Revista Brasileira de Computação Aplicada, November, 2024

DOI: 10.5335/rbca.v16i3.16005
Vol. 16, Nº 3, pp. 100–115
Homepage: seer.upf.br/index.php/rbca/index

ORIGINAL PAPER

# A systematic literature mapping on the security of 5G and vertical applications

Álvaro Sobrinho [1], Matheus V. P. dos Santos[2], Amanda B. Silva[2], Edmar C. Gurjao[2], Danilo F. S. Santos [2]

[1]Federal University of the Agreste of Pernambuco, Garanhuns, Pernambuco, Brazil, [2]Federal University of Campina Grande, Campina Grande, Paraíba, Brazil

*alvaro.alvares@ufape.edu.br; matheus.vilarim@ee.ufcg.edu.br; amanda.silva@ee.ufcg.edu.br; ecg@dee.ufcg.edu.br; danilo.santos@dee.ufcg.edu.br

**Received:** 2024-06-25. **Revised:** 2024-11-12. **Accepted:** 2024-11-30.

## Abstract

**Background:** The deployment of 5G infrastructure is one of the vectors for new application scenarios since it enables enhanced data bandwidth, low latency, and comprehensive signal coverage. This communication system supports various vertical applications such as smart health, smart cities, smart grids, and transportation systems. However, these applications bring new challenges to 5G networks due to specific requirements for such scenarios. Furthermore, as software-based technologies, including network slicing, software-defined networks, network function virtualization, and multi-access edge computing, are a fundamental part of the 5G architecture, the network can expose these applications to new security and privacy concerns. **Results:** This study summarizes existing literature on 5G vertical applications security. We highlight vulnerabilities, threats, attacks, and solutions for 5G vertical applications. We conducted a systematic literature mapping to discuss security and privacy challenges regarding the 5G vertical applications. We reviewed 389 papers from 2,349 produced by searching with a curated search query and discussed vulnerabilities, threats, attacks, and solutions for 5G vertical applications. **Conclusions:** Smart cities, Industry 4.0, smart transportation, public services, smart grids, and smart health are vertical applications with relevant security concerns. We observed the need for more research since the 5G and vertical applications continuously evolve.

**Keywords**: Vertical Applications; 5G; Security; Privacy

## Resumo

**Background:** A implantação da infraestrutura 5G é um dos vetores para novos cenários de aplicação, pois permite maior largura de banda de dados, baixa latência e cobertura de sinal abrangente. Este sistema de comunicação suporta várias aplicações verticais, como saúde inteligente, cidades inteligentes, redes inteligentes e sistemas de transporte. No entanto, essas aplicações trazem novos desafios para as redes 5G devido a requisitos específicos para esses cenários. Além disso, como tecnologias baseadas em software, incluindo fateamento de rede, redes definidas por software, virtualização de funções de rede e computação de borda de acesso múltiplo, são parte fundamental da arquitetura 5G, a rede pode expor essas aplicações a novas preocupações de segurança e privacidade. **Resultados:** Este estudo resume a literatura existente sobre a segurança das aplicações verticais do 5G. São destacadas vulnerabilidades, ameaças, ataques e soluções para as aplicações verticais do 5G. Foi realizado um mapeamento sistemático da literatura para discutir os desafios de segurança e privacidade em relação às aplicações verticais do 5G. Foram revisados 389 artigos de um total de 2.349, identificados por meio de uma busca, e foram discutidas vulnerabilidades, ameaças, ataques e soluções para as aplicações verticais em 5G. **Conclusões:** Cidades inteligentes, Indústria 4.0, transporte inteligente, serviços públicos, redes inteligentes e saúde inteligente são aplicações verticais com preocupações relevantes de segurança. Foi observada a necessidade de mais pesquisas, uma vez que 5G e as aplicações verticais evoluem continuamente.

**Palavras-Chave**: Aplicações verticais; 5G; Segurança; Privacidade

## 1 Introduction

The fifth-generation (5G) mobile communication systems improvements in signal coverage (Khan et al., 2020) and its pillars, namely enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low-Latency Communications (URLLC), and Massive Machine-Type Communications (mMTC), enable various vertical applications such as smart health, cities, grids, and transportation. However, these applications can potentially open vulnerabilities for 5G networks due to the necessity of interconnection between objects with the Internet, worldwide connection, and weak cyber-protected hardware and software. For instance, the massive communication of Internet of Things (IoT) devices results in vulnerabilities in 5G-enabled verticals. The coexistence of 5G and legacy networks and interaction with other technologies (e.g., WI-FI) can result in relevant threats (Angelogianni et al., 2020).

Security and privacy are critical in communications systems, especially in software-defined systems like the 5G networks. Network Slicing (NS) (Gonzalez et al., 2020), Software Defined Networks (SDN) (Hussein et al., 2017), Network Function Virtualization (NFV) (Siddiqui et al., 2016), and Multi-Access Edge Computing (MEC) (Ksentini and Frangoudis, 2020) are key technologies in 5G. Therefore, considering both the native cyber-security of 5G networks and those of vertical applications, academia, industry, and government agencies need a comprehensive overview of technologies regarding security and privacy in 5G networks and the existing threat in current vertical applications.

Observing the literature, revisions (discussed in Section 2) need more comprehensive discussions focusing on the security and privacy of 5G vertical applications. Instead, they usually discussed challenges regarding specific verticals such as Industrial IoT (IIoT), e.g., the studies of Varga et al. (2020) and Jiang et al. (2021). However, 5G-enabled vertical applications bring new security and privacy challenges that can compromise service consumers and providers. Therefore, in this paper, we complement other previously published knowledge syntheses.

We reviewed the literature regarding the security and privacy of 5G-enabled vertical applications, such as smart cities, Industry 4.0, and smart transportation. The guidelines presented by Kitchenham et al. (2009) supported our Systematic Literature Review (SLM). In addition, we searched for research papers based on widely used databases: IEEE Xplore and ACM Digital Library. The main contributions of this revision include the following: (1) the analysis of general vulnerabilities, threats, attacks, and solutions for security and privacy in 5G networks and (2) the analysis of specific vulnerabilities, threats, attacks, and solutions for security and privacy in 5G vertical applications.

## 2 Related Work

Many 5G reviews focus on specific technologies such as MEC, Blockchain, IoT, NS, industrial verticals, Artificial Intelligence (AI) techniques, privacy, security, free space optical communication, Low Power Wide Area Networks (LPWAN) technologies, and attacks such as Distributed Denial of Service (DDoS) attack detection, NFV, and SDN. Therefore, our review did not find reviews related to a study focusing on the security and privacy of 5G networks and usage by different vertical applications.

For instance, Pham et al. (2020) focused on the MEC technology. The authors presented an overview of MEC technology and potential use cases and applications. Besides, Spinelli and Mancuso (2021) studied MEC as a technology that enables industrial verticals. Thus, standardization has a fundamental role for MEC, considering MEC architecture, MEC and NFV management and orchestration, and 5G-MEC. The authors also present a discussion of flexible provisioning. Ranaweera et al. (2021a) analyzed the security and privacy aspects of the MEC system. The authors discuss the security aspects of MEC, such as confidentiality, integrity, availability, authentication, and authorization. Ranaweera et al. (2021b) also presented 5G use cases deployed based on MEC security vulnerabilities.

Nguyen, Pathirana, Ding and Seneviratne (2020) analyzed the opportunities of using blockchain in 5G services. Wazid et al. (2021) provided details on the network and threat models required for the IoT-enabled communication environment. In addition, they discuss future research challenges related to protocol security, efficient security protocol design, security protocol scalability, recorded data privacy, device heterogeneity, and blockchain-based protocol design.

Varga et al. (2020) identified challenges and solutions related to 5G-enabled IIoT. In addition, the authors highlight 5G support for IIoT applications that use robotics, such as Industry 4.0, physical-cybernetic systems, tactile Internet, and the diverse use of 5G technologies for industrial purposes.

Wijethilaka and Liyanage (2021) presented an analysis of the use of NS in IoT implementation. The technique divides the physical network into multiple logical networks to provide specific capabilities and characteristics for a particular use case. They showed that NS plays a relevant role in IoT implementation, improving scalability, dynamics, security, privacy, quality of service, end-to-end orchestration, and resource prioritization and allocation. Bochie et al. (2021) provided an overview of Deep Learning (DL), explaining the approach's benefits in IoT and sensor, mobile, industrial, and vehicular networks. They propose a workflow based on observations of DL applications and analyze the literature on solutions based on DL at an application-oriented level. However, there needs to be a more in-depth discussion of 5G.

Although we only highlighted the previous studies, readers can also consider other published research (e.g., Tang et al. (2022); Tanveer et al. (2022); Sullivan et al. (2021)). However, the existing reviews usually discuss challenges regarding specific verticals or technologies such as IIoT. Therefore, this article reviews the literature addressing many 5G vertical applications.

## 3 Research Methodology

In this study, we defined the following main research question: *what is the state-of-the-art regarding security in 5G networks and vertical applications?* Based on the main research question, we defined five Secondary Research Question (SRQ): *What are the main threats considering different vertical applications in 5G networks?* (SRQ1); *What are the main challenges and possible solutions for security in 5G networks?* (SRQ2) *What are the main existing/considered security requirements for 5G networks?* (SRQ3) *What is the impact of using legacy networks (e.g., 3G and 4G) along with 5G networks in terms of security?* (SRQ4); and *What threats and solutions exist when using 5G along with other networks (e.g., Wi-Fi)?* (SRQ5).

Besides, we included the following keywords: 5G, 5G core, 5G NR, 5G New Radio, 5G architecture, the fifth generation of mobile networks, security, security model, security scheme, security policy, privacy, network, solution, and threat. Based on the keywords, we searched for studies on IEEE Xplore and ACM Digital Library using the search string: *(((5G OR "5G core" OR "5G New Radio" OR "5G NR" OR "5G architecture" OR "5G scheme" OR "fifth generation of mobile network") AND (security OR "security model" OR "security scheme" OR "security policy" OR privacy) AND (network AND (solution OR threat OR approach))))*.

Table 1 presents the inclusion and exclusion criteria for the study selection process. We did not exclude secondary research papers because some present solutions proposals, such as security frameworks (Ramezan et al., 2018). Besides, secondary research papers can provide information on vulnerabilities, threats, and attacks. The selection procedure started with the document's titles and abstracts and applying inclusion and exclusion criteria (Step 1). When necessary, the researchers also analyzed the conclusions to increase confidence in the selection. During the selection process, two researchers evaluated each study. We defined two selection teams (Team 1 and Team 2), comprising two researchers for each group. Subsequently, two research supervisors reviewed the selection process based on Cohan's Kappa statistics results. We used Cohan's Kappa statistics to enhance the study selection process of our revision (Pérez et al., 2020). We used the strength of agreement using Cohen's Kappa (k) classification to interpret the results (Landis and Koch, 1977).

In the second selection step (Step 2), the researchers carefully analyzed the studies resulting from the first selection to verify if extracting data based on the data extraction form was possible, accepting the studies that allow extraction.

Each researcher answered a form to extract data. One evaluator worked as an extractor, and another as an extract reviewer. We used Google Forms for data collection and recording.

## 4 Overview of Search and Data Extraction

We identified 2,349 articles published in international conferences, journals, and magazines. We managed the identified articles using the EndNote web application during this examination. The preliminary selection process resulted in 734 accepted and 1,615 rejected papers (Fig. 1). The full paper reading from the accepted papers enabled us to conduct the second filtering step, resulting in 389 final papers. Thus, we extracted data from these 389 to answer the research questions and analyzed their quality according to the protocol presented in Section 3.

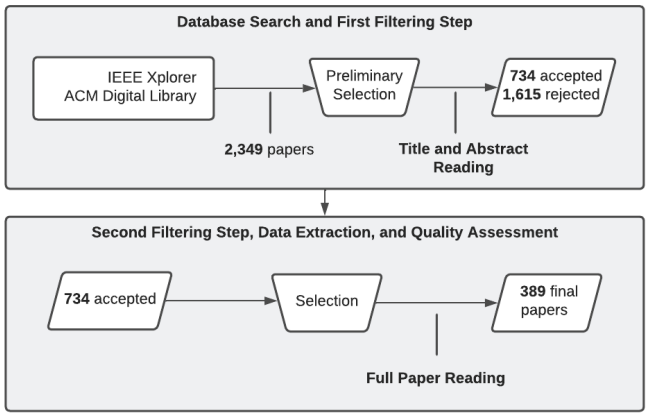


**Figure 1:** Study selection process and data extraction.

To increase confidence in the filtering steps, we applied Cohen's Kappa statistics for each team of researchers. Using the IBM SPSS tool, we performed a descriptive statistical analysis calculating the Cohen's Kappa measure based on a cross-reference table. Assimilation of the inclusion and exclusion criteria implies reducing the Kappa index. Table 2 summarizes the Cohen's Kappa values for Teams 1 and 2.

The Kappa index variation indicates an improvement or a reduction in Team 1's or Team 2's understanding of the inclusion and exclusion criteria, respectively. We also used these results to support the consolidation of the peer-review decisions, providing special attention to the lowest Kappa evaluation results.

## 5 Security and Privacy Concerns

This article focuses on security and privacy concerns regarding 5G and vertical applications (SRQ1 and SRQ2). Thus, this section discusses threats and related vulnerabilities and attacks.

### 5.1 Landscape of General Threats

Discussing general threats is relevant because they affect all vertical applications. We highlight 41 general threats for 5G networks, regardless of vertical applications (Dutta and Hammad, 2020). An adversary can maliciously (1) use legitimate orchestrator access to manipulate the configuration and run a compromised network function, (2) take advantage of malicious insiders attacks, (3) perform unauthorized access (e.g., to confidential data (Isaksson and Norrman, 2020) and to RFID tags (Rahimi et al., 2018)), (4) tampering, (5) perform resource exhaustion, (6) turn services unavailable, (7) analyze or

**Table 1:** Inclusion criteria and exclusion criteria.

| Inclusion Criteria | Exclusion Criteria |
|---|---|
| The full document is available. | Posters. |
| Articles published from 2010 to 2022. | Short papers. |
| Articles published in journals. | Books. |
| Articles published in magazines. | Book chapters. |
| Articles published in conferences. | Duplicated papers. |
| It presents solutions, threats, and architectures. | The study does not focus on security/privacy. |

**Table 2:** Summary of Cohen's Kappa values for Teams 1 and 2.

| Team | Papers | Kappa ($k$) | Agreement Level | Asymptotic Standard Error | T | Significance |
|---|---|---|---|---|---|---|
| Team 1 | 1,174 | 0.601 | Moderate | 0.023 | 20,813 | < 0.001 |
| Team 1 (First 300 Papers) | 300 | 0.393 | Fair | 0.051 | 6,987 | < 0.001 |
| Team 1 (Next 874 Papers) | 874 | 0.671 | Substantial | 0.025 | 19,989 | < 0.001 |
| Team 2 | 1,175 | 0.361 | Fair | 0.033 | 12,668 | < 0.001 |
| Team 2 (First 300 Papers) | 300 | 0.434 | Moderate | 0.062 | 7,667 | < 0.001 |
| Team 2 (Next 875 Papers) | 875 | 0.330 | Fair | 0.040 | 10,015 | < 0.001 |

modify traffic, (8) perform data leakage (e.g., capturing valuable personal information (Bordel et al., 2021)), (9) perform attacks for resource shortages, (10) extract users private information using a shared service in an unauthorized manner, (11) compromise security controls, (12) use north and south boundary interfaces to attack the SDN controller, (13) interference for resource exhaustion, (14) change network elements configuration using the management interface, (15) eavesdrop (e.g., using massive Multiple-Input Multiple-Output (MIMO) (Chen et al., 2016)) messages to legitimize users, (16) compromise isolation, (17) transmit false Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS), (18) attack IoT devices, (19) block, sniffing, and spoofing the Physical Broadcast Channel (PBCH), (20) block the Physical Downlink Control Channel (PDCCH), (21) block uplink or downlink signal, (22) spoof the Physical Random Access Channel (PRACH), (23) unauthorized access to home subscriber server to steal user parameters, (24) use software to compromise encryption algorithms (25) application layer attacks using northbound interfaces, (26) reprogram or attack controller functions, (27) forged or spoofed traffic streams, (28) communication channels attacks, (29) classic IP-based attacks, (30) compromise the advanced encryption standard, (31) use application instance to intercept traffic flows or perform black holes, (31) intercept a key, (32) identify a subscriber's identity, (33) track a subscriber's location (Omone et al., 2021), (34) get the International Mobile Subscriber Identity (IMSI) to register with a Base Station (BS), (35) calculate valid session keys to reproduce the same message, (36) take advantage of a fake identity or fake/unauthorized MEC gateway, (37) attack open edge APIs, (38) disable IoT device power saving abilities, (39) spoof DNS servers and IP addresses to spread viruses, (40) attack the weakest link of heterogeneous networks, and (41) perform Economical Denial of Sustainability (EDoS) (Vidal et al., 2018).

Adversaries can also take advantage of the flexibility of orchestration, internal agents, authentication failure, physical downlink control channel, confidentiality failures in the communication channel, sensor networks vulnerabilities, cloud radio access networks vulnerabilities (Jeyakumar and Rajabhushanam, 2019), C-RAN vulnerabilities (Tian et al., 2017), EAP-TLS vulnerabilities (Zhang et al., 2020), Subscriber Identity Module (SIM) vulnerabilities (Zhao, Ding, Guo, Tan and Lu, 2021), machine learning models vulnerabilities (Suomalainen et al., 2020), software-defined mobile networks vulnerabilities, named data networks vulnerabilities (Bertino and Nabeel, 2018), MEC vulnerabilities, UE vulnerabilities (Amgoune and Mazri, 2018), D2D communication vulnerabilities (Abd-Elrahman et al., 2015), System Information Block (SIB) and RRC message parameters in 5G NR, edge security flaw, key sent over an insecure channel, security flaw in NS (Martini et al., 2020), credential theft, devices without robust security mechanisms, 5G-AKA vulnerabilities (Basin et al., 2018), and security flaws in NFV and SDN (Ahmad et al., 2021). Operating Systems (OS) using insecure protocols provide excessive privileges, IoT devices may have different protocols, lack processing robustness, and fail to control sensitive data privacy. Also, open networks and the PSS/SSS design permit detection at a low signal-to-noise ratio. In addition, the network can be vulnerable when the division of resources for the slices is done by a system common to all the resulting resources. The handover authentication mechanism of 5G networks is also a relevant attack surface (Gupta et al., 2018).

The attackers can use an application on the user's device to change the contents of a token, steal confidential information, and send malicious packets to the 5G core. Other examples of attacks include Man-In-The-Middle (MITM), stolen verifier, replay, pilot contamination (e.g., non-orthogonal multiple access in 5G mm-Wave massive MIMO networks (Wang et al., 2020)) (Osorio et al., 2020), pollution attack (e.g., in cooperative MEC caching (Yang et al., 2018)), stolen smart card (enabling offline password guessing (Shin and Kwon, 2018)), jamming (e.g., pulsed based jamming attack (Schinianakis et al., 2019)), signaling storm (Ahmad et al., 2017), byzantine, sinkhole, IMSI catchers (Chlosta et al., 2021), greyhole, wormhole, back holes, hello flooding, SQL, ack flooding, forgery, side channel, REST API parameters exploration, API flood, protocol fuzzing, physical device capture, malware (e.g., ransomware (Luntovskyy and Shubyn, 2020)), pulsed interference, compression ratio info-

leak made easy, SDN controller personification, PBCH interference, SIB message spoofing, service theft, massive replay, redirection, botnet (Raj et al., 2019), exhaustive search, spectrum scanning, internet control message protocol packages, statistical, SYN flooding, ping of death, backdoor, UDP flooding, slice-initiated, IP spoofing, bug exploitation, TCP reset, differential (e.g., differential fault attack), cyberphysical, selective forwarding, and host resource starvation.

It is also possible to transmit multiple false PSS to the target 5G NR frame (at higher power), impersonate a BS during the RRC handshake, and conduct masquerading attacks (e.g., focusing on the mobility management entity (Moreira et al., 2018)). Besides, identifiers (e.g., MAC addresses) can be cloned or spoofed, data from the IoT deployment to the 5G BS (or 5G BS to the IoT deployment) can be captured, and node memory extracted to fraudulently use the private key (Bordel et al., 2021).

Attackers can exploit the direct communication in high-density device scenarios, lacking a central controller, resulting in actions such as inserting an infected device into the network. Compromised devices enable DDoS attacks (e.g., Distributed Reflection Denial of Service (DRDoS) attacks with User Datagram Protocols (UDPs) (Huang et al., 2019)) and overwhelm the network (Hakiri and Dezfouli, 2021). Attackers can also explore the existence of abandoned and "zombie" cellular IoT devices (Soós and Varga, 2019).

Immersive technologies like Augmented Reality (AR) and Virtual Reality (VR) are also attack surfaces. For instance, the attacker can access and manipulate unauthorized video streams of AR applications. In addition, AR and VR applications can also be subject to tampering, side-channel attacks, malicious code injections, and hardware Trojans (Ranaweera et al., 2021b).

Other relevant attacks for 5G networks are downgrade attacks. For instance, a logjam attack allows an attacker to downgrade vulnerable transport layer security connections to 512-bit export-level encryption (Schinianakis, 2017). A downgrade attack can also force a UE to use a legacy network, vulnerable to many threats addressed by the newest generation (Angelogianni et al., 2020; Ghosh et al., 2019; Sheoran et al., 2019; Peltonen et al., 2021).

## 5.2 Vertical Applications

This section focuses on security and privacy concerns regarding 5G and the vertical applications: smart cities, Industry 4.0, smart transportation, public services, smart grids, smart health, and smart agriculture. However, the existing threats can also affect other vertical applications such as education and retail (Nowak et al., 2021).

### 5.2.1 *Smart Cities*

We can consider a city as smart when it comprises a set of embedded devices (sensors and actuators) controlled by a central point. Smart city applications rely on sensors distributed through different things (e.g., a bus) to improve efficiency and management quality. We highlight 16 smart city threats based on our revision. This application vertical is highly dependent on IoT (e.g., Internet of Drones (IoD) (Abdel-Malek et al., 2021)) and underlying wireless access technologies, such as Software Defined Radio (SDR) and Cognitive Radio (CR), for intelligent information gathering in dynamic heterogeneous environments (Akhunzada et al., 2020). An adversary can maliciously (1) use spectrum bands in an unauthorized manner, (2) saturate the cognitive control channel, (3) compromise IoT devices directly or through a remote connection, (4) affect spectrum detection/sensing, (5) affect spectrum sharing abilities, (6) interrupt the CR mechanism, (7) masquerade a primary user and CR node, (8) use SDR failures in the context of the physical layer to perform improper actions, (9) extract configuration data of SDR in the context of the physical layer, (10) disruption of CR engine, (11) insert malicious programs in systems that run SDR codes, (12) transmit messages between drones by claiming to be a UE network relay, (13) use a malicious drone to sniff out communication between legitimate drones and transmit a repeated or delayed signatures to verify itself to the network leader, (14) disrupt the drones operation to prevent services (e.g., delivery of products), (15) use low-cost SDR tools to generate false signals with false navigation data and trick the GPS of drones to calculate false positions, and (16) insert an unauthorized waveform in SDR configuration.

Therefore, they can explore the network and physical layers, vulnerabilities of the SDR and MAC, OS that enables backdoor accounts and patches with open ports and services, and the fact that SDR devices and components are easily programmable and accessible in an open environment. The attacker can benefit from the hidden node problem; change cognitive messages and CR node; conduct real-time (physical layer-related) OS software alteration/destruction, and other general attacks. The remote access for access and control of smart home devices can also enable attacks in 5G-IoT networks (Shin et al., 2019).

### 5.2.2 *Industry 4.0*

The fourth industrial revolution relies on cyber-physical systems, IoT, and cloud computing to improve efficiency and productivity. We highlight 11 threats for Industry 4.0 based on our revision. This vertical application is highly dependent on IoT (Astrakhantsev et al., 2021; Corici et al., 2020, 2019; Nasir et al., 2019; Dey et al., 2018; Ali and Ware, 2021; Abdel-Basset et al., 2022). Thus, we discuss IIoT and cyber-physical systems as part of Industry 4.0. An adversary can maliciously (1) improperly upgrade and reset industrial equipment, (2) turn industrial equipment unavailable, (3) real-time attacks on cyber-physical industrial systems environment that disrupt/damage physical infrastructure or degrade performance by injecting false data by malicious users, (4) unauthorized update of legacy subsystems in the plant, (5) take advantage of compromised hardware certificates or inactive malicious code to perform attacks, (6) install undesired software on industrial devices, (7) make an undesired device connection to a factory network, (8) perform unauthorized access to factory resources (e.g., network and data storage/retrieval), (9) perform unauthorized access to factory resources while

transferring between security domains that run its core network, (10) compromise the communication frequency or spectrum usage of different nearby transmitter-receiver pairs in the production environment, and (11) perform unauthorized commands on plant actuators.

Adversaries can explore the low security of industrial protocols, real-time operation, use of legacy subsystems, use of insecure channels for communication between smart devices and users, supply chain security breaches, lack of confidentiality protection, lack of access control, allowance of remote access to devices, and lack of control in software installations. For instance, attackers can modify device behaviors and move devices in a factory without permission.

#### *5.2.3 Smart Transportation*

This vertical strongly relates to smart city applications. Smart transportation can include, for example, smart cars and intelligent railway systems. We highlight 20 threats to smart transportation based on our revision. This vertical application relates to concepts such as the Internet of Vehicles and it is highly dependent on vehicular networks (Eltahlawy and Azer, 2021; Hussein et al., 2017; Falchetti et al., 2015; Lai et al., 2020; Saglam and Bahtiyar, 2019; Moulahi et al., 2021; Ayoub and Mazri, 2018; Lu et al., 2020; Aljeri and Boukerche, 2020; Huang et al., 2020; Hasan and Hasan, 2021). An adversary can maliciously (1) transmit meaningless or false information to manipulate other vehicles, (2) perform global positioning system spoofing attacks to deceive innocent vehicles, (3) perform DoS attacks on Internet of Vehicles, (4) impair the availability of vehicular networks services, (5) take advantage of malicious and compromised vehicles to publish false information to cause system damage, (6) forge the identity and claim to be an authentic and valid vehicle using the identifier on the network (node impersonation), (7) use malicious vehicles to add delay time slots to the transmitted message without any changes (neighbor vehicles receive time-sensitive messages when they are no longer needed), (8) monitor and analyze network traffic and steal confidential vehicle information (e.g., vehicle location and identity - the road side unit is an attack surface), (9) behave as a road side unit, (10) interfere with transmission by preventing communication between vehicles in a given transmission and reception range, (11) track vehicles, (12) monitor and capture route and destination address, (13) manipulate route and destination, (14) track (transmit) reported accident videos by eavesdropping on wireless communications (attacking small cells or hacking into the cloud), (15) transmit fake traffic accident videos to mislead authorities, (16) send valid dummy reports, (17) use cars with malware to eavesdrop other cars' identity authentication information and cause traffic disruption/property losses, (18) inject repeatedly messages to authorized control actuators in vehicles, (19) access the engine control unit to compromise safety-critical systems of vehicles, and (20) take advantage of a malicious vehicle that can remain between two unsuspecting vehicles, receive the message from the transmitting ones (e.g., identifier or private security keys), change its contents, and forward the wrong message to the receiver.

For instance, adversaries can explore the vulnerabilities of authentication and encryption algorithms (e.g., incorrect choice of algorithms that use short keys), lack of a mechanism to guarantee confidentiality, and that applications rely on cooperation between neighbors (exchanging location details between vehicles). For instance, the attackers can flood the network with traffic to arbitrary vehicles to deplete resources or disrupt the controller's network view, affecting the forwarding process in the data plane or denying the controller its services.

The vulnerabilities discussed above can also be valid for the vertical applications presented in the following sections. For example, public services, smart grids, smart health, and smart agriculture relate to smart cities and smart transportation. Besides, these verticals usually rely on IoT.

#### *5.2.4 Public Services*

This vertical also strongly relates to smart cities, as a city requires services such as public safety and tactical applications. They relate to concepts such as the IoD. We highlight seven threats for public services based on our revision (Suomalainen et al., 2021; Elmasry and Corwin, 2021). An adversary can maliciously (1) access user equipment or devices in a tactical bubble, (2) leak operational information on the capabilities of public safety actors (e.g., number of operatives or drones in the field, device data, and location), (3) disrupt public safety services, (4) eavesdrop and block (jamming) tactical activities, (5) compromise and take control of drones (e.g., using embedded weapons), (6) use malicious drones to attack MEC nodes and steal tactical information, and (7) report false GPS data to violate no-flying zone regulation and/or cause collision hazards.

#### *5.2.5 Smart Grids*

This vertical also strongly relates to smart cities, as technological electric network advances relate to smart grids. For instance, Smart Energy Meters (SEM) can be placed in community residences to measure the energy consumption for billing purposes. We highlight five threats for smart grids based on our revision (Ranaweera et al., 2021b; Xuesong et al., 2021). An adversary can maliciously (1) eavesdrop on home SEM, (2) modify home SEM, (3) interrupt home SEM, (4) unbalance the power load to provide misleading information to edge entities, and (5) connect to the closest data plane gateway to conduct physical attacks on the power grid. Besides, in the context of SEM, once the attacker intercepts energy consumption data (i.e., eavesdroping on home SEM), He/She can infer people's behavior in a community residency aiming to conduct robbery.

#### *5.2.6 Smart Health*

Smart health is a relevant vertical to improve the patients' diagnosis, monitoring, and treatment. Therefore, applications handle very sensitive and private clinical information. This vertical also strongly relates to smart cities. Smart health applications reuse the smart city infrastructure to deliver healthcare more effectively in citizens' daily lives. We highlight six threats for smart

health based on our revision (Le and Hsu, 2021; Nowak et al., 2021; Fatima et al., 2020). An adversary can maliciously (1) leak sensitive data to cause financial losses to healthcare facilities, (2) leak sensitive data to expose the privacy of patients, (3) disrupt healthcare services (e.g., remote surgeries), (4) compromise the availability of data to compromise the treatment of patients, (5) move of valuable items in a healthcare facility, and (6) tamper with clinical data to compromise the treatment of patients.

#### 5.2.7 *Smart Agriculture*

Advances in farming aim to optimize activities such as plantation process management. We highlight four threats to smart agriculture based on our revision (Nowak et al., 2021). An adversary can maliciously (1) tamper with farm sensors for damages, (2) access agricultural systems (e.g., decision support system and drones), (3) falsify data to disrupt the functioning of agricultural systems (e.g., crop or livestock), and (4) disrupt the availability of positioning/weather data. Drone threats like those of smart cities and public services also impact this vertical.

## 6 Solutions and Recommendations

We identified research focusing on solutions such as lightweight encryption schemes (SRQ2 and SRQ3). An example focused on image encryption based on quantum walks for data transfer using IoT and wireless networking (El-Latif et al., 2020). Many studies also offer solutions to improve authentication/authorization for 5G networks (Ali et al., 2020), and B5G (Al Mousa et al., 2020). Others present solutions for lightweight security (Schmittner et al., 2017), SDN/NFV-based core NS (Ma et al., 2020), and computation of security metrics (Zhao, Oshman, Zhang, Moghaddam, Chander and Pourzandi, 2021).

Specific solutions focus, for instance, on cross-layer authentication for ultra-dense 5G networks (Moreira et al., 2018) and identity and access control for micro-services for 5G NFV platforms (Guija and Siddiqui, 2018). Studies also use SIM for security Beyond 5G (B5G) (Al Mousa et al., 2020), in addition to security solutions for 5G tactile Internet (e.g., adaptive wormhole (Zenger et al., 2016)).

Other proposed solutions address the Physical Layer Security (PLS) for wireless networks (Nasir et al., 2019). Anomaly/threat detection is another focus of many of the proposed solutions (Ali and Ware, 2021). Studies also addressed the applicability of forensic solutions to 5G (Nieto, 2018), privacy (Khan et al., 2019), and some others focus on the security of legacy networks (only mentioning possible future 5G applications) (Sheoran et al., 2019).

Some studies also propose or analyze strategies to prevent eavesdropping (Bhuyan et al., 2021), DoS (Barik et al., 2020), EDoS (Vidal et al., 2018), scanning attacks (Cabaj et al., 2018), IMSI catchers (van den Broek et al., 2015), spoofing attacks (Chopra et al., 2018), resource depletion attacks (e.g., botnet attacks (Gokul and Sankaran, 2021)) jamming (Jagannath et al., 2020), localization attack (Roth et al., 2021), pilot contamination (Wang et al., 2020), pollution attacks (Adat et al., 2019), false data injection (Moudoud et al., 2021), DDoS (Mamolar et al., 2019), and DRDoS (Huang et al., 2019). Some proposed solutions focus on resource management considering service quality, including security (Astrakhantsev et al., 2021).

Other proposed solutions address the secure handover (e.g., for heterogeneous IoT networks (Torroglosa-Garcia et al., 2020)), which enables devices to trustfully join domains (e.g., using authentication frameworks (Corici et al., 2019), and protocols (Sharma et al., 2018)). Some studies are concerned with the proposal of architectures (Han et al., 2017), controlling the access/use of NS (Martini et al., 2020), ensuring isolation of NS (Gonzalez et al., 2020), ensuring intra-slice security (Bordel et al., 2018), and ensuring security in D2D communications (Wang and Yan, 2015).

Some of the identified solutions focus on the security and privacy of 5G in vertical applications such as smart transportation (Hussein et al., 2017), Industry 4.0 (Al-Turjman and Alturjman, 2018), smart cities (Akhunzada et al., 2020), public services (Schmittner et al., 2017), smart grids (Xuesong et al., 2021), and smart health (Ghassemian et al., 2020).

Fig. Fig. 2 presents the focus of the 389 reviewed papers. Most studies (i.e., 323) do not focus on a specific vertical application. Besides, 280 of the reviewed papers proposed a specific solution. Some only discussed or mentioned existing solutions (e.g., review papers). Of the 389 papers, 364 focused on 5G, 16 focused on B5G, and 9 focused on 4G (only stating the possibility of adaptations for 5G).

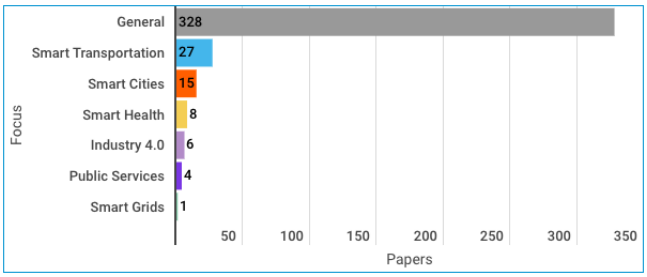


**Figure 2:** Main focus of the 389 reviewed papers.

Other general solutions address the security of SDMN (Liyanage et al., 2015), security policies (Zhao, Zhang, Yu, Zhang, Qiu and Xu, 2021), security schemes (models or protocols) (Ksentini and Frangoudis, 2020), security architectures (or frameworks) (Vijay and Umadevi, 2019), security platforms (or systems) (Ortiz et al., 2020), algorithms (or methods) (Tang and Zhou, 2021), AI-based security (Thantharate et al., 2020), blockchain-based security (Feng et al., 2021), and testbeds (Gabrielson et al., 2021). We also observed studies addressing solutions to MEC security (Ali et al., 2020) and others focusing on privacy (Liyanage et al., 2018).

5G network security can also rely on biologically inspired intelligent algorithms such as colonies honeybees, ant colony optimization, physarum autonomic optimization, artificial immune system, swarm intelligence algorithm, and neural networks (Saleem et al., 2020).

Other general recommendations include hiding the

user identities during service authentication, assuring robust access point/BS identity (Bouras et al., 2017), detecting malicious signaling (Soldani, 2019), securing virtual infrastructure and NS (Panwar and Sharma, 2020), securing authentication chip (Xingzhong et al., 2019), preserving privacy (Nguyen, Tran, Loven, Partala, Kechadi and Pirttikangas, 2020), providing intrusion detection system (Shah and Pramod Bendale, 2019), providing PLS (Singh et al., 2018), and providing service-oriented authentication protocols (Ni et al., 2018). Fig. 3 relates the papers and purpose (e.g., mitigate DDoS attacks). For instance, if an article addressed eavesdropping and jamming (as the solution of Nieto et al. (Nieto et al., 2017)), it appears in both threat categories. The following threats are addressed in one paper: EDoS, zombie devices, impersonation, hijacking, redirection, fingerprinting, sniffing, scanning, botnets, device capabilities, forgery, proximity-based attacks, malware, pilot contamination, resource depletion, adaptive wormholes, quantum, and MITM. Fig. 4 details the focus of the 306 papers addressing other topics, including position papers, experiments, syntheses of knowledge, threat models, and general security solutions.

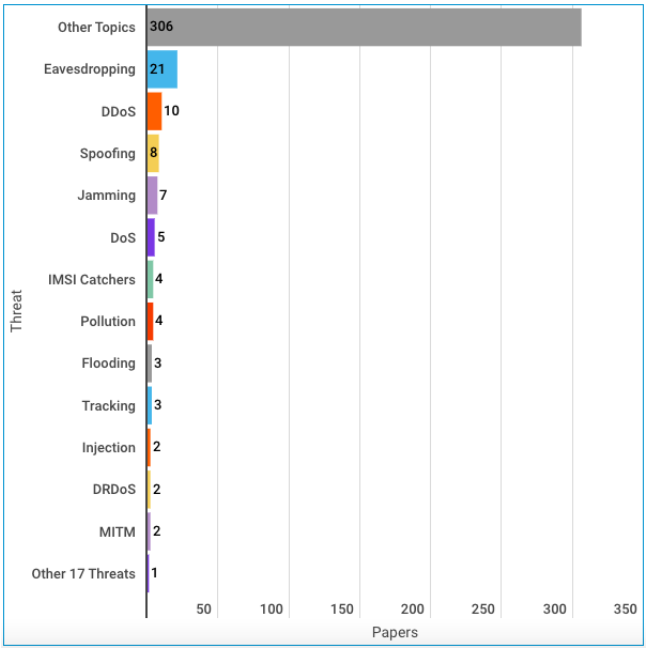


**Figure 3:** Reviewed papers and purposes.

Fig. 5 presents a bubble chart that illustrates the studies by omitting papers that do not present novel proposed solutions, resulting in 280 studies. Thus, the size of the bubble relates to the number of solutions. We grouped the solutions considering management, detection, and mitigation categories. For instance, we omitted some surveys, systematic literature reviews (or mappings), threat models, attack proposals, and experimentation of existing solutions. The proposed solutions included 38 frameworks, 98 approaches (also called mechanisms or systems), 44 schemes, 20 protocols, 32 models (or algorithms), 4 testbeds, 18 methodologies (or methods), 22 architectures, 1 metric, and 1 security protection policy. Security metrics and protection policies relate to the management category.

Most proposed solutions did not focus on specific threats (i.e., 165 for mitigation, 27 for detection, and 11 for management). Of the solutions addressing specific threats, 21 concentrate on mitigating eavesdropping, followed by DDoS (5 mitigation and 4 detection solutions), spoofing (7 detection solutions), jamming (2 mitigation and 2 detection solutions), tracking (3 mitigation solutions), DoS (4 mitigations and 1 detection solutions), IMSI Catchers (3 mitigation solutions), DRDoS (2 mitigation solutions), flooding (2 detection solutions), and pollution (3 mitigation solutions). The remaining threats are related to only one solution.

## 7 Discussion and Future Research Directions

We extracted data from 389 studies after the SLM selection process. Only two papers presented proposals for security metrics and security protection policies. Besides, few papers presented proposals for solutions to address specific threats such as pilot contamination and injection attacks. For instance, our revision did not identify mitigation solutions for pilot contamination and injection attacks. The reviewed papers also need to include specific solutions for smart agriculture. Although we identified solutions focusing on other vertical applications, the number was low (e.g., one solution for smart grids (Xuesong et al., 2021)).

Analyzing the distribution of papers by publication venues is also relevant to presenting journals, magazines, and conferences with the highest number of publications in the field. The journal IEEE Access published the highest number of papers (i.e., 45), followed by IEEE Network. In addition to recent special issues on the topic of 5G, the rapid review/publication process of IEEE Access may explain the number of publications. The remaining journals/magazines published less than ten papers. Thus, the review included 139 papers published in journals or magazines (i.e., 35,73%).

The review included 203 papers published in IEEE conferences (i.e., 52,19%). Additionally, the review included 47 papers published in ACM conferences (i.e., 12,08%). For IEEE conferences, the IEEE 5G World Forum published the highest number of papers (i.e., 10), followed by the IEEE Global Communications Conference (i.e., 8) and IEEE Globecom Workshops (i.e., 8). However, the number of publications is not expressive when considering the total of reviewed IEEE conference papers. The distribution of papers by the remaining IEEE conferences is similar. For ACM conferences, the International Conference on Availability, Reliability, and Security published the highest number of papers (i.e., 13), followed by the ACM Conference on Security and Privacy in Wireless and Mobile Networks (i.e., 9). The remaining ACM conferences published less than four papers. The focus of such conferences on security and privacy may explain this distribution of papers by ACM publication venues.

Researchers from 64 countries authored the papers.

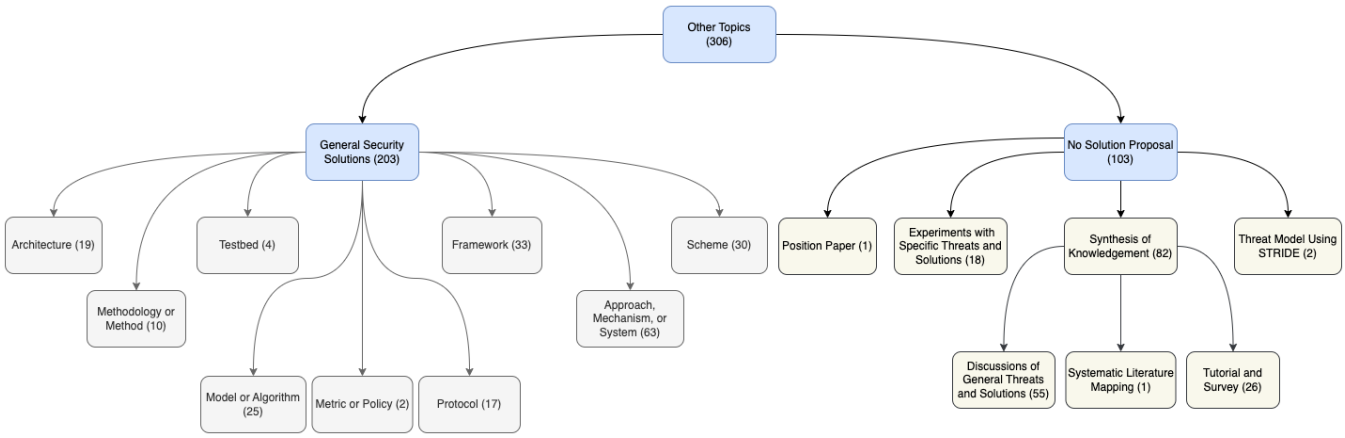


**Figure 4:** Focus of the 306 papers addressing other topics (first bar of Figure Fig. 3).

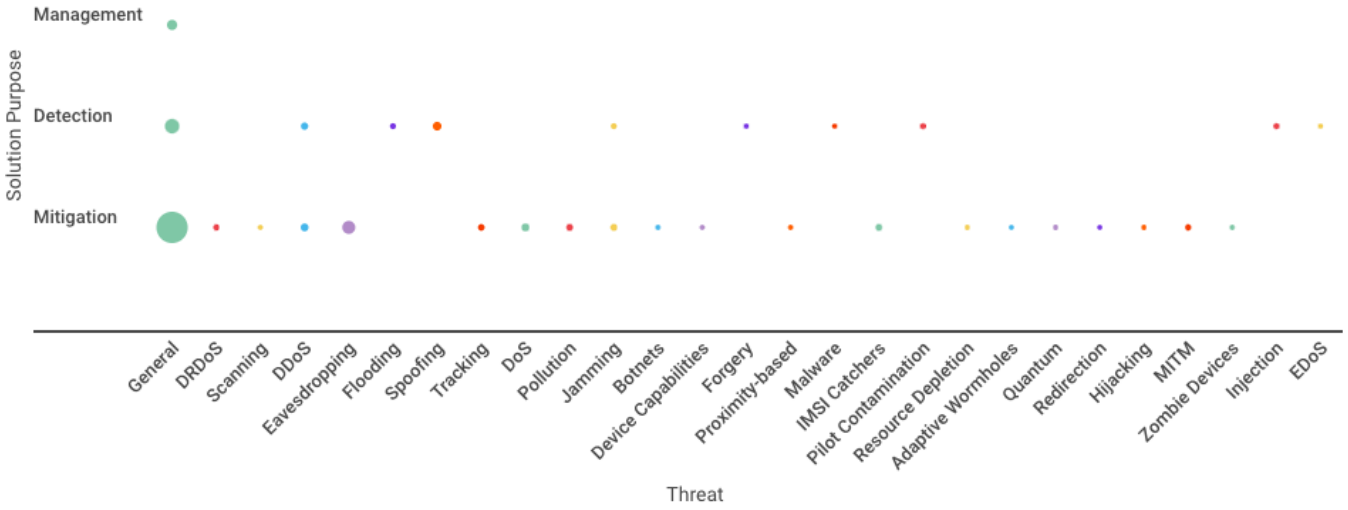


**Figure 5:** Bubble chart presenting the 280 identified solutions and purposes.

The countries with the highest number of authors of papers were China (85 papers), the USA (72 papers), the United Kingdom (46 papers), Germany (34 papers), Canada (32 papers), Finland (31 papers), India (31 papers), and Spain (24 papers). Authors from Latin American countries published a few papers: Brazil (7 papers), Ecuador (2 papers), and Chile (1 paper). Analyzing the distribution of publications on 5G security and privacy per country is relevant to identifying potentially less concerned regions in researching such a topic. The frequency of research publication is only one of many possible indicators of concern. During our SLM, we noticed that less concerned countries could be more vulnerable (e.g., allowing devices with fewer security protections) to security and privacy threats. It is usual for governments around the current widely connected world to keep track of potential foreign security threats using indicators of concern.

However, our SLM only partially shows the full picture because we cannot cover all existing publication venues, only indicating potentially less concerned regions. We cover two relevant paper publication databases: IEEE Xplore and ACM Digital Library. Future research can complement our SLM using other publication databases like Springer, Elsevier, and Wiley online libraries.

Based on our revision, the downgrade attacks are other relevant threats to empathize (SRQ4). For instance, if an adversary forces the downgrade from 5G to previous networks, the user becomes vulnerable to unsolved threats. Threats include, but are not limited to eavesdropping and gathering (i.e., eavesdrop on the communication and collect information about the user's equipment, equipment capabilities, or signature); redirection, discard and creation (i.e., redirect, drop, or create authentication calls/messages/vectors); redirection, discard, and Injection (i.e., redirect, drop or inject calls or messages); traffic flow interception and redirection (i.e., compromising confidentiality); location recovery (i.e., retrieve the subscriber's location); inference mapping (i.e., perform the mapping between information); disabling or separation of UE (disable or separate it from the network); eavesdropping with access or listening (i.e., eavesdrop on the communication and later access a message or listen to a call); eavesdropping with key access (i.e.,

eavesdrop on the communication and access the keys or "break" the encryption scheme); DoS and quality of service degradation (i.e., impersonating a legitimate user); and representation of UE or BS (i.e., impersonate, collect transmission information from neighboring cells, and personify authentic network elements).

It is also relevant to discuss and be aware of possible threats (e.g., quantum attacks (Cho and Sergeev, 2021)) for B5G (El-Latif et al., 2020). For instance, adversaries can maliciously take advantage of the high capabilities of quantum computing, which can be misused and, consequently, improperly access private data, for example, using insecure data transfer on IoT platforms.

In addition, they can exploit the fact that the current information security mechanisms do not consider the high computational capabilities of quantum devices. Therefore, attackers can conduct attacks from quantum devices. Furthermore, due to key size limitations, restricted by traditional physical SIM storage, the network becomes vulnerable to unauthorized access, replay attacks, spoofing attacks, and MITM attacks (Al Mousa et al., 2020). However, we need to identify publications with deep discussions on threats and solutions when 5G networks are used with other networks (e.g., Wi-Fi). This work can be a relevant future research direction (SRQ5).

## 8 Conclusions

We performed an SLM considering cyber-security aspects of vertical applications enabled for 5G networks. As a result, we identified relevant vulnerabilities, threats, attacks, solutions, and recommendations for the security and privacy of 5G vertical applications. Results show the variety of vulnerabilities for each vertical application and the existence of proposed solutions. Our results can support academia, industry, and governments in prioritizing and addressing security and privacy concerns. However, from the SLM findings, the literature requires more investigations to evaluate the threats and practical viability of many solutions identified for 5G and vertical applications.

## Acknowledgments

The authors thank ANATEL for supporting this research. We also acknowledge the support provided by the Virtus Research, Development, and Innovation Center, including the VIRTUS-CC (EMBRAPII VIRTUS Competence Center - Intelligent Hardware for Industry), at the Federal University of Campina Grande. EMBRAPII (Brazilian Company for Industrial Research and Innovation) has made this initiative possible through funding from the Brazilian Ministry of Science and Technology (MCTI) under the PPI HardwareBR program.

## References

Abd-Elrahman, E., Ibn-khedher, H. and Afifi, H. (2015). D2d group communications security, *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, pp. 1–6. http://dx.doi.org/10.1109/NOTERE.2015.7293504.

Abdel-Basset, M., Hawash, H. and Sallam, K. (2022). Federated threat-hunting approach for microservice-based industrial cyber-physical system, *IEEE Transactions on Industrial Informatics* **18**(3): 1905–1917. http://dx.doi.org/10.1109/TII.2021.3091150.

Abdel-Malek, M. A., Akkaya, K., Bhuyan, A. and Ibrahim, A. S. (2021). A proxy signature-based drone authentication in 5g d2d networks, *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, pp. 1–7. http://dx.doi.org/10.1109/VTC2021-Spring51267.2021.9448962.

Adat, V., Politis, I., Tselios, C. and Kotsopoulos, S. (2019). 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)*, pp. 1–6. http://dx.doi.org/10.1109/CAMAD.2019.8858457.

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M. and Gurtov, A. (2017). 5g security: Analysis of threats and solutions, *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 193–199. http://dx.doi.org/10.1109/CSCN.2017.8088621.

Ahmad, I., Pinola, J., Harjula, I., Suomalainen, J., Harjula, E., Huusko, J. and Kumar, T. (2021). An overview of the security landscape of virtual mobile networks, *IEEE Access* **9**: 169014–169030. http://dx.doi.org/10.1109/ACCESS.2021.3133319.

Akhunzada, A., Islam, S. u. and Zeadally, S. (2020). Securing cyberspace of future smart cities with 5g technologies, *IEEE Network* **34**(4): 336–342. http://dx.doi.org/10.1109/MNET.001.1900559.

Al Mousa, A., Al Qomri, M., Al Hajri, S. and Zagrouba, R. (2020). Utilizing the esim for public key cryptography: a network security solution for 6g, *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, pp. 1–6. http://dx.doi.org/10.1109/ICCIS49240.2020.9257601.

Al-Turjman, F. and Alturjman, S. (2018). Context-sensitive access in industrial internet of things (iiot) healthcare applications, *IEEE Transactions on Industrial Informatics* **14**(6): 2736–2744. http://dx.doi.org/10.1109/TII.2018.2808190.

Ali, A., Lin, Y.-D., Li, C.-Y. and Lai, Y.-C. (2020). Transparent 3rd-party authentication with application mobility for 5g mobile edge computing, *2020 European Conference on Networks and Communications (EuCNC)*, pp. 219–224. http://dx.doi.org/10.1109/EuCNC48522.2020.9200937.

Ali, A. and Ware, A. (2021). Anomaly based ids via customised cusum algorithm for industrial communication systems, *2021 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, pp. 31–36. http://dx.doi.org/10.1109/MENACOMM50742.2021.9678305.

Aljeri, N. and Boukerche, A. (2020). Mobility management in 5g-enabled vehicular networks: Models, protocols, and classification, *ACM Comput. Surv.* **53**(5). http://dx.doi.org/10.1145/3403953.

Amgoune, H. and Mazri, T. (2018). 5g: Interconnection of services and security approaches, *Proceedings of the 3rd International Conference on Smart City Applications*, SCA '18, Association for Computing Machinery, New York, NY, USA. http://dx.doi.org/10.1145/3286606.3286795.

Angelogianni, A., Politis, I., Mohammadi, F. and Xenakis, C. (2020). On identifying threats and quantifying cybersecurity risks of mnos deploying heterogeneous rats, *IEEE Access* **8**: 224677–224701. http://dx.doi.org/10.1109/ACCESS.2020.3045322.

Astrakhantsev, A., Globa, L., Novogrudska, R., Skulysh, M. and O.Ye, S. (2021). Improving resource allocation system for 5g networks, *2021 International Conference on Information and Digital Technologies (IDT)*, pp. 182–188. http://dx.doi.org/10.1109/IDT52577.2021.9497634.

Ayoub, T. and Mazri, T. (2018). Security challenges in v2i architectures and proposed solutions, *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, pp. 594–599. http://dx.doi.org/10.1109/CIST.2018.8596599.

Barik, D., Sanyal, J. and Samanta, T. (2020). 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)*, pp. 239–244. http://dx.doi.org/10.1109/5GWF49715.2020.9221441.

Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R. and Stettler, V. (2018). A formal analysis of 5g authentication, *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, Association for Computing Machinery, New York, NY, USA, p. 1383–1396. http://dx.doi.org/10.1145/3243734.3243846.

Bertino, E. and Nabeel, M. (2018). Securing named data networks: Challenges and the way forward, *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, SACMAT '18, Association for Computing Machinery, New York, NY, USA, p. 51–59. http://dx.doi.org/10.1145/3205977.3205996.

Bhuyan, A., Guvenç, I., Dai, H., Sichitiu, M. L., Singh, S., Rahmati, A. and Maeng, S. J. (2021). Secure 5g network for a nationwide drone corridor, *2021 IEEE Aerospace Conference (50100)*, pp. 1–10. http://dx.doi.org/10.1109/AERO50100.2021.9438162.

Bochie, K., Gilbert, M. S., Gantert, L., Barbosa, M. S., Medeiros, D. S. and Campista, M. E. M. (2021). A survey on deep learning for challenged networks: Applications and trends, *Journal of Network and Computer Applications* **194**: 103213. http://dx.doi.org/https://doi.org/10.1016/j.jnca.2021.103213.

Bordel, B., Alcarria, R., Robles, T. and Iglesias, M. S. (2021). Data authentication and anonymization in iot scenarios and future 5g networks using chaotic digital watermarking, *IEEE Access* **9**: 22378–22398. http://dx.doi.org/10.1109/ACCESS.2021.3055771.

Bordel, B., Orúe, A. B., Alcarria, R. and Sánchez-De-Rivera, D. (2018). An intra-slice security solution for emerging 5g networks based on pseudo-random number generators, *IEEE Access* **6**: 16149–16164. http://dx.doi.org/10.1109/ACCESS.2018.2815567.

Bouras, C., Kollia, A. and Papazois, A. (2017). Teaching network security in mobile 5g using onos sdn controller, *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 465–470. http://dx.doi.org/10.1109/ICUFN.2017.7993828.

Cabaj, K., Gregorczyk, M., Mazurczyk, W., Nowakowski, P. and Żórawski, P. (2018). 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*, ARES 2018, Association for Computing Machinery, New York, NY, USA. http://dx.doi.org/10.1145/3230833.3233248.

Chen, B., Zhu, C., Li, W., Wei, J., Leung, V. C. M. and Yang, L. T. (2016). Original symbol phase rotated secure transmission against powerful massive mimo eavesdropper, *IEEE Access* **4**: 3016–3025. http://dx.doi.org/10.1109/ACCESS.2016.2580673.

Chlosta, M., Rupprecht, D., Pöpper, C. and Holz, T. (2021). 5g suci-catchers: Still catching them all?, *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '21, Association for Computing Machinery, New York, NY, USA, p. 359–364. http://dx.doi.org/10.1145/3448300.3467826.

Cho, J. Y. and Sergeev, A. (2021). Secure open fronthaul interface for 5g networks, *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ARES 21, Association for Computing Machinery, New York, NY, USA. http://dx.doi.org/10.1145/3465481.3470080.

Chopra, G., Jha, R. K. and Jain, S. (2018). Tpa: Prediction of spoofing attack using thermal pattern analysis in ultra dense network for high speed handover scenario, *IEEE Access* **6**: 66268–66284. http://dx.doi.org/10.1109/ACCESS.2018.2875921.

Corici, A. A., Corici, M., Troudt, E., Riemer, B. and Magedanz, T. (2020). Framework for trustful handover of m2m devices between security domains, *2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pp. 102–109. http://dx.doi.org/10.1109/ICIN48450.2020.9059457.

Corici, A. A., Shashi, Y., Corici, M., Shrestha, R. and Guzman, D. (2019). Enabling dynamic iot security domains: Cellular core network and device management meet authentication framework, *2019 Global IoT Summit (GIoTS)*, pp. 1–6. http://dx.doi.org/10.1109/GIOTS.2019.8766390.

Dey, A., Nandi, S. and Sarkar, M. (2018). Security measures in iot based 5g networks, *2018 3rd International Conference on Inventive Computation Technologies (ICICT)*, pp. 561–566. http://dx.doi.org/10.1109/ICICT43934.2018.9034365.

Dutta, A. and Hammad, E. (2020). 5g security challenges and opportunities: A system approach, *2020 IEEE 3rd 5G World Forum (5GWF)*, pp. 109–114. http://dx.doi.org/10.1109/5GWF49715.2020.9221122.

El-Latif, A. A. A., Abd-El-Atty, B., Venegas-Andraca, S. E., Elwahsh, H., Piran, M. J., Bashir, A. K., Song, O.-Y. and Mazurczyk, W. (2020). Providing end-to-end security using quantum walks in iot networks, *IEEE Access* **8**: 92687–92696. http://dx.doi.org/10.1109/ACCESS.2020.2992820.

Elmasry, G. and Corwin, P. (2021). Hiding the rf signal signature in tactical 5g, *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*, pp. 733–738. http://dx.doi.org/10.1109/MILCOM52596.2021.9652968.

Eltahlawy, A. M. and Azer, M. A. (2021). Using blockchain technology for the internet of vehicles, *2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, pp. 54–61. http://dx.doi.org/10.1109/MIUCC52538.2021.9447622.

Falchetti, A., Azurdia-Meza, C. and Cespedes, S. (2015). Vehicular cloud computing in the dawn of 5g, *2015 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, pp. 301–305. http://dx.doi.org/10.1109/Chilecon.2015.7400392.

Fatima, R., Manal, R. and Tomader, M. (2020). Cryptography in e-health using 5g based iot: A comparison study, *Proceedings of the 4th International Conference on Big Data and Internet of Things*, BDIoT'19, Association for Computing Machinery, New York, NY, USA. http://dx.doi.org/10.1145/3372938.3372955.

Feng, C., Yu, K., Bashir, A. K., Al-Otaibi, Y. D., Lu, Y., Chen, S. and Zhang, D. (2021). Efficient and secure data sharing for 5g flying drones: A blockchain-enabled approach, *IEEE Network* **35**(1): 130–137. http://dx.doi.org/10.1109/MNET.011.2000223.

Gabrielson, A., Bauer, K., Kelly, D., Kearns, A. and Smith, W. M. (2021). Cue: A standalone testbed for 5g experimentation, *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*, pp. 745–750. http://dx.doi.org/10.1109/MILCOM52596.2021.9653117.

Ghassemian, M., Smith-Creasey, M. and Nekovee, M. (2020). Secure non-public health enterprise networks, *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6. http://dx.doi.org/10.1109/ICCWorkshops49005.2020.9145350.

Ghosh, A., Maeder, A., Baker, M. and Chandramouli, D. (2019). 5g evolution: A view on 5g cellular technology beyond 3gpp release 15, *IEEE Access* **7**: 127639–127651. http://dx.doi.org/10.1109/ACCESS.2019.2939938.

Gokul, N. and Sankaran, S. (2021). Modeling and defending against resource depletion attacks in 5g networks, *2021 IEEE 18th India Council International Conference (INDICON)*, pp. 1–7. http://dx.doi.org/10.1109/INDICON52576.2021.9691522.

Gonzalez, A. J., Ordonez-Lucena, J., Helvik, B. E., Nencioni, G., Xie, M., Lopez, D. R. and Grønsund, P. (2020). The isolation concept in the 5g network slicing, *2020 European Conference on Networks and Communications (EuCNC)*, pp. 12–16. http://dx.doi.org/10.1109/EuCNC48522.2020.9200939.

Guija, D. and Siddiqui, M. S. (2018). Identity and access control for micro-services based 5g nfv platforms, *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, Association for Computing Machinery, New York, NY, USA. http://dx.doi.org/10.1145/3230833.3233255.

Gupta, S., Parne, B. L. and Chaudhari, N. S. (2018). Security vulnerabilities in handover authentication mechanism of 5g network, *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pp. 369–374. http://dx.doi.org/10.1109/ICSCCC.2018.8703355.

Hakiri, A. and Dezfouli, B. (2021). 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*, SDN-NFV Sec'21, Association for Computing Machinery, New York, NY, USA, p. 11–18. http://dx.doi.org/10.1145/3445968.3452090.

Han, B., Wong, S., Mannweiler, C., Dohler, M. and Schotten, H. D. (2017). Security trust zone in 5g networks, *2017 24th International Conference on Telecommunications (ICT)*, pp. 1–5. http://dx.doi.org/10.1109/ICT.2017.7998270.

Hasan, R. and Hasan, R. (2021). Towards a threat model and privacy analysis for v2p in 5g networks, *2021 IEEE 4th 5G World Forum (5GWF)*, pp. 383–387. http://dx.doi.org/10.1109/5GWF52925.2021.00074.

Huang, H., Hu, L., Chu, J. and Cheng, X. (2019). An authentication scheme to defend against udp drdos attacks in 5g networks, *IEEE Access* **7**: 175970–175979. http://dx.doi.org/10.1109/ACCESS.2019.2957565.

Huang, J., Qian, Y. and Hu, R. Q. (2020). Secure and efficient privacy-preserving authentication scheme for 5g software defined vehicular networks, *IEEE Transactions on Vehicular Technology* **69**(8): 8542–8554. http://dx.doi.org/10.1109/TVT.2020.2996574.

Hussein, A., Elhajj, I. H., Chehab, A. and Kayssi, A. (2017). Sdn vanets in 5g: An architecture for resilient security services, *2017 Fourth International Conference on Software Defined Systems (SDS)*, pp. 67–74. http://dx.doi.org/10.1109/SDS.2017.7939143.

Isaksson, M. and Norrman, K. (2020). Secure federated learning in 5g mobile networks, *GLOBECOM 2020 - 2020*

*IEEE Global Communications Conference*, pp. 1–6. http://dx.doi.org/10.1109/GLOBECOM42002.2020.9322479.

Jagannath, A., Jagannath, J. and Drozd, A. (2020). High rate-reliability beamformer design for 2×2 mimo-ofdm system under hostile jamming, *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–9. http://dx.doi.org/10.1109/ICCCN49398.2020.9209635.

Jeyakumar, D. and Rajabhushanam, C. (2019). Security challenges and solutions for cloud radio access networks, *2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 961–965. http://dx.doi.org/10.1109/ICSSIT46314.2019.8987806.

Jiang, B., Li, J., Yue, G. and Song, H. (2021). Differential privacy for industrial internet of things: Opportunities, applications, and challenges, *IEEE Internet of Things Journal* **8**(13): 10430–10451. http://dx.doi.org/10.1109/JIOT.2021.3057419.

Khan, M., Ginzboorg, P. and Niemi, V. (2019). Privacy preserving akma in 5g, *Proceedings of the 5th ACM Workshop on Security Standardisation Research Workshop*, SSR'19, Association for Computing Machinery, New York, NY, USA, p. 45–56. http://dx.doi.org/10.1145/3338500.3360337.

Khan, R., Kumar, P., Jayakody, D. N. K. and Liyanage, M. (2020). A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions, *IEEE Communications Surveys & Tutorials* **22**(1): 196–248. http://dx.doi.org/10.1109/COMST.2019.2933899.

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J. and Linkman, S. (2009). Systematic literature reviews in software engineering – a systematic literature review, *Information and Software Technology* **51**(1): 7–15. http://dx.doi.org/https://doi.org/10.1016/j.infsof.2008.09.009.

Ksentini, A. and Frangoudis, P. A. (2020). Toward slicing-enabled multi-access edge computing in 5g, *IEEE Network* **34**(2): 99–105. http://dx.doi.org/10.1109/MNET.001.1900261.

Lai, C., Lu, R., Zheng, D. and Shen, X. (2020). Security and privacy challenges in 5g-enabled vehicular networks, *IEEE Network* **34**(2): 37–45. http://dx.doi.org/10.1109/MNET.001.1900220.

Landis, J. R. and Koch, G. G. (1977). A coefficient of agreement for nominal scales, *Biometrics* **33**(1): 159–174. https://doi.org/10.1177/001316446002000104.

Le, T.-V. and Hsu, C.-L. (2021). An anonymous key distribution scheme for group healthcare services in 5g-enabled multi-server environments, *IEEE Access* **9**: 53408–53422. http://dx.doi.org/10.1109/ACCESS.2021.3070641.

Liyanage, M., Ahmed, I., Ylianttila, M., Santos, J. L., Kantola, R., Perez, O. L., Itzazelaia, M. U., Montes De Oca, E., Valtierra, A. and Jimenez, C. (2015). Security for future software defined mobile networks, *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, pp. 256–264. http://dx.doi.org/10.1109/NGMAST.2015.43.

Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S. and Ylianttila, M. (2018). 5g privacy: Scenarios and solutions, *2018 IEEE 5G World Forum (5GWF)*, pp. 197–203. http://dx.doi.org/10.1109/5GWF.2018.8516981.

Lu, R., Zhang, L., Ni, J. and Fang, Y. (2020). 5g vehicle-to-everything services: Gearing up for security and privacy, *Proceedings of the IEEE* **108**(2): 373–389. http://dx.doi.org/10.1109/JPROC.2019.2948302.

Luntovskyy, A. and Shubyn, B. (2020). Advanced architectures for iot scenarios, *2020 5th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6. http://dx.doi.org/10.23919/SpliTech49282.2020.9243784.

Ma, N., Zhong, X., Liu, P. and Zhou, S. (2020). A sdn/nfv-based core network slicing for secure mobile communication, *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–5. http://dx.doi.org/10.1109/VTC2020-Spring48590.2020.9128924.

Mamolar, A. S., Pervez, Z., Wang, Q. and Alcaraz-Calero, J. M. (2019). Towards the detection of mobile ddos attacks in 5g multi-tenant networks, *2019 European Conference on Networks and Communications (EuCNC)*, pp. 273–277. http://dx.doi.org/10.1109/EuCNC.2019.8801975.

Martini, B., Mori, P., Marino, F., Saracino, A., Lunardelli, A., Marra, A. L., Martinelli, F. and Castoldi, P. (2020). Pushing forward security in network slicing by leveraging continuous usage control, *IEEE Communications Magazine* **58**(7): 65–71. http://dx.doi.org/10.1109/MCOM.001.1900712.

Moreira, C. M., Kaddoum, G. and Bou-Harb, E. (2018). Cross-layer authentication protocol design for ultra-dense 5g hetnets, *2018 IEEE International Conference on Communications (ICC)*, pp. 1–7. http://dx.doi.org/10.1109/ICC.2018.8422404.

Moudoud, H., Khoukhi, L. and Cherkaoui, S. (2021). Prediction and detection of fdia and ddos attacks in 5g enabled iot, *IEEE Network* **35**(2): 194–201. http://dx.doi.org/10.1109/MNET.011.2000449.

Moulahi, T., Zidi, S., Alabdulatif, A. and Atiquzzaman, M. (2021). Comparative performance evaluation of intrusion detection based on machine learning in in-vehicle controller area network bus, *IEEE Access* **9**: 99595–99605. http://dx.doi.org/10.1109/ACCESS.2021.3095962.

Nasir, A. A., Tuan, H. D., Nguyen, H. H. and Nguyen, N. M. (2019). Physical layer security by exploiting interference and heterogeneous signaling, *IEEE Wireless Communications* **26**(5): 26–31. http://dx.doi.org/10.1109/MWC.001.1900048.

Nguyen, D. C., Pathirana, P. N., Ding, M. and Seneviratne, A. (2020). Blockchain for 5g and beyond networks: A state of the art survey, *Journal of Network and Computer Applications* **166**: 102693. http://dx.doi.org/https://doi.org/10.1016/j.jnca.2020.102693.

Nguyen, T., Tran, N., Loven, L., Partala, J., Kechadi, M.-T. and Pirttikangas, S. (2020). Privacy-aware blockchain innovation for 6g: Challenges and opportunities, *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5. http://dx.doi.org/10.1109/6GSUMMIT49458.2020.9083832.

Ni, J., Lin, X. and Shen, X. S. (2018). Efficient and secure service-oriented authentication supporting network slicing for 5g-enabled iot, *IEEE Journal on Selected Areas in Communications* **36**(3): 644–657. http://dx.doi.org/10.1109/JSAC.2018.2815418.

Nieto, A. (2018). An overview of proactive forensic solutions and its applicability to 5g, *2018 IEEE 5G World Forum (5GWF)*, pp. 191–196. http://dx.doi.org/10.1109/5GWF.2018.8516940.

Nieto, A., Nomikos, N., Lopez, J. and Skianis, C. (2017). Dynamic knowledge-based analysis in nonsecure 5g green environments using contextual data, *IEEE Systems Journal* **11**(4): 2479–2489. http://dx.doi.org/10.1109/JSYST.2015.2477782.

Nowak, T. W., Sepczuk, M., Kotulski, Z., Niewolski, W., Artych, R., Bocianiak, K., Osko, T. and Wary, J.-P. (2021). Verticals in 5g mec-use cases and security challenges, *IEEE Access* **9**: 87251–87298. http://dx.doi.org/10.1109/ACCESS.2021.3088374.

Omone, O. M., Kucarov, M., Benhamida, A., Vincze, M. and Kozlovszky, M. (2021). Cybersecurity aspects of location-based services (lbs) in 5g networks, *2021 IEEE 21st International Symposium on Computational Intelligence and Informatics (CINTI)*, pp. 000079–000084. http://dx.doi.org/10.1109/CINTI53070.2021.9668499.

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. and Lopez, D. (2020). Inspire-5gplus: Intelligent security and pervasive trust for 5g and beyond networks, *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ARES '20, Association for Computing Machinery, New York, NY, USA. http://dx.doi.org/10.1145/3407023.3409219.

Osorio, D. P. M., Olivo, E. E. B., Alves, H. and Latva-Aho, M. (2020). Safeguarding mtc at the physical layer: Potentials and challenges, *IEEE Access* **8**: 101437–101447. http://dx.doi.org/10.1109/ACCESS.2020.2996383.

Panwar, N. and Sharma, S. (2020). Security and privacy aspects in 5g networks, *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, pp. 1–5. http://dx.doi.org/10.1109/NCA51143.2020.9306740.

Peltonen, A., Sasse, R. and Basin, D. (2021). A comprehensive formal analysis of 5g handover, *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '21, Association for Computing Machinery, New York, NY, USA, p. 1–12. http://dx.doi.org/10.1145/3448300.3467823.

Pham, Q.-V., Fang, F., Ha, V. N., Piran, M. J., Le, M., Le, L. B., Hwang, W.-J. and Ding, Z. (2020). A survey of multi-access edge computing in 5g and beyond: Fundamentals, technology integration, and state-of-the-art, *IEEE Access* **8**: 116974–117017. http://dx.doi.org/10.1109/ACCESS.2020.3001277.

Pérez, J., Díaz, J., Garcia-Martin, J. and Tabuenca, B. (2020). Systematic literature reviews in software engineering—enhancement of the study selection process using cohen's kappa statistic, *Journal of Systems and Software* **168**: 110657. http://dx.doi.org/https://doi.org/10.1016/j.jss.2020.110657.

Rahimi, H., Zibaeenejad, A., Rajabzadeh, P. and Safavi, A. A. (2018). On the security of the 5g-iot architecture, *Proceedings of the International Conference on Smart Cities and Internet of Things*, SCIOT '18, Association for Computing Machinery, New York, NY, USA. http://dx.doi.org/10.1145/3269961.3269968.

Raj, D., Lekshmi, S. S., Nair, B. B. and Ponnekanti, S. (2019). Effective gi-lan optimisation towards hardening the 5g service provider platform, *2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, pp. 543–547. http://dx.doi.org/10.1109/WiSPNET45539.2019.9032776.

Ramezan, G., Leung, C. and Wang, Z. J. (2018). A survey of secure routing protocols in multi-hop cellular networks, *IEEE Communications Surveys & Tutorials* **20**(4): 3510–3541. http://dx.doi.org/10.1109/COMST.2018.2859900.

Ranaweera, P., Jurcut, A. D. and Liyanage, M. (2021a). Survey on multi-access edge computing security and privacy, *IEEE Communications Surveys & Tutorials* **23**(2): 1078–1124. http://dx.doi.org/10.1109/COMST.2021.3062546.

Ranaweera, P., Jurcut, A. and Liyanage, M. (2021b). Mec-enabled 5g use cases: A survey on security vulnerabilities and countermeasures, *ACM Comput. Surv.* **54**(9). http://dx.doi.org/10.1145/3474552.

Roth, S., Tomasin, S., Maso, M. and Sezgin, A. (2021). Localization attack by precoder feedback overhearing in 5g networks and countermeasures, *IEEE Transactions on Wireless Communications* **20**(7): 4100–4112. http://dx.doi.org/10.1109/TWC.2021.3055851.

Saglam, E. T. and Bahtiyar, S. (2019). A survey: Security and privacy in 5g vehicular networks, *2019 4th International Conference on Computer Science and Engineering (UBMK)*, pp. 108–112. http://dx.doi.org/10.1109/UBMK.2019.8907026.

Saleem, K., Alabduljabbar, G. M., Alrowais, N., Al-Muhtadi, J., Imran, M. and Rodrigues, J. J. P. C.

(2020). Bio-inspired network security for 5g-enabled iot applications, *IEEE Access* **8**: 229152–229160. http://dx.doi.org/10.1109/ACCESS.2020.3046325.

Schinianakis, D. (2017). Alternative security options in the 5g and iot era, *IEEE Circuits and Systems Magazine* **17**(4): 6–28. http://dx.doi.org/10.1109/MCAS.2017.2757080.

Schinianakis, D., Trapero, R., Michalopoulos, D. S. and Crespo, B. G.-N. (2019). Security considerations in 5g networks: A slice-aware trust zone approach, *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–8. http://dx.doi.org/10.1109/WCNC.2019.8885658.

Schmittner, M., Asadi, A. and Hollick, M. (2017). Semud: Secure multi-hop device-to-device communication for 5g public safety networks, *2017 IFIP Networking Conference (IFIP Networking) and Workshops*, pp. 1–9. http://dx.doi.org/10.23919/IFIPNetworking.2017.8264846.

Shah, S. and Pramod Bendale, S. (2019). An intuitive study: Intrusion detection systems and anomalies, how ai can be used as a tool to enable the majority, in 5g era, *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, pp. 1–8. http://dx.doi.org/10.1109/ICCUBEA47591.2019.9128786.

Sharma, S., Satapathy, S., Singh, S., Sahu, A. K., Obaidat, M. S., Saxena, S. and Puthal, D. (2018). Secure authentication protocol for 5g enabled iot network, *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pp. 621–626. http://dx.doi.org/10.1109/PDGC.2018.8745799.

Sheoran, A., Fahmy, S., Peng, C. and Modi, N. (2019). Nascent: Tackling caller-id spoofing in 4g networks via efficient network-assisted validation, *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pp. 676–684. http://dx.doi.org/10.1109/INFOCOM.2019.8737567.

Shin, D., Yun, K., Kim, J., Astillo, P. V., Kim, J.-N. and You, I. (2019). A security protocol for route optimization in dmm-based smart home iot networks, *IEEE Access* **7**: 142531–142550. http://dx.doi.org/10.1109/ACCESS.2019.2943929.

Shin, S. and Kwon, T. (2018). Two-factor authenticated key agreement supporting unlinkability in 5g-integrated wireless sensor networks, *IEEE Access* **6**: 11229–11241. http://dx.doi.org/10.1109/ACCESS.2018.2796539.

Siddiqui, M., Escalona, E., Trouva, E., Kourtis, M., Kritharidis, D., Katsaros, K., Spirou, S., Canales, C. and Lorenzo, M. (2016). 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)*, pp. 44–49. http://dx.doi.org/10.1109/NFV-SDN.2016.7919474.

Singh, P., Pawar, P. and Trivedi, A. (2018). Physical layer security approaches in 5g wireless communication networks, *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pp. 477–482. http://dx.doi.org/10.1109/ICSCCC.2018.8703344.

Soldani, D. (2019). 5g and the future of security in ict, *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–8. http://dx.doi.org/10.1109/ITNAC46935.2019.9078011.

Soós, G. and Varga, P. (2019). On the security threat of abandoned and zombie cellular iot devices, *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, Vol. 1, pp. 996–1001. http://dx.doi.org/10.1109/INDIN41052.2019.8972107.

Spinelli, F. and Mancuso, V. (2021). Toward enabled industrial verticals in 5g: A survey on mec-based approaches to provisioning and flexibility, *IEEE Communications Surveys & Tutorials* **23**(1): 596–630. http://dx.doi.org/10.1109/COMST.2020.3037674.

Sullivan, S., Brighente, A., Kumar, S. A. P. and Conti, M. (2021). 5g security challenges and solutions: A review by osi layers, *IEEE Access* **9**: 116294–116314. http://dx.doi.org/10.1109/ACCESS.2021.3105396.

Suomalainen, J., Juhola, A., Shahabuddin, S., Mämmelä, A. and Ahmad, I. (2020). Machine learning threatens 5g security, *IEEE Access* **8**: 190822–190842. http://dx.doi.org/10.1109/ACCESS.2020.3031966.

Suomalainen, J., Julku, J., Vehkaperä, M. and Posti, H. (2021). Securing public safety communications on commercial and tactical 5g networks: A survey and future research directions, *IEEE Open Journal of the Communications Society* **2**: 1590–1615. http://dx.doi.org/10.1109/OJCOMS.2021.3093529.

Tang, B.-h. and Zhou, Z.-x. (2021). 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*, ICCPR 2020, Association for Computing Machinery, New York, NY, USA, p. 405–412. http://dx.doi.org/10.1145/3436369.3436481.

Tang, Q., Ermis, O., Nguyen, C. D., Oliveira, A. D. and Hirtzig, A. (2022). A systematic analysis of 5g networks with a focus on 5g core security, *IEEE Access* **10**: 18298–18319. http://dx.doi.org/10.1109/ACCESS.2022.3151000.

Tanveer, J., Haider, A., Ali, R. and Kim, A. (2022). Machine learning for physical layer in 5g and beyond wireless networks: A survey, *Electronics* **11**(1). http://dx.doi.org/10.3390/electronics11010121.

Thantharate, A., Paropkari, R., Walunj, V., Beard, C. and Kankariya, P. (2020). Secure5g: A deep learning framework towards a secure network slicing in 5g and beyond, *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0852–0857. http://dx.doi.org/10.1109/CCWC47524.2020.9031158.

Tian, F., Zhang, P. and Yan, Z. (2017). A survey on c-ran security, *IEEE Access* **5**: 13372–13386. http://dx.doi.org/10.1109/ACCESS.2017.2717852.

Torroglosa-Garcia, E. M., Calero, J. M. A., Bernabe, J. B. and Skarmeta, A. (2020). Enabling roaming across heterogeneous iot wireless networks: Lorawan meets 5g, *IEEE Access* **8**: 103164–103180. http://dx.doi.org/10.1109/ACCESS.2020.2998416.

van den Broek, F., Verdult, R. and de Ruiter, J. (2015). Defeating imsi catchers, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, Association for Computing Machinery, New York, NY, USA, p. 340–351. http://dx.doi.org/10.1145/2810103.2813615.

Varga, P., Peto, J., Franko, A., Balla, D., Haja, D., Janky, F., Soos, G., Ficzere, D., Maliosz, M. and Toka, L. (2020). 5g support for industrial iot applications— challenges, solutions, and research gaps, *Sensors* **20**(3). http://dx.doi.org/10.3390/s20030828.

Vidal, J. M., Monge, M. A. S. and Villalba, L. J. G. (2018). Detecting workload-based and instantiation-based economic denial of sustainability on 5g environments, *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, Association for Computing Machinery, New York, NY, USA. http://dx.doi.org/10.1145/3230833.3233247.

Vijay, A. and Umadevi, K. (2019). 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)*, pp. 468–472. http://dx.doi.org/10.1109/ICOEI.2019.8862712.

Wang, M. and Yan, Z. (2015). Security in d2d communications: A review, *2015 IEEE Trustcom/BigDataSE/ISPA*, Vol. 1, pp. 1199–1204. http://dx.doi.org/10.1109/Trustcom.2015.505.

Wang, N., Jiao, L., Alipour-Fanid, A., Dabaghchian, M. and Zeng, K. (2020). Pilot contamination attack detection for noma in 5g mm-wave massive mimo networks, *IEEE Transactions on Information Forensics and Security* **15**: 1363–1378. http://dx.doi.org/10.1109/TIFS.2019.2939742.

Wazid, M., Das, A. K., Shetty, S., Gope, P. and Rodrigues, J. J. P. C. (2021). Security in 5g-enabled internet of things communication: Issues, challenges, and future research roadmap, *IEEE Access* **9**: 4466–4489. http://dx.doi.org/10.1109/ACCESS.2020.3047895.

Wijethilaka, S. and Liyanage, M. (2021). Survey on network slicing for internet of things realization in 5g networks, *IEEE Communications Surveys & Tutorials* **23**(2): 957–994. http://dx.doi.org/10.1109/COMST.2021.3067807.

Xingzhong, J., Qingshui, X., Haifeng, M., Jiageng, C. and Haozhi, Z. (2019). The research on identity authentication scheme of internet of things equipment in 5g network environment, *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, pp. 312–316. http://dx.doi.org/10.1109/ICCT46805.2019.8947126.

Xuesong, H., Wei, L., Tao, Z., Haidong, H., Kangle, Y. and Pei, P. (2021). An endogenous security protection framework adapted to 5g mec in power industry, *2021 China Automation Congress (CAC)*, pp. 5155–5159. http://dx.doi.org/10.1109/CAC53003.2021.9728395.

Yang, C., Li, H., Wang, L. and Tang, D. (2018). Exploring the behaviors and threats of pollution attack in cooperative mec caching, *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6. http://dx.doi.org/10.1109/WCNC.2018.8377317.

Zenger, C. T., Zimmer, J., Pietersz, M., Driessen, B. and Paar, C. (2016). Constructive and destructive aspects of adaptive wormholes for the 5g tactile internet, *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '16, Association for Computing Machinery, New York, NY, USA, p. 109–120. http://dx.doi.org/10.1145/2939918.2939923.

Zhang, J., Yang, L., Cao, W. and Wang, Q. (2020). Formal analysis of 5g eap-tls authentication protocol using proverif, *IEEE Access* **8**: 23674–23688. http://dx.doi.org/10.1109/ACCESS.2020.2969474.

Zhao, G., Zhang, F., Yu, L., Zhang, H., Qiu, Q. and Xu, S. (2021). Collaborative 5g multiaccess computing security: Threats, protection requirements and scenarios, *2021 ITU Kaleidoscope: Connecting Physical and Virtual Worlds (ITU K)*, pp. 1–8. http://dx.doi.org/10.23919/ITUK53220.2021.9662088.

Zhao, J., Ding, B., Guo, Y., Tan, Z. and Lu, S. (2021). Securesim: Rethinking authentication and access control for sim/esim, *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, MobiCom '21, Association for Computing Machinery, New York, NY, USA, p. 451–464. http://dx.doi.org/10.1145/3447993.3483254.

Zhao, L., Oshman, M. S., Zhang, M., Moghaddam, F. F., Chander, S. and Pourzandi, M. (2021). Towards 5g-ready security metrics, *ICC 2021 - IEEE International Conference on Communications*, pp. 1–6. http://dx.doi.org/10.1109/ICC42927.2021.9500349.