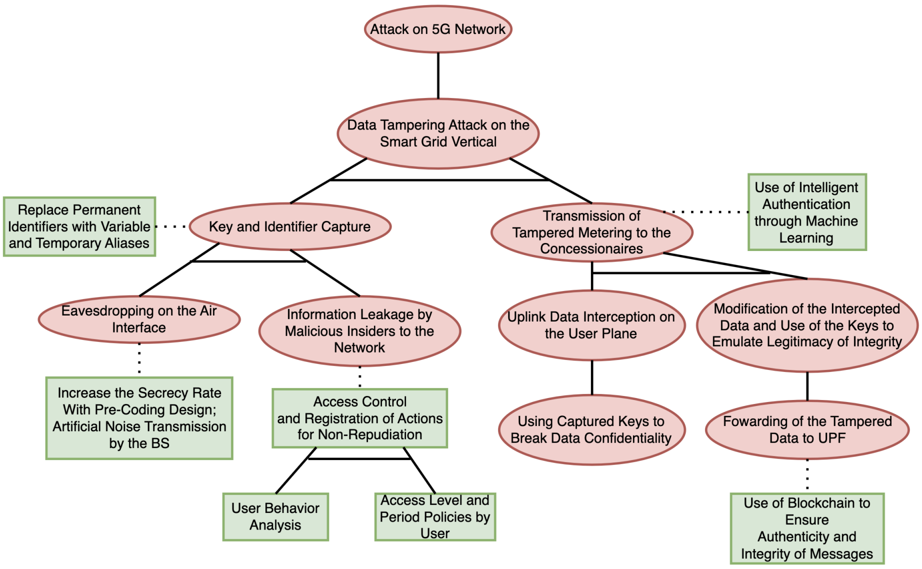

Attack on 5G Network
Data Tampering Attack on the Smart Grid Vertical
Replace Permanent Identifiers with Variable and Temporary Aliases
Key and Identifier Capture
Transmission of Tampered Metering to the Concessionaires
Use of Intelligent Authentication through Machine Learning
Eavesdropping on the Air Interface
Information Leakage by Malicious Insiders to the Network
Uplink Data Interception on the User Plane
Modification of the Intercepted Data and Use of the Keys to Emulate Legitimacy of Integrity
Increase the Secrecy Rate With Pre-Coding Design; Artificial Noise Transmission by the BS
Access Control and Registration of Actions for Non-Repudiation
Using Captured Keys to Break Data Confidentiality
Fowarding of the Tampered Data to UPF
User Behavior Analysis
Access Level and Period Policies by User
Use of Blockchain to Ensure Authenticity and Integrity of Messages

Figure 13. Attack-defense tree for the data tampering scenario in smart grids.

As an example of a countermeasure to protect the air interface, increasing the secrecy rate with pre-coding design and artificial noise transmission by the fake base station is presented [107]. Against the exposure of confidential information, access control and action logging for non-repudiation, user behavior analysis, and user-specific access policies in terms of level and time are presented [114].

The attack of transmitting adulterated data consists of using the captured keys to access intercepted user plane data and retransmit modified information, which has the potential countermeasure of using intelligent authentication through machine learning [115]. With the lack of measures to mitigate the vulnerabilities mentioned above, modification of data sent by the smart meter to feed the utility company with false or maliciously biased information may occur, with a potential countermeasure being the use of blockchain to ensure message authenticity and integrity [119].

3.11.6. Attack-Defense Tree for the Smart Health Scenario

Figure 14 presents an attack-defense tree for smart health's 5G network signal degradation scenario. A set of solutions for physical layer security is presented [106]. Subsequently, we can observe that the capture occurs through eavesdropping on the air interface.

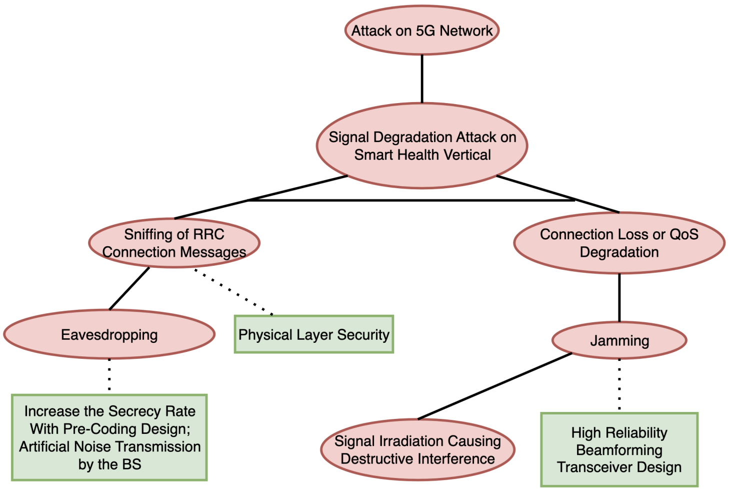

Attack on 5G Network
Signal Degradation Attack on Smart Health Vertical
Sniffing of RRC Connection Messages
Connection Loss or QoS Degradation
Eavesdropping
Physical Layer Security
Jamming
Increase the Secrecy Rate With Pre-Coding Design; Artificial Noise Transmission by the BS
Signal Irradiation Causing Destructive Interference
High Reliability Beamforming Transceiver Design

Figure 14. Attack-defense tree for the signal degradation scenario in smart health.

As an example of countermeasure, increasing the secrecy rate through pre-coder design and artificial noise transmission by the fake base station is presented [107]. The attack that causes loss of connection or QoS degradation is carried out through Jamming, which can be mitigated by designing a high-reliability beamforming transceiver. With the lack of measures to mitigate the mentioned vulnerabilities, attackers could conduct signal radiation, causing destructive interference on the legitimate network signal.

3.11.7. Attack-Defense Tree for the Smart Agriculture Scenario

Figure 15 presents an attack-defense tree for the scenario of command tampering in smart agriculture. A set of solutions is presented to combat the capture of identifiers and keys, replacing permanent identifiers with variable and temporary pseudonyms [113].

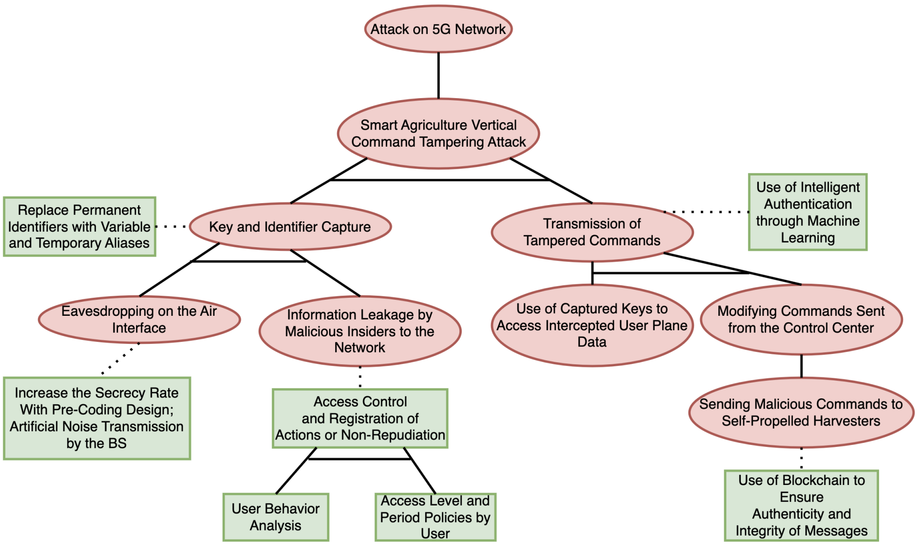

Attack on 5G Network
Smart Agriculture Vertical Command Tampering Attack
Replace Permanent Identifiers with Variable and Temporary Aliases
Key and Identifier Capture
Transmission of Tampered Commands
Use of Intelligent Authentication through Machine Learning
Eavesdropping on the Air Interface
Information Leakage by Malicious Insiders to the Network
Use of Captured Keys to Access Intercepted User Plane Data
Modifying Commands Sent from the Control Center
Increase the Secrecy Rate With Pre-Coding Design; Artificial Noise Transmission by the BS
Access Control and Registration of Actions or Non-Repudiation
Sending Malicious Commands to Self-Propelled Harvesters
User Behavior Analysis
Access Level and Period Policies by User
Use of Blockchain to Ensure Authenticity and Integrity of Messages

Figure 15. Attack-defense tree for the smart agriculture command tampering scenario.

Afterward, we can observe that the capture occurs through eavesdropping on the air interface and information leakage by malicious insiders within the network. A countermeasure to protect the air interface is to increase the secrecy rate by designing a pre-coder and artificial noise transmission by the fake base station [107]. To counter the exposure of confidential information, access control and action logging can be implemented for non-repudiation, user behavior analysis, and user-specific access policies based on level and time [114].

The attack of transmitting adulterated commands consists of using the captured keys to access intercepted data from the user plane. In this case, one countermeasure is using intelligent authentication through machine learning [115]. With the lack of measures to mitigate the mentioned vulnerabilities, the attacker could conduct the modification of commands sent by the control center and subsequent sending of malicious commands to the self-driving harvesters, with a possible countermeasure being the use of blockchain to ensure authenticity and integrity of messages [119]. This solution was initially designed to address security issues in the smart transportation vertical. However, given the similarities between attacks that adulterate data in transit in the network, the same solution could apply to the smart agriculture scenario.

4. Other Concerns on the Privacy in Vertical Applications

4.1. Privacy in Vertical Applications Communications

This section discusses privacy based on communication, NS, and MEC. For communication, we exemplify two application scenarios: vehicular networks and drones.

4.1.1. Privacy of 5G Vehicular Networks

The most recurring threats mentioned in the literature are eavesdropping, MitM, impersonation, collusion, identity disclosure, de-anonymization/re-identification, tracking, and inference. Li et al. [120], for instance, presented some privacy preservation solutions, organizing them according to different types and classifications of services. The solutions can address data privacy, identity privacy, location privacy, and mobility privacy.

4.1.2. Privacy of 5G Drone Communications

In specific scenarios where drones are used as 5G base stations or relays, such as in public safety situations, the data collected by these drones becomes a potential target. Intruders aim to extract sensitive information from the drones. Similarly, intruders may attempt to compromise the drones and control them for malicious purposes when drones are used for civilian monitoring and surveillance purposes. This can pose serious threats, as compromised drones can be used as weapons to carry out attacks against crowds. Moreover, compromised drones can exploit communications between devices to eavesdrop on data acquired by other nearby drones.

4.2. Privacy in Network Slicing

The division of the network into distinct slices, each with appropriate isolation measures, is essential to meet the privacy needs of various vertical applications [121]. By incorporating the necessary NF to preserve privacy, allocating separate slices helps address the diverse privacy requirements of different verticals. More robust authentication mechanisms and effective slice isolation techniques restrict access from one slice to another, ensuring data confidentiality. The dynamic modification of the NFV structure adds complexity to disrupting privacy-preserving mechanisms.

Compliance with specific privacy schemes adds another layer of complexity. Given the various data protection regulations in different countries or regions, there may be conflicts of laws requiring adherence to privacy frameworks tailored to the respective geographical context. These schemes are essential to maintain data integrity and security during transmission [12]. One possible solution is to modify settings within the slices, such as adjusting the arrangement of NF.

4.3. Privacy of Application Data in MEC

Regarding security and privacy protection from the MEC perspective, several solutions are proposed in the literature to enhance network trust. In the work presented by Khan *et al.* [4], various examples of solutions related to this relevant topic are discussed. In 5G networks, the mobile edge is the point of access for users and services from the RAN, and it is also a point of vulnerability in terms of security. Identified vulnerabilities and potential attacks can cause significant damage to the MEC system.

5. Discussion and Future Research Directions

Downgrade attacks are noteworthy among the various threats targeting legacy and 5G networks. In the event of a successful downgrade attack, it is essential to minimize the impact on network users. Such concerns are particularly relevant for countries where the transition between legacy networks and 5G occurs gradually. Government documents highlight the downgrade attack as a relevant threat to national security. For instance, in a technical document [122], the United States Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and the Office of the Director of National Intelligence presented the following scenario: (1) an attacker accesses a 5G small cell near a government office, (2) the attacker configures the small cell to enable spoofing in the context of 4G, (3) the attacker forces a downgrade in the 5G network to a vulnerable 4G configuration (exploiting vulnerabilities in the Signaling System 7 (SS7)) to gain access to information technology and communication components used by government employees, and (4) the attacker can use the obtained information to access more secure networks and obtain confidential data. In addition to governments, we propose that vertical industries thoroughly analyze comparable scenarios to mitigate such cyber-attacks proactively.

Some studies analyzed in this extensive survey propose or verify strategies to prevent general threats such as eavesdropping [107,123–126], DoS [127–129], EDoS [130], scanning attacks [131], IMSI catchers [113,132], spoofing attacks [133,134,134–136], resource depletion attacks (e.g., botnet attacks [108,137]), jamming [138–140], localization attack [112], pilot contamination [141,142], pollution attacks [143–145], false data injection [117], DDoS [105,146–150], and DRDoS [151,152]. Other proposed solutions address secure handover (e.g., for heterogeneous IoT networks [153]), enabling devices to join domains with trust (e.g., using authentication frameworks [88,154,155] and protocols [156]). Some studies concern the proposal of improved authentication/authorization [157–161], architectures [162–167], lightweight security [168–172], security schemes (models or protocols) [58,62,173–175], security platforms (or systems) [176–180], algorithms (or methods) [181–185], SDN/NFV-based core NS [186], anomaly/threat detection [118,187–190], controlling NS access/use [191], ensuring NS isolation [192], ensuring intra-slice security [193], ensuring security in D2D communications [64,194–198], security based on blockchain [54,119,199–201], and testbeds for 5G experimentation [202–206].

Some proposed solutions focus on resource management considering the QoS, including security [207]. Other solutions focus on security and privacy in 5G networks and vertical applications, such as smart transportation [208], Industry 4.0 [209], smart cities [104], public services [168], smart grids [95], smart agriculture [210], and smart health [211].

However, the literature lacks comprehensive discussions on threats and solutions for other vertical applications, including education. For instance, this encompasses potential threats to the confidentiality of students' historical records within the education system. Due to the unique requirements and challenges introduced by vertical applications, generic security solutions may only partially align with the specific needs of individual services for effectively mitigating distinct threats such verticals face.

Some surveyed papers also propose applying formal methods to enhance trust (regarding security) in 5G networks (e.g., [210,212–215]). In this case, one of the challenges is the appropriate choice of how to represent network components, specific components of application scenarios, potential attacks, and mitigation strategies. Analyzing the security properties of specific solutions (e.g., protocols) is a common and recognized activity within the community. However, when integrated with network elements, the formal modeling and analysis of 5G application scenarios remain challenging in the field [212]. As each vertical application has specific security threats, its characteristics should be considered in formal security analyses of 5G networks.

Moreover, other surveyed papers propose applying machine learning techniques to detect threats [216], as with intrusion detection systems. In this case, a relevant issue relates to trust in 5G systems based on artificial intelligence [68]. Applying formal methods is also an interesting research opportunity to increase trust in these systems. However, several challenges are identified when using formal methods, such as (1) the representation of traditional machine learning models as part of 5G-enabled systems, (2) the representation of deep learning models as part of 5G-enabled systems, and (3) the formal analysis of such models' properties (including security).

6. Conclusion

This extensive survey included analyses of research papers, technical reports, technical specifications, and white papers. Upon analyzing the documents, we observed that several vulnerabilities, threats, and attacks highlighted in research papers are also emphasized as concerns by industry, governments, and standardization institutions.

We categorized threats to vertical applications, such as smart cities and Industry 4.0. We defined attack scenarios and attack-defense trees to provide a more in-depth discussion of some identified threats. We highlighted the relevance of a set of threats and attacks based on our extensive survey. For instance, DoS attacks are highly critical for all vertical applications discussed. We filled the gap in the literature regarding comprehensive discussions on threats and solutions for other vertical applications, including education.

Acknowledgments: The authors thank the Brazilian national telecommunications agency (Agência Nacional de Telecomunicações - ANATEL) for supporting this research. Moreover, the authors would like to thank all the Federal University of Campina Grande students who directly or indirectly participated in developing this work.

References

1. Salahdine, F.; Han, T.; Zhang, N. Security in 5G and beyond recent advances and future challenges. *Security and Privacy* **2023**, *6*, e271.
2. Lin, C.C.; Tsai, C.T.; Liu, Y.L.; Chang, T.T.; Chang, Y.S. Security and Privacy in 5G-IIoT Smart Factories: Novel Approaches, Trends, and Challenges. *Mobile Networks and Applications* **2023**, pp. 1–16.
3. Fragkos, D.; Makropoulos, G.; Sarantos, P.; Koumaras, H.; Charismiadis, A.S.; Tsolkas, D. 5G Vertical Application Enablers Implementation Challenges and Perspectives. 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), 2021, pp. 117–122. doi:10.1109/MeditCom49071.2021.9647460.
4. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Communications Surveys & Tutorials* **2020**, *22*, 196–248. doi:10.1109/COMST.2019.2933899.
5. Wan, L.; Guo, Z.; Chen, X. Enabling efficient 5G NR and 4G LTE coexistence. *IEEE Wireless Communications* **2019**, *26*, 6–8.
6. NSA. Potential Threat Vectors to 5g Infrastructure. Technical report, Cybersecurity & Infrastructure Security Agency, National Security Agency, and Office of the Director of Nacional Intelligence, 2021.
7. Sullivan, S.; Brighente, A.; Kumar, S.A.P.; Conti, M. 5G Security Challenges and Solutions: A Review by OSI Layers. *IEEE Access* **2021**, *9*, 116294–116314. doi:10.1109/ACCESS.2021.3105396.
8. Tanveer, J.; Haider, A.; Ali, R.; Kim, A. Machine Learning for Physical Layer in 5G and beyond Wireless Networks: A Survey. *Electronics* **2022**, *11*. doi:10.3390/electronics11010121.
9. Tang, Q.; Ermis, O.; Nguyen, C.D.; Oliveira, A.D.; Hirtzig, A. A Systematic Analysis of 5G Networks With a Focus on 5G Core Security. *IEEE Access* **2022**, *10*, 18298–18319. doi:10.1109/ACCESS.2022.3151000.
10. Suomalainen, J.; Juhola, A.; Shahabuddin, S.; Mämmelä, A.; Ahmad, I. Machine Learning Threatens 5G Security. *IEEE Access* **2020**, *8*, 190822–190842. doi:10.1109/ACCESS.2020.3031966.
11. Varga, P.; Peto, J.; Franko, A.; Balla, D.; Haja, D.; Janky, F.; Soos, G.; Ficzere, D.; Maliosz, M.; Toka, L. 5G support for Industrial IoT Applications— Challenges, Solutions, and Research gaps. *Sensors* **2020**, *20*. doi:10.3390/s20030828.
12. Wijethilaka, S.; Liyanage, M. Survey on Network Slicing for Internet of Things Realization in 5G Networks. *IEEE Communications Surveys & Tutorials* **2021**, *23*, 957–994. doi:10.1109/COMST.2021.3067807.
13. Wazid, M.; Das, A.K.; Shetty, S.; Gope, P.; Rodrigues, J.J.P.C. Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap. *IEEE Access* **2021**, *9*, 4466–4489. doi:10.1109/ACCESS.2020.3047895.
14. Sanchez-Gomez, J.; Carrillo, D.G.; Sanchez-Iborra, R.; Hernández-Ramos, J.L.; Granjal, J.; Marin-Perez, R.; Zamora-Izquierdo, M.A. Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions. *IEEE Access* **2020**, *8*, 216437–216460. doi:10.1109/ACCESS.2020.3041057.
15. Sharma, P.; Jain, S.; Gupta, S.; Chamola, V. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Networks* **2021**, *123*, 102685. doi:https://doi.org/10.1016/j.adhoc.2021.102685.
16. Zhang, J.; Yan, Z.; Fei, S.; Wang, M.; Li, T.; Wang, H. Is Today's End-to-End Communication Security Enough for 5G and Its Beyond? *IEEE Network* **2022**, *36*, 105–112. doi:10.1109/MNET.101.2100189.
17. Liu, J.; Shu, L.; Lu, X.; Liu, Y. Survey of Intelligent Agricultural IoT Based on 5G. *Electronics* **2023**, *12*, 2336.
18. Ahad, A.; Tahir, M.; Aman Sheikh, M.; Ahmed, K.I.; Mughees, A.; Numani, A. Technologies trend towards 5G network for smart health-care using IoT: A review. *Sensors* **2020**, *20*, 4047.
19. Hui, H.; Ding, Y.; Shi, Q.; Li, F.; Song, Y.; Yan, J. 5G network-based Internet of Things for demand response in smart grid: A survey on application potential. *Applied Energy* **2020**, *257*, 113972.

20. Ogbodo, E.U.; Abu-Mahfouz, A.M.; Kurien, A.M. A survey on 5G and LPWAN-IoT for improved smart cities and remote area applications: From the aspect of architecture and security. *Sensors* **2022**, *22*, 6313.
21. Hakak, S.; Gadekallu, T.R.; Maddikunta, P.K.R.; Ramu, S.P.; Parimala, M.; De Alwis, C.; Liyanage, M. Autonomous Vehicles in 5G and beyond: A Survey. *Vehicular Communications* **2022**, p. 100551.
22. Qiu, Q.; Liu, S.; Xu, S.; Yu, S. Study on security and privacy in 5g-enabled applications. *Wireless Communications and Mobile Computing* **2020**, *2020*, 1–15.
23. Valinevicius, A.; Zilys, M.; Kilius, S. Mobile Technologies Applications in Security Systems. 2007 29th International Conference on Information Technology Interfaces, 2007, pp. 657–662. doi:10.1109/ITI.2007.4283849.
24. Pal, S.; Bandyopadhyay, M.; Chowdhury Kolay, S.; Chattopadhyay, S. Remote Air Quality Sensing and Temperature Monitoring System using GSM for Smart City Application. 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), 2023, pp. 338–342. doi:10.1109/AISC56616.2023.10085138.
25. Benbatouche, A.; Kadri, B. Design and realization of low-cost solenoid valve remotely controlled, application in irrigation network. *Bulletin of Electrical Engineering and Informatics* **2022**.
26. Khan, M.A.; Jawed, S.F.; Khan, M.O.; Mazhar, O. An innovative approach towards E-health in development of tele auscultation system for heart using GSM mobile communication technology. 2013 IEEE 19th International Symposium for Design and Technology in Electronic Packaging (SIITME), 2013, pp. 201–204. doi:10.1109/SIITME.2013.6743673.
27. Baswa, M.; Karthik, R.; Natarajan, P.B.; Jyothi, K.; Annapurna, B. Patient health management system using e-health monitoring architecture. 2017 International Conference on Intelligent Sustainable Systems (ICISS), 2017, pp. 1120–1124. doi:10.1109/ISS1.2017.8389356.
28. Elgali, A.; Saad, A. An Industrial SC AD A System Remote Control Using Mobile Phones. 2022 IEEE 7th International Energy Conference (ENERGYCON), 2022, pp. 1–6. doi:10.1109/ENERGYCON53164.2022.9830195.
29. Jarwal, M.K.; Barun, A.; Singh, A.; Srivastava, A. Mobile Application based Tracking using GPS and GSM. 2022 8th International Conference on Signal Processing and Communication (ICSC), 2022, pp. 153–156. doi:10.1109/ICSC56524.2022.10009250.
30. Phuoc Dai, N.H.; Ruiz, L.; Zoltán, R. Mobile Technology Security Concerns and NESAS as a Solution. 2022 IEEE 26th International Conference on Intelligent Engineering Systems (INES), 2022, pp. 000127–000130. doi:10.1109/INES56734.2022.9922653.
31. Clavier, C. An improved SCARE cryptanalysis against a secret A3/A8 GSM algorithm. Information Systems Security: Third International Conference, ICISS 2007, Delhi, India, December 16-20, 2007. Proceedings 3. Springer, 2007, pp. 143–155.
32. Wamyil, M.; Mu'Azu, M. Gsm Networks: A Review Of Security Threats And Mitigation Measures. *Information Manager (The)* **2008**, *6*. doi:10.4314/tim.v6i1.27226.
33. Toorani, M.; Beheshti, A. Solutions to the GSM Security Weaknesses. 2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies. IEEE, 2008. doi:10.1109/ngmast.2008.88.
34. Qiu, R.; Zhu, W.; Zhang, Y.Q. Third-generation and beyond (3.5G) wireless networks and its applications. 2002 IEEE International Symposium on Circuits and Systems (ISCAS), 2002, Vol. 1, pp. I–I. doi:10.1109/ISCAS.2002.1009772.
35. Zhang, Y.; Zhao, G.; Zhang, Y. A Smart Home Security System Based on 3G. 2009 International Forum on Computer Science-Technology and Applications, 2009, Vol. 2, pp. 291–294. doi:10.1109/IFCSTA.2009.193.
36. Sun, J.; Lin, D.; Zhao, P.; Zhang, Y. Based on Internet/2G/3G Converged Network Intelligent Image Monitoring System. 2010 International Forum on Information Technology and Applications, 2010, Vol. 2, pp. 277–279. doi:10.1109/IFITA.2010.248.
37. Xu, F.; Zhou, Q. The application of 3G technology in water resources monitoring system. 5th International Conference on Computer Sciences and Convergence Information Technology, 2010, pp. 977–980. doi:10.1109/ICCIT.2010.5711202.
38. Kang, J.; Shin, I.H.; Koo, Y.; Jung, M.Y.; Suh, G.J.; Kim, H.C. HSDPA (3.5G)-Based Ubiquitous Integrated Biotelemetry System for Emergency Care. 2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2007, pp. 3665–3668. doi:10.1109/IEMBS.2007.4353126.

39. Yamamoto, H.; Fujii, T.; Ha, P.T.T.; Yamazaki, K. New development of remote control system for air vehicle using 3G cellular network. 16th International Conference on Advanced Communication Technology, 2014, pp. 456–461. doi:10.1109/ICACT.2014.6779002.
40. Ye, H.; Ding, G. A digital vehicle monitoring system based on 3G for public security. 2010 International Conference on Computer and Information Application, 2010, pp. 146–148. doi:10.1109/ICCIA.2010.6141557.
41. Yundong, L.; Weigang, Z. Intelligent bridge monitoring system based on 3G. 2011 International Conference on Consumer Electronics, Communications and Networks (CECNet), 2011, pp. 426–429. doi:10.1109/CECNET.2011.5768621.
42. Jianqiang, K.; Zhaochenxu.; Kanghaiping. Research and application of 3G electrical safety job site intelligent monitoring device. 2014 China International Conference on Electricity Distribution (CICED), 2014, pp. 745–747. doi:10.1109/CICED.2014.6991810.
43. Yun, H.; hua, P.A.; zhi, Z.S. Intelligent video monitoring system based on 3G. 2010 International Conference on Educational and Network Technology, 2010, pp. 135–138. doi:10.1109/ICENT.2010.5532145.
44. Lundevall, M.; Olin, B.; Olsson, J.; Wiberg, N.; Wanstedt, S.; Eriksson, J.; Eng, F. Streaming applications over HSDPA in mixed service scenarios. IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004, 2004, Vol. 2, pp. 841–845 Vol. 2. doi:10.1109/VETECF.2004.1400139.
45. Li, H.; Guo, S.; Zheng, K.; Chen, Z.; Zhang, Z.; Du, X. Security analysis and defense strategy on access domain in 3G. 2009 First International Conference on Information Science and Engineering, 2009, pp. 1851–1854. doi:10.1109/ICISE.2009.1050.
46. Lian, Y.; Zhang, W.; Jiang, J. The architecture of the remote control system oriented to 4G networks. 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp. 1386–1390. doi:10.1109/CECNet.2012.6201863.
47. Ting, C.; Yun, X.; Xiangmo, Z.; Tao, G.; Zhigang, X. 4G UAV communication system and hovering height optimization for public safety. 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), 2017, pp. 1–6. doi:10.1109/HealthCom.2017.8210823.
48. Naveed, M.; Qazi, S.; Khawaja, B.A. UAV-based Life-Saving Solution For Police To Maintain Social-Distancing During Covid-19 Pandemic Using 4G-LTE Technology. 2021 International Conference on Communication Technologies (ComTech), 2021, pp. 28–32. doi:10.1109/ComTech52583.2021.9616854.
49. Lin, B.S.P.; Tsai, W.H.; Wu, C.; Hsu, P.; Huang, J.; Liu, T.H. The Design of Cloud-Based 4G/LTE for Mobile Augmented Reality with Smart Mobile Devices. 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, 2013, pp. 561–566. doi:10.1109/SOSE.2013.57.
50. Hiramatsu, K.; Nakao, S.; Hoshino, M.; Imamura, D. Technology evolutions in LTE/LTE-advanced and its applications. 2010 IEEE International Conference on Communication Systems, 2010, pp. 161–165. doi:10.1109/ICCS.2010.5686376.
51. Widjaja, D.; Damar Wisya Wicaksana, D. Performance Evaluation of Body Temperature Data Transmission Using Turbo Codes in 4G-LTE. 2020 2nd International Conference on Industrial Electrical and Electronics (ICIEE), 2020, pp. 179–182. doi:10.1109/ICIEE49813.2020.9276959.
52. Gözde, H.; Taplamacıoğlu, M.C.; Arı, M.; Shalaf, H. 4G/LTE technology for smart grid communication infrastructure. 2015 3rd International Istanbul Smart Grid Congress and Fair (ICSG), 2015, pp. 1–4. doi:10.1109/SGCF.2015.7354914.
53. Cao, J.; Ma, M.; Li, H.; Zhang, Y.; Luo, Z. A Survey on Security Aspects for LTE and LTE-A Networks. *IEEE Communications Surveys & Tutorials* **2014**, *16*, 283–302. doi:10.1109/SURV.2013.041513.00174.
54. Tahir, M.; Habaebi, M.H.; Dabbagh, M.; Mughees, A.; Ahad, A.; Ahmed, K.I. A Review on Application of Blockchain in 5G and Beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities. *IEEE Access* **2020**, *8*, 115876–115904. doi:10.1109/ACCESS.2020.3003020.
55. Liyanage, M.; Salo, J.; Braeken, A.; Kumar, T.; Seneviratne, S.; Ylianttila, M. 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF), 2018, pp. 197–203. doi:10.1109/5GWF.2018.8516981.
56. Sharma, A.; Balasubramanian, V.; Jolfaei, A. Security Challenges and Solutions for 5G HetNet. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1318–1323. doi:10.1109/TrustCom50675.2020.00177.
57. Nieto, A.; Acien, A.; Lopez, J. Capture the RAT: Proximity-Based Attacks in 5G Using the Routine Activity Theory. 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and

Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2018, pp. 520–527. doi:10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00100.

58. Dutta, A.; Hammad, E. 5G Security Challenges and Opportunities: A System Approach. 2020 IEEE 3rd 5G World Forum (5GWF), 2020, pp. 109–114. doi:10.1109/5GWF49715.2020.9221122.
59. Dey, A.; Nandi, S.; Sarkar, M. Security Measures in IOT based 5G Networks. 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 561–566. doi:10.1109/ICICT43934.2018.9034365.
60. Lichtman, M.; Rao, R.; Marojevic, V.; Reed, J.; Jover, R.P. 5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation. 2018 IEEE International Conference on Communications Workshops (ICC Workshops), 2018, pp. 1–6. doi:10.1109/ICCW.2018.8403769.
61. Liyanage, M.; Abro, A.B.; Ylianttila, M.; Gurtov, A. Opportunities and Challenges of Software-Defined Mobile Networks in Network Security. *IEEE Security & Privacy* **2016**, *14*, 34–44. doi:10.1109/MSP.2016.82.
62. Ksentini, A.; Frangoudis, P.A. Toward Slicing-Enabled Multi-Access Edge Computing in 5G. *IEEE Network* **2020**, *34*, 99–105. doi:10.1109/MNET.001.1900261.
63. Ghafoor, A.; Shah, M.A.; Mushtaq, M.; Iftikhar, M. 5G SECURITY THREATS AFFECTING DIGITAL ECONOMY AND THEIR COUNTERMEASURES. Competitive Advantage in the Digital Economy (CADE 2021), 2021, Vol. 2021, pp. 70–77. doi:10.1049/icp.2021.2419.
64. Zhang, A.; Lin, X. Security-Aware and Privacy-Preserving D2D Communications in 5G. *IEEE Network* **2017**, *31*, 70–77. doi:10.1109/MNET.2017.1600290.
65. Liyanage, M.; Ahmed, I.; Ylianttila, M.; Santos, J.L.; Kantola, R.; Perez, O.L.; Itzazelaia, M.U.; Montes De Oca, E.; Valtierra, A.; Jimenez, C. Security for Future Software Defined Mobile Networks. 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, pp. 256–264. doi:10.1109/NGMAST.2015.43.
66. Mazin, A.; Davaslioglu, K.; Gitlin, R.D. Secure key management for 5G physical layer security. 2017 IEEE 18th Wireless and Microwave Technology Conference (WAMICON), 2017, pp. 1–5. doi:10.1109/WAMICON.2017.7930246.
67. Settembre, M. A 5G Core Network Challenge: Combining Flexibility and Security. 2021 AEIT International Annual Conference (AEIT), 2021, pp. 1–6. doi:10.23919/AEIT53387.2021.9627014.
68. Thantharate, A.; Paropkari, R.; Walunj, V.; Beard, C.; Kankariya, P. Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond. 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), 2020, pp. 0852–0857. doi:10.1109/CCWC47524.2020.9031158.
69. Barrachina, J.; Garrido, P.; Fogue, M.; Martinez, F.J.; Cano, J.C.; Calafate, C.T.; Manzoni, P. Road side unit deployment: A density-based approach. *IEEE Intelligent Transportation Systems Magazine* **2013**, *5*, 30–39.
70. Bajpai, A.; Balodi, A. *Applications of 5G and Beyond in Smart Cities*; CRC Press, 2023.
71. Abdel-Malek, M.A.; Akkaya, K.; Bhuyan, A.; Ibrahim, A.S. A Proxy Signature-Based Drone Authentication in 5G D2D Networks. 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), 2021, pp. 1–7. doi:10.1109/VTC2021-Spring51267.2021.9448962.
72. Shin, D.; Yun, K.; Kim, J.; Astillo, P.V.; Kim, J.N.; You, I. A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks. *IEEE Access* **2019**, *7*, 142531–142550. doi:10.1109/ACCESS.2019.2943929.
73. Nowak, T.W.; Sepczuk, M.; Kotulski, Z.; Niewolski, W.; Artych, R.; Bocianiak, K.; Osko, T.; Wary, J.P. Verticals in 5G MEC-use cases and security challenges. *IEEE Network* **2021**, *9*, 87251–87298. doi:10.1109/ACCESS.2021.3088374.
74. Swami, M.; Swami, S. The Role of 5G in Smart Transportation. In *Applications of 5G and Beyond in Smart Cities*; CRC Press, 2023; pp. 27–42.
75. Eltahlawy, A.M.; Azer, M.A. Using Blockchain Technology for the Internet Of Vehicles. 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), 2021, pp. 54–61. doi:10.1109/MIUCC52538.2021.9447622.
76. Falchetti, A.; Azurdia-Meza, C.; Cespedes, S. Vehicular cloud computing in the dawn of 5G. 2015 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), 2015, pp. 301–305. doi:10.1109/Chilecon.2015.7400392.

77. Moulahi, T.; Zidi, S.; Alabdulatif, A.; Atiquzzaman, M. Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus. *IEEE Access* **2021**, *9*, 99595–99605. doi:10.1109/ACCESS.2021.3095962.
78. Ayoub, T.; Mazri, T. Security Challenges in V2I Architectures and Proposed Solutions. 2018 IEEE 5th International Congress on Information Science and Technology (CiSt), 2018, pp. 594–599. doi:10.1109/CIST.2018.8596599.
79. Lu, R.; Zhang, L.; Ni, J.; Fang, Y. 5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy. *Proceedings of the IEEE* **2020**, *108*, 373–389. doi:10.1109/JPROC.2019.2948302.
80. Aljeri, N.; Boukerche, A. Mobility Management in 5G-Enabled Vehicular Networks: Models, Protocols, and Classification. *ACM Comput. Surv.* **2020**, *53*. doi:10.1145/3403953.
81. Huang, J.; Qian, Y.; Hu, R.Q. Secure and Efficient Privacy-Preserving Authentication Scheme for 5G Software Defined Vehicular Networks. *IEEE Transactions on Vehicular Technology* **2020**, *69*, 8542–8554. doi:10.1109/TVT.2020.2996574.
82. Hasan, R.; Hasan, R. Towards a Threat Model and Privacy Analysis for V2P in 5G Networks. 2021 IEEE 4th 5G World Forum (5GWF), 2021, pp. 383–387. doi:10.1109/5GWF52925.2021.00074.
83. Asensio, R.; Benzaid, C.; Alemany, P.; Ayed, D.; Christopoulou, M.; Dangerville, C.; Gür, G.; La, V.H.; Lefebvre, V.; E. Montes de Oca, R.M.; Nguyen, H.; Nguyen, M.; Ortiz, J.; Pastor, A.; Porambage, P.; Santinelli, G.; W. Soussi, T.T.; Vilalta, R.; Zarca, A. Evolution of 5G Cyber Threats and Security Solutions. Technical report, INSPIRE-5Gplus, 2022.
84. Suomalainen, J.; Julku, J.; Vehkaperä, M.; Posti, H. Securing public safety communications on commercial and tactical 5G networks: A survey and future research directions. *IEEE Open Journal of the Communications Society* **2021**, *2*, 1590–1615. doi:10.1109/OJCOMS.2021.3093529.
85. Suomalainen, J.; Julku, J.; Vehkaperä, M.; Posti, H. Securing Public Safety Communications on Commercial and Tactical 5G Networks: A Survey and Future Research Directions. *IEEE Open Journal of the Communications Society* **2021**, *2*, 1590–1615. doi:10.1109/OJCOMS.2021.3093529.
86. Elmasry, G.; Corwin, P. Hiding the RF Signal Signature in Tactical 5G. MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM), 2021, pp. 733–738. doi:10.1109/MILCOM52596.2021.9652968.
87. Makropoulos, G.; Fragkos, D.; Koumaras, H.; Alonistioti, N.; Kaloxylos, A.; Koumaras, V.; Dounia, T.; Sakkas, C.; Tsolkas, D. 5G Network Programmability Enabling Industry 4.0 Transformation. In *Opportunities and Challenges of Industrial IoT in 5G and 6G Networks*; IGI Global, 2023; pp. 119–137.
88. Corici, A.A.; Corici, M.; Troudt, E.; Riemer, B.; Magedanz, T. Framework for Trustful Handover of M2M devices between Security Domains. 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 2020, pp. 102–109. doi:10.1109/ICIN48450.2020.9059457.
89. Abdel-Basset, M.; Hawash, H.; Sallam, K. Federated threat-hunting approach for microservice-based industrial cyber-physical system. *IEEE Transactions on Industrial Informatics* **2021**, *18*, 1905–1917. doi:10.1109/TII.2021.3091150.
90. Abdel-Basset, M.; Hawash, H.; Sallam, K. Federated Threat-Hunting Approach for Microservice-Based Industrial Cyber-Physical System. *IEEE Transactions on Industrial Informatics* **2022**, *18*, 1905–1917. doi:10.1109/TII.2021.3091150.
91. Selvam, P.; Sridhar, J.; Ganesan, V.; Ravindraiah, R. The future of Industry 4.0: private 5G networks. In *Advanced Signal Processing for Industry 4.0, Volume 1: Evolution, communication protocols, and applications in manufacturing systems*; IOP Publishing Bristol, UK, 2023; pp. 3–1.
92. FORTINET. Securing 5G Private Mobile Networks. Technical report, FORTINET, 2021.
93. Jamshidi, M.; Yahya, S.I.; Nouri, L.; Hashemi-Dezaki, H.; Rezaei, A.; Chaudhary, M.A. A High-Efficiency Diplexer for Sustainable 5G-Enabled IoT in Metaverse Transportation System and Smart Grids. *Symmetry* **2023**, *15*, 821.
94. Ranaweera, P.; Jurcut, A.; Liyanage, M. MEC-Enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures. *ACM Comput. Surv.* **2021**, *54*. doi:10.1145/3474552.
95. Xuesong, H.; Wei, L.; Tao, Z.; Haidong, H.; Kangle, Y.; Pei, P. An Endogenous Security Protection Framework adapted to 5G MEC in Power Industry. 2021 China Automation Congress (CAC), 2021, pp. 5155–5159. doi:10.1109/CAC53003.2021.9728395.
96. Devi, D.H.; Duraisamy, K.; Armghan, A.; Alsharari, M.; Aliqab, K.; Sorathiya, V.; Das, S.; Rashid, N. 5g technology in healthcare and wearable devices: A review. *Sensors* **2023**, *23*, 2519.

97. Menon, S.P.; Shukla, P.K.; Sethi, P.; Alasiry, A.; Marzougui, M.; Alouane, M.T.H.; Khan, A.A. An intelligent diabetic patient tracking system based on machine learning for E-health applications. *Sensors* **2023**, *23*, 3004.
98. Le, T.V.; Hsu, C.L. An Anonymous Key Distribution Scheme for Group Healthcare Services in 5G-Enabled Multi-Server Environments. *IEEE Access* **2021**, *9*, 53408–53422. doi:10.1109/ACCESS.2021.3070641.
99. Fatima, R.; Manal, R.; Tomader, M. Cryptography in E-Health Using 5G Based IOT: A Comparison Study. Proceedings of the 4th International Conference on Big Data and Internet of Things; Association for Computing Machinery: New York, NY, USA, 2020; BDIoT'19. doi:10.1145/3372938.3372955.
100. Le, T.V.; Hsu, C.L. An anonymous key distribution scheme for group healthcare services in 5G-enabled multi-server environments. *IEEE Access* **2021**, *9*, 53408–53422. doi:10.1109/ACCESS.2021.3070641.
101. Mangra, N.; Behmann, F.; Thakur, A.; Popescu, A.; Suciu Jr, G.; Giannattasio, G.; Uppal, R.; Montlouis, W. White Paper-5G Enabled Agriculture Ecosystem: Food Supply Chain, Rural Development, and Climate Resiliency. *5G Enabled Agriculture Ecosystem: Food Supply Chain, Rural Development, and Climate Resiliency* **2023**, pp. 1–40.
102. Nowak, T.W.; Sepczuk, M.; Kotulski, Z.; Niewolski, W.; Artych, R.; Bocianiak, K.; Osko, T.; Wary, J.P. Verticals in 5G MEC-Use Cases and Security Challenges. *IEEE Access* **2021**, *9*, 87251–87298. doi:10.1109/ACCESS.2021.3088374.
103. Yu, L.; Enzheng, W. 5G network education and smart campus based on heterogeneous distributed platform and multi-scheduling optimization. *Soft Computing* **2023**, pp. 1–12.
104. Akhunzada, A.; Islam, S.u.; Zeadally, S. Securing Cyberspace of Future Smart Cities with 5G Technologies. *IEEE Network* **2020**, *34*, 336–342. doi:10.1109/MNET.001.1900559.
105. Mamolar, A.S.; Pervez, Z.; Wang, Q.; Alcaraz-Calero, J.M. Towards the Detection of Mobile DDoS Attacks in 5G Multi-Tenant Networks. 2019 European Conference on Networks and Communications (EuCNC), 2019, pp. 273–277. doi:10.1109/EuCNC.2019.8801975.
106. Nasir, A.A.; Tuan, H.D.; Nguyen, H.H.; Nguyen, N.M. Physical Layer Security by Exploiting Interference and Heterogeneous Signaling. *IEEE Wireless Communications* **2019**, *26*, 26–31. doi:10.1109/MWC.001.1900048.
107. Bhuyan, A.; Guvenç, I.; Dai, H.; Sichitiu, M.L.; Singh, S.; Rahmati, A.; Maeng, S.J. Secure 5G Network for a Nationwide Drone Corridor. 2021 IEEE Aerospace Conference (50100), 2021, pp. 1–10. doi:10.1109/AERO50100.2021.9438162.
108. Gokul, N.; Sankaran, S. Modeling and Defending against Resource Depletion Attacks in 5G Networks. 2021 IEEE 18th India Council International Conference (INDICON), 2021, pp. 1–7. doi:10.1109/INDICON52576.2021.9691522.
109. Lin, M.; Huang, Q.; de Cola, T.; Wang, J.B.; Wang, J.; Guizani, M.; Wang, J.Y. Integrated 5G-Satellite Networks: A Perspective on Physical Layer Reliability and Security. *IEEE Wireless Communications* **2020**, *27*, 152–159. doi:10.1109/MWC.001.2000143.
110. Yerrapragada, A.K.; Ormond, P.; Kelley, B. On the Application of Key-Based Physical Layer Security in 5G Heterogeneous Networks. MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), 2019, pp. 1–6. doi:10.1109/MILCOM47813.2019.9020882.
111. Li, A. Enhancing the Physical Layer Security of Cooperative NOMA System. 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2019, pp. 2194–2198. doi:10.1109/ITNEC.2019.8729389.
112. Roth, S.; Tomasin, S.; Maso, M.; Sezgin, A. Localization Attack by Precoder Feedback Overhearing in 5G Networks and Countermeasures. *IEEE Transactions on Wireless Communications* **2021**, *20*, 4100–4112. doi:10.1109/TWC.2021.3055851.
113. van den Broek, F.; Verdult, R.; de Ruiter, J. Defeating IMSI Catchers. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security; Association for Computing Machinery: New York, NY, USA, 2015; CCS '15, p. 340–351. doi:10.1145/2810103.2813615.
114. Schinianakis, D.; Trapero, R.; Michalopoulos, D.S.; Crespo, B.G.N. Security Considerations in 5G Networks: A Slice-Aware Trust Zone Approach. 2019 IEEE Wireless Communications and Networking Conference (WCNC), 2019, pp. 1–8. doi:10.1109/WCNC.2019.8885658.
115. Fang, H.; Wang, X.; Tomasin, S. Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks. *IEEE Wireless Communications* **2019**, *26*, 55–61. doi:10.1109/MWC.001.1900054.

116. Moreira, C.M.; Kaddoum, G.; Bou-Harb, E. Cross-Layer Authentication Protocol Design for Ultra-Dense 5G HetNets. 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1–7. doi:10.1109/ICC.2018.8422404.
117. Moudoud, H.; Khoukhi, L.; Cherkaoui, S. Prediction and Detection of FDIA and DDoS Attacks in 5G Enabled IoT. *IEEE Network* **2021**, *35*, 194–201. doi:10.1109/MNET.011.2000449.
118. Ali, A.; Ware, A. Anomaly Based IDS Via Customised CUSUM Algorithm for Industrial Communication Systems. 2021 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), 2021, pp. 31–36. doi:10.1109/MENACOMM50742.2021.9678305.
119. Feng, C.; Yu, K.; Bashir, A.K.; Al-Otaibi, Y.D.; Lu, Y.; Chen, S.; Zhang, D. Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach. *IEEE Network* **2021**, *35*, 130–137. doi:10.1109/MNET.011.2000223.
120. Li, M.; Zhu, L.; Zhang, Z.; Lal, C.; Conti, M.; Martinelli, F. Privacy for 5G-Supported Vehicular Networks. *IEEE Open Journal of the Communications Society* **2021**, *2*, 1935–1956. doi:10.1109/OJCOMS.2021.3103445.
121. Zhang, Y.; Li, J.; Zheng, D.; Li, P.; Tian, Y. Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice. *Journal of Network and Computer Applications* **2018**, *122*, 50–60. doi:https://doi.org/10.1016/j.jnca.2018.07.017.
122. CISA.; NSA.; of the Director of National Intelligence, O. Potential Threat Vectors to 5G Infrastructure. Technical report, Department of Computer Science, Michigan State University, 2021.
123. Abdalla, A.S.; Shang, B.; Marojevic, V.; Liu, L. Performance Evaluation of Aerial Relaying Systems for Improving Secrecy in Cellular Networks. 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), 2020, pp. 1–5. doi:10.1109/VTC2020-Fall49728.2020.9348686.
124. Chen, B.; Zhu, C.; Li, W.; Wei, J.; Leung, V.C.M.; Yang, L.T. Original Symbol Phase Rotated Secure Transmission Against Powerful Massive MIMO Eavesdropper. *IEEE Access* **2016**, *4*, 3016–3025. doi:10.1109/ACCESS.2016.2580673.
125. Benzid, D.; Kadoch, M.; Cheriet, M. Raptor Code based on punctured LDPC for Secrecy in Massive MiMo. 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019, pp. 1884–1889. doi:10.1109/IWCMC.2019.8766490.
126. Lin, C.H.; Wu, C.C.; Chen, K.F.; Lee, T.S. A Variational Autoencoder-Based Secure Transceiver Design Using Deep Learning. GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1–7. doi:10.1109/GLOBECOM42002.2020.9348041.
127. Barik, D.; Sanyal, J.; Samanta, T. Prevention of Denial-of-Service Attacks in 5GD2D Wireless Communication Networks Employing Double Auction Game Based Resource Trading. 2020 IEEE 3rd 5G World Forum (5GWF), 2020, pp. 239–244. doi:10.1109/5GWF49715.2020.9221441.
128. Fang, L.; Zhao, B.; Li, Y.; Liu, Z.; Ge, C.; Meng, W. Countermeasure Based on Smart Contracts and AI against DoS/DDoS Attack in 5G Circumstances. *IEEE Network* **2020**, *34*, 54–61. doi:10.1109/MNET.021.1900614.
129. Tan, Z.; Ding, B.; Zhang, Z.; Li, Q.; Guo, Y.; Lu, S. Device-Centric Detection and Mitigation of Diameter Signaling Attacks against Mobile Core. 2021 IEEE Conference on Communications and Network Security (CNS), 2021, pp. 29–37. doi:10.1109/CNS53000.2021.9705031.
130. Vidal, J.M.; Monge, M.A.S.; Villalba, L.J.G. Detecting Workload-Based and Instantiation-Based Economic Denial of Sustainability on 5G Environments. Proceedings of the 13th International Conference on Availability, Reliability and Security; Association for Computing Machinery: New York, NY, USA, 2018; ARES 2018. doi:10.1145/3230833.3233247.
131. Cabaj, K.; Gregorczyk, M.; Mazurczyk, W.; Nowakowski, P.; Żórawski, P. SDN-Based Mitigation of Scanning Attacks for the 5G Internet of Radio Light System. Proceedings of the 13th International Conference on Availability, Reliability and Security; Association for Computing Machinery: New York, NY, USA, 2018; ARES 2018. doi:10.1145/3230833.3233248.
132. Norrman, K.; Näslund, M.; Dubrova, E. Protecting IMSI and User Privacy in 5G Networks. Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, BEL, 2016; MobiMedia '16, p. 159–166.
133. Chopra, G.; Jha, R.K.; Jain, S. TPA: Prediction of Spoofing Attack Using Thermal Pattern Analysis in Ultra Dense Network for High Speed Handover Scenario. *IEEE Access* **2018**, *6*, 66268–66284. doi:10.1109/ACCESS.2018.2875921.

134. Li, W.; Wang, N.; Jiao, L.; Zeng, K. Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks. *IEEE Access* **2021**, *9*, 60419–60432. doi:10.1109/ACCESS.2021.3073115.
135. Wang, N.; Jiao, L.; Wang, P.; Li, W.; Zeng, K. Exploiting Beam Features for Spoofing Attack Detection in mmWave 60-GHz IEEE 802.11ad Networks. *IEEE Transactions on Wireless Communications* **2021**, *20*, 3321–3335. doi:10.1109/TWC.2021.3049160.
136. Dang, Y.; Benzaïd, C.; Shen, Y.; Taleb, T. GPS Spoofing Detector with Adaptive Trustable Residence Area for Cellular based-UAVs. GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1–6. doi:10.1109/GLOBECOM42002.2020.9348030.
137. Pérez, M.G.; Celdrán, A.H.; Ippoliti, F.; Giardina, P.G.; Bernini, G.; Alaez, R.M.; Chirivella-Perez, E.; Clemente, F.J.G.; Pérez, G.M.; Kraja, E.; Carrozzo, G.; Calero, J.M.A.; Wang, Q. Dynamic Reconfiguration in 5G Mobile Networks to Proactively Detect and Mitigate Botnets. *IEEE Internet Computing* **2017**, *21*, 28–36. doi:10.1109/MIC.2017.3481345.
138. Jagannath, A.; Jagannath, J.; Drozd, A. High Rate-Reliability Beamformer Design for 2×2 Mimo-OFDM System Under Hostile Jamming. 2020 29th International Conference on Computer Communications and Networks (ICCCN), 2020, pp. 1–9. doi:10.1109/ICCCN49398.2020.9209635.
139. Hachimi, M.; Kaddoum, G.; Gagnon, G.; Illy, P. Multi-stage Jamming Attacks Detection using Deep Learning Combined with Kernelized Support Vector Machine in 5G Cloud Radio Access Networks. 2020 International Symposium on Networks, Computers and Communications (ISNCC), 2020, pp. 1–5. doi:10.1109/ISNCC49221.2020.9297290.
140. Arjoune, Y.; Salahdine, F.; Islam, M.S.; Ghribi, E.; Kaabouch, N. A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication. 2020 International Conference on Information Networking (ICOIN), 2020, pp. 459–464. doi:10.1109/ICOIN48656.2020.9016462.
141. Wang, N.; Jiao, L.; Alipour-Fanid, A.; Dabaghchian, M.; Zeng, K. Pilot Contamination Attack Detection for NOMA in 5G mm-Wave Massive MIMO Networks. *IEEE Transactions on Information Forensics and Security* **2020**, *15*, 1363–1378. doi:10.1109/TIFS.2019.2939742.
142. Wang, N.; Li, W.; Alipour-Fanid, A.; Jiao, L.; Dabaghchian, M.; Zeng, K. Pilot Contamination Attack Detection for 5G MmWave Grant-Free IoT Networks. *IEEE Transactions on Information Forensics and Security* **2021**, *16*, 658–670. doi:10.1109/TIFS.2020.3017932.
143. Adat, V.; Politis, I.; Tselios, C.; Kotsopoulos, S. Blockchain Enhanced SECRET Small Cells for the 5G Environment. 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1–6. doi:10.1109/CAMAD.2019.8858457.
144. Adat Vasudevan, V.; Tselios, C.; Politis, I. On Security Against Pollution Attacks in Network Coding Enabled 5G Networks. *IEEE Access* **2020**, *8*, 38416–38437. doi:10.1109/ACCESS.2020.2975761.
145. Vasudevan, V.A.; Akhtar, T.; Tselios, C.; Politis, I.; Kotsopoulos, S. Study of Secure Network Coding Enabled Mobile Small Cells. ICC 2021 - IEEE International Conference on Communications, 2021, pp. 1–5. doi:10.1109/ICC42927.2021.9500614.
146. Hakiri, A.; Dezfouli, B. Towards a Blockchain-SDN Architecture for Secure and Trustworthy 5G Massive IoT Networks. Proceedings of the 2021 ACM International Workshop on Software Defined Networks & Network Function Virtualization Security; Association for Computing Machinery: New York, NY, USA, 2021; SDN-NFV Sec'21, p. 11–18. doi:10.1145/3445968.3452090.
147. Sattar, D.; Matrawy, A. Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices. 2019 IEEE Conference on Communications and Network Security (CNS), 2019, pp. 82–90. doi:10.1109/CNS.2019.8802852.
148. Li, H.; Wang, L. Online orchestration of cooperative defense against DDoS attacks for 5G MEC. 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1–6. doi:10.1109/WCNC.2018.8377309.
149. Ettiane, R.; Chaoub, A.; Elkouch, R. Robust detection of signaling DDoS threats for more secure machine type communications in next generation mobile networks. 2018 19th IEEE Mediterranean Electrotechnical Conference (MELECON), 2018, pp. 62–67. doi:10.1109/MELCON.2018.8379069.
150. Tan, X.; Li, H.; Wang, L.; Xu, Z. Global Orchestration of Cooperative Defense against DDoS Attacks for MEC. 2019 IEEE Wireless Communications and Networking Conference (WCNC), 2019, pp. 1–6. doi:10.1109/WCNC.2019.8885499.

151. Huang, H.; Hu, L.; Chu, J.; Cheng, X. An Authentication Scheme to Defend Against UDP DrDoS Attacks in 5G Networks. *IEEE Access* **2019**, *7*, 175970–175979. doi:10.1109/ACCESS.2019.2957565.
152. Chen, X.; Feng, W.; Ma, Y.; Ge, N.; Wang, X. Preventing DRDoS Attacks in 5G Networks: a New Source IP Address Validation Approach. GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1–6. doi:10.1109/GLOBECOM42002.2020.9322314.
153. Torroglosa-Garcia, E.M.; Calero, J.M.A.; Bernabe, J.B.; Skarmeta, A. Enabling Roaming Across Heterogeneous IoT Wireless Networks: LoRaWAN MEETS 5G. *IEEE Access* **2020**, *8*, 103164–103180. doi:10.1109/ACCESS.2020.2998416.
154. Corici, A.A.; Shashi, Y.; Corici, M.; Shrestha, R.; Guzman, D. Enabling Dynamic IoT Security Domains: Cellular Core Network and Device Management Meet Authentication Framework. 2019 Global IoT Summit (GIoTS), 2019, pp. 1–6. doi:10.1109/GIOTS.2019.8766390.
155. Ni, J.; Lin, X.; Shen, X.S. Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT. *IEEE Journal on Selected Areas in Communications* **2018**, *36*, 644–657. doi:10.1109/JSAC.2018.2815418.
156. Sharma, S.; Satapathy, S.; Singh, S.; Sahu, A.K.; Obaidat, M.S.; Saxena, S.; Puthal, D. Secure Authentication Protocol for 5G Enabled IoT Network. 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2018, pp. 621–626. doi:10.1109/PDGC.2018.8745799.
157. Ali, A.; Lin, Y.D.; Li, C.Y.; Lai, Y.C. Transparent 3rd-Party Authentication with Application Mobility for 5G Mobile Edge Computing. 2020 European Conference on Networks and Communications (EuCNC), 2020, pp. 219–224. doi:10.1109/EuCNC48522.2020.9200937.
158. Sutrala, A.K.; Obaidat, M.S.; Saha, S.; Das, A.K.; Alazab, M.; Park, Y. Authenticated Key Agreement Scheme With User Anonymity and Untraceability for 5G-Enabled Softwarized Industrial Cyber-Physical Systems. *IEEE Transactions on Intelligent Transportation Systems* **2022**, *23*, 2316–2330. doi:10.1109/TITS.2021.3056704.
159. Ouaissa, M.; Ouaissa, M. An Improved Privacy Authentication Protocol for 5G Mobile Networks. 2020 International Conference on Advances in Computing, Communication & Materials (ICACCM), 2020, pp. 136–143. doi:10.1109/ICACCM50413.2020.9212910.
160. Abdel-Malek, M.A.; Akkaya, K.; Bhuyan, A.; Cebe, M.; Ibrahim, A.S. Enabling Second Factor Authentication for Drones in 5G using Network Slicing. 2020 IEEE Globecom Workshops (GC Wkshps, 2020, pp. 1–6. doi:10.1109/GCWkshps50303.2020.9367441.
161. Matos, B.; Dzogovic, B.; Feng, B.; Do, V.T.; Jacot, N.; Van Do, T. Towards Achieving a Secure Authentication Mechanism for IoT Devices in 5G Networks. 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2019, pp. 130–135. doi:10.1109/CSCloud/EdgeCom.2019.000-7.
162. Han, B.; Wong, S.; Mannweiler, C.; Dohler, M.; Schotten, H.D. Security Trust Zone in 5G networks. 2017 24th International Conference on Telecommunications (ICT), 2017, pp. 1–5. doi:10.1109/ICT.2017.7998270.
163. Blanc, G.; Kheir, N.; Ayed, D.; Lefebvre, V.; de Oca, E.M.; Bisson, P. Towards a 5G Security Architecture: Articulating Software-Defined Security and Security as a Service. Proceedings of the 13th International Conference on Availability, Reliability and Security; Association for Computing Machinery: New York, NY, USA, 2018; ARES 2018. doi:10.1145/3230833.3233251.
164. Fernández Maimó, L.; Perales Gómez, L.; García Clemente, F.J.; Gil Pérez, M.; Martínez Pérez, G. A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks. *IEEE Access* **2018**, *6*, 7700–7712. doi:10.1109/ACCESS.2018.2803446.
165. Vijay, A.; Umadevi, K. Secured AI guided Architecture for D2D Systems of Massive MIMO deployed in 5G Networks. 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 468–472. doi:10.1109/ICOEI.2019.8862712.
166. Siddiqui, M.; Escalona, E.; Trouva, E.; Kourtis, M.; Kritharidis, D.; Katsaros, K.; Spirou, S.; Canales, C.; Lorenzo, M. Policy based virtualised security architecture for SDN/NFV enabled 5G access networks. 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2016, pp. 44–49. doi:10.1109/NFV-SDN.2016.7919474.
167. Mantas, E.; Papadopoulos, D.; Fernández, C.; Ortiz, N.; Compastié, M.; Martínez, A.L.; Pérez, M.G.; Kourtis, A.; Xylouris, G.; Mlakar, I.; Tsarsitalidis, S.; Klonidis, D.; Pedone, I.; Canavese, D.; Pérez, G.M.; Sanvito, D.; Logothetis, V.; Lopez, D.; Pastor, A.; Lioy, A.; Jacquin, L.; Bifulco, R.; Kapodistria, A.; Priovolos, A.; Gardikis, G.; Neokosmidis, I.; Rokkas, T.; Papadakis, N.; Paraschos, D.; Jeran, P.; Litke, A.; Athanasiou,

G. Practical Autonomous Cyberhealth for resilient Micro, Small and Medium-sized Enterprises. 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), 2021, pp. 500–505. doi:10.1109/MeditCom49071.2021.9647609.

168. Schmittner, M.; Asadi, A.; Hollick, M. SEMUD: Secure multi-hop device-to-device communication for 5G public safety networks. 2017 IFIP Networking Conference (IFIP Networking) and Workshops, 2017, pp. 1–9. doi:10.23919/IFIPNetworking.2017.8264846.

169. Meshram, C.; Imoize, A.L.; Elhassouny, A.; Aljaedi, A.; Alharbi, A.R.; Jamal, S.S. IBOOST: A Lightweight Provably Secure Identity-Based Online/Offline Signature Technique Based on FCM for Massive Devices in 5G Wireless Sensor Networks. *IEEE Access* **2021**, *9*, 131336–131347. doi:10.1109/ACCESS.2021.3114287.

170. Shi, D.; Zhang, X.; Vladimirescu, A.; Shi, L.; Huang, Y.; Liu, Y. A Device Identification Method Based on LED Fingerprint for Visible Light Communication System. Proceedings of the 15th International Conference on Availability, Reliability and Security; Association for Computing Machinery: New York, NY, USA, 2020; ARES '20. doi:10.1145/3407023.3409214.

171. Abdulqadder, I.H.; Zhou, S.; Zou, D.; Aziz, I.T.; Akber, S.M.A. Bloc-Sec: Blockchain-Based Lightweight Security Architecture for 5G/B5G Enabled SDN/NFV Cloud of IoT. 2020 IEEE 20th International Conference on Communication Technology (ICCT), 2020, pp. 499–507. doi:10.1109/ICCT50939.2020.9295823.

172. Yao, Y.; Chang, X.; Mišić, J.; Mišić, V.B. Lightweight Batch AKA Scheme for User-Centric Ultra-Dense Networks. *IEEE Transactions on Cognitive Communications and Networking* **2020**, *6*, 597–606. doi:10.1109/TCCN.2020.2982141.

173. Chaikalis, C.; Kosmanos, D.; Samaras, N.S. Utilizing turbo codes for secure 5G V2X. 2020 IEEE Microwave Theory and Techniques in Wireless Communications (MTTW), 2020, Vol. 1, pp. 30–34. doi:10.1109/MTTW51045.2020.9245035.

174. Ali, B.; Gregory, M.A.; Li, S. Uplifting Healthcare Cyber Resilience with a Multi-access Edge Computing Zero-Trust Security Model. 2021 31st International Telecommunication Networks and Applications Conference (ITNAC), 2021, pp. 192–197. doi:10.1109/ITNAC53136.2021.9652141.

175. Angelogianni, A.; Politis, I.; Mohammadi, F.; Xenakis, C. On Identifying Threats and Quantifying Cybersecurity Risks of Mnos Deploying Heterogeneous Rats. *IEEE Access* **2020**, *8*, 224677–224701. doi:10.1109/ACCESS.2020.3045322.

176. Ortiz, J.; Sanchez-Iborra, R.; Bernabe, J.B.; Skarmeta, A.; Benzaid, C.; Taleb, T.; Alemany, P.; Muñoz, R.; Vilalta, R.; Gaber, C.; Wary, J.P.; Ayed, D.; Bisson, P.; Christopoulou, M.; Xilouris, G.; de Oca, E.M.; Gür, G.; Santinelli, G.; Lefebvre, V.; Pastor, A.; Lopez, D. INSPIRE-5Gplus: Intelligent Security and Pervasive Trust for 5G and beyond Networks. Proceedings of the 15th International Conference on Availability, Reliability and Security; Association for Computing Machinery: New York, NY, USA, 2020; ARES '20. doi:10.1145/3407023.3409219.

177. Ricart-Sanchez, R.; Malagon, P.; Alcaraz-Calero, J.M.; Wang, Q. NetFPGA-Based Firewall Solution for 5G Multi-Tenant Architectures. 2019 IEEE International Conference on Edge Computing (EDGE), 2019, pp. 132–136. doi:10.1109/EDGE.2019.00037.

178. Cunha, V.A.; Maroulis, N.; Papagianni, C.; Sacido, J.; Jiménez, M.; Ubaldi, F.; Gharbaoui, M.; Chang, C.Y.; Koursioumpas, N.; Tomakh, K.; Corujo, D.; Barraca, J.P.; Barmpounakis, S.; Kucherenko, D.; Giorgetti, A.; Boddi, A.; Valcarenghi, L.; Kolodiazhnyi, O.; Zabala, A.; Salvat, J.X.; Garcia-Saavedra, A. 5 Growth: Secure and Reliable Network Slicing for Verticals. 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), 2021, pp. 347–352. doi:10.1109/EuCNC/6GSummit51104.2021.9482536.

179. Erel-Özçevik, M.; Tekçe, F. SDN/NFV based Secure SCMA design in SDR. 2021 17th International Conference on Network and Service Management (CNSM), 2021, pp. 319–325. doi:10.23919/CNSM52442.2021.9615517.

180. Pustišek, M.; Turk, J.; Kos, A. Secure Modular Smart Contract Platform for Multi-Tenant 5G Applications. *IEEE Access* **2020**, *8*, 150626–150646. doi:10.1109/ACCESS.2020.3013402.

181. Tang, B.h.; Zhou, Z.x. High-Speed Mobile Communication Network and Wireless Sensor Network Convergence Service Traffic Prediction Model and Security Mechanism Design. Proceedings of the 2020 9th International Conference on Computing and Pattern Recognition; Association for Computing Machinery: New York, NY, USA, 2021; ICCPR 2020, p. 405–412. doi:10.1145/3436369.3436481.

182. Suraci, C.; Pizzi, S.; Molinaro, A.; Iera, A.; Araniti, G. An RSA-based Algorithm for Secure D2D-aided Multicast Delivery of Multimedia Services. 2020 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), 2020, pp. 1–6. doi:10.1109/BMSB49480.2020.9379851.

183. Papadopoulos, S.; Drosou, A.; Kalamaras, I.; Tzovaras, D. Behavioural Network Traffic Analytics for Securing 5G Networks. 2018 IEEE International Conference on Communications Workshops (ICC Workshops), 2018, pp. 1–6. doi:10.1109/ICCW.2018.8403674.
184. Chen, K.; Wang, Y.; Yu, P.; Li, N. Security-Oriented Network Slice Backup Method. 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS), 2021, pp. 330–335. doi:10.23919/APNOMS52696.2021.9562592.
185. Lou, D.; Kuang, R.; He, A. Entropy Transformation and Expansion with Quantum Permutation Pad for 5G Secure Networks. 2021 IEEE 21st International Conference on Communication Technology (ICCT), 2021, pp. 840–845. doi:10.1109/ICCT52962.2021.9657891.
186. Ma, N.; Zhong, X.; Liu, P.; Zhou, S. A SDN/NFV-based Core Network Slicing for Secure Mobile Communication. 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 2020, pp. 1–5. doi:10.1109/VTC2020-Spring48590.2020.9128924.
187. Priovolos, A.; Lioprasitis, D.; Gardikis, G.; Costicoglou, S. Using Anomaly Detection Techniques for Securing 5G Infrastructure and Applications. 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), 2021, pp. 519–524. doi:10.1109/MeditCom49071.2021.9647668.
188. Nediyanchath, A.; Singh, C.; Singh, H.J.; Mangla, H.; Mangla, K.; Sakhala, M.K.; Balasubramanian, S.; Pareek, S.; Shwetha. Anomaly Detection in Mobile Networks. 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2020, pp. 1–5. doi:10.1109/WCNCW48565.2020.9124843.
189. Ketzaki, E.; Drosou, A.; Papadopoulos, S.; Tzovaras, D. A light-weighted ANN architecture for the classification of cyber-threats in modern communication networks. 2019 10th International Conference on Networks of the Future (NoF), 2019, pp. 17–24. doi:10.1109/NoF47743.2019.9015063.
190. Xu, S.; Fang, D.; Sharif, H. Efficient Network Anomaly Detection for Edge Gateway Defense in 5G. 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1–5. doi:10.1109/GCWkshps45667.2019.9024554.
191. Martini, B.; Mori, P.; Marino, F.; Saracino, A.; Lunardelli, A.; Marra, A.L.; Martinelli, F.; Castoldi, P. Pushing Forward Security in Network Slicing by Leveraging Continuous Usage Control. *IEEE Communications Magazine* **2020**, *58*, 65–71. doi:10.1109/MCOM.001.1900712.
192. Gonzalez, A.J.; Ordonez-Lucena, J.; Helvik, B.E.; Nencioni, G.; Xie, M.; Lopez, D.R.; Grønsund, P. The Isolation Concept in the 5G Network Slicing. 2020 European Conference on Networks and Communications (EuCNC), 2020, pp. 12–16. doi:10.1109/EuCNC48522.2020.9200939.
193. Bordel, B.; Orúe, A.B.; Alcarria, R.; Sánchez-De-Rivera, D. An Intra-Slice Security Solution for Emerging 5G Networks Based on Pseudo-Random Number Generators. *IEEE Access* **2018**, *6*, 16149–16164. doi:10.1109/ACCESS.2018.2815567.
194. Wang, M.; Yan, Z. Security in D2D Communications: A Review. 2015 IEEE Trustcom/BigDataSE/ISPA, 2015, Vol. 1, pp. 1199–1204. doi:10.1109/Trustcom.2015.505.
195. Abd-Elrahman, E.; Ibn-khedher, H.; Afifi, H.; Toukabri, T. Fast group discovery and non-repudiation in D2D communications using IBE. 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), 2015, pp. 616–621. doi:10.1109/IWCMC.2015.7289154.
196. Abd-Elrahman, E.; Ibn-khedher, H.; Afifi, H. D2D group communications security. 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015, pp. 1–6. doi:10.1109/NOTERE.2015.7293504.
197. Sedidi, R.; Kumar, A. Key exchange protocols for secure Device-to-Device (D2D) communication in 5G. 2016 Wireless Days (WD), 2016, pp. 1–6. doi:10.1109/WD.2016.7461477.
198. Saxena, N.; Kumbhar, F.H.; Roy, A. Exploiting Social Relationships for Trustworthy D2D Relay in 5G Cellular Networks. *IEEE Communications Magazine* **2020**, *58*, 48–53. doi:10.1109/MCOM.001.1900089.
199. Luntovskyy, A.; Zobjack, T.; Shubyn, B.; Klymash, M. Energy Efficiency and Security for IoT Scenarios via WSN, RFID and NFC : Invited Paper. 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 2021, pp. 1–6. doi:10.1109/UkrMiCo52950.2021.9716591.
200. Vera-Rivera, A.; Refaey, A.; Hossain, E. Task Sharing and Scheduling for Edge Computing Servers Using Hyperledger Fabric Blockchain. 2021 IEEE Globecom Workshops (GC Wkshps), 2021, pp. 1–6. doi:10.1109/GCWkshps52748.2021.9682057.

201. Shukla, A.; Gupta, R.; Tanwar, S.; Kumar, N.; Rodrigues, J.J.P.C. Block-RAS: A P2P Resource Allocation Scheme in 6G Environment with Public Blockchains. GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1–6. doi:10.1109/GLOBECOM42002.2020.9348008.
202. Gabrielson, A.; Bauer, K.; Kelly, D.; Kearns, A.; Smith, W.M. CUE: A Standalone Testbed for 5G Experimentation. MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM), 2021, pp. 745–750. doi:10.1109/MILCOM52596.2021.9653117.
203. Shorov, A. 5G Testbed Development for Network Slicing Evaluation. 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2019, pp. 39–44. doi:10.1109/EIConRus.2019.8656861.
204. Dzogovic, B.; Santos, B.; Do, V.T.; Feng, B.; Jacot, N.; Van Do, T. Connecting Remote eNodeB with Containerized 5G C-RANs in OpenStack Cloud. 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2019, pp. 14–19. doi:10.1109/CSCloud/EdgeCom.2019.00013.
205. Pepito, R.; Dutta, A. Open Source 5G Security Testbed for Edge Computing. 2021 IEEE 4th 5G World Forum (5GWF), 2021, pp. 388–393. doi:10.1109/5GWF52925.2021.00075.
206. Lee, G.; Lee, J.; Kim, Y.; Park, J.G. Network Flow Data Re-collecting Approach Using 5G Testbed for Labeled Dataset. 2021 23rd International Conference on Advanced Communication Technology (ICACT), 2021, pp. 254–258. doi:10.23919/ICACT51234.2021.9370561.
207. Astrakhantsev, A.; Globa, L.; Novogrudska, R.; Skulysh, M.; O.Ye, S. Improving resource allocation system for 5G networks. 2021 International Conference on Information and Digital Technologies (IDT), 2021, pp. 182–188. doi:10.1109/IDT52577.2021.9497634.
208. Hussein, A.; Elhajj, I.H.; Chehab, A.; Kayssi, A. SDN VANETs in 5G: An architecture for resilient security services. 2017 Fourth International Conference on Software Defined Systems (SDS), 2017, pp. 67–74. doi:10.1109/SDS.2017.7939143.
209. Al-Turjman, F.; Alturjman, S. Context-Sensitive Access in Industrial Internet of Things (IIoT) Healthcare Applications. *IEEE Transactions on Industrial Informatics* **2018**, *14*, 2736–2744. doi:10.1109/TII.2018.2808190.
210. Khalid, H.; Hashim, S.J.; Ahmad, S.M.S.; Hashim, F.; Chaudhary, M.A. Robust Multi-Gateway Authentication Scheme for Agriculture Wireless Sensor Network in Society 5.0 Smart Communities. *Agriculture* **2021**, *11*. doi:10.3390/agriculture11101020.
211. Ghassemian, M.; Smith-Creasey, M.; Nekovee, M. Secure Non-Public Health Enterprise Networks. 2020 IEEE International Conference on Communications Workshops (ICC Workshops), 2020, pp. 1–6. doi:10.1109/ICCWorkshops49005.2020.9145350.
212. Li, X.; Hu, X.; Zhang, R.; Zhou, C.; Yin, Q.; Yang, L. A Model-Driven Security Analysis Approach for 5G Communications in Industrial Systems. *IEEE Transactions on Wireless Communications* **2023**, *22*, 889–902. doi:10.1109/TWC.2022.3199378.
213. Kim, J.; Duguma, D.G.; Astillo, P.V.; Park, H.Y.; Kim, B.; You, I.; Sharma, V. A Formally Verified Security Scheme for Inter-gNB-DU Handover in 5G Vehicle-to-Everything. *IEEE Access* **2021**, *9*, 119100–119117. doi:10.1109/ACCESS.2021.3107308.
214. Unal, D.; Hammoudeh, M.; Kiraz, M.S. Policy specification and verification for blockchain and smart contracts in 5G networks. *ICT Express* **2020**, *6*, 43–47. doi:https://doi.org/10.1016/j.icte.2019.07.002.
215. Hou, W.; Sun, Y.; Li, D.; Guan, Z.; Liu, J. Lightweight and Privacy-Preserving Charging Reservation Authentication Protocol for 5G-V2G. *IEEE Transactions on Vehicular Technology* **2023**, *72*, 7871–7883. doi:10.1109/TVT.2023.3241324.
216. Afaq, A.; Haider, N.; Baig, M.Z.; Khan, K.S.; Imran, M.; Razzak, I. Machine learning for 5G security: Architecture, recent advances, and challenges. *Ad Hoc Networks* **2021**, *123*, 102667. doi:https://doi.org/10.1016/j.adhoc.2021.102667.

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