


IoT and 5G Networks: A Discussion of SDN, NFV and Information Security


Roger William Coelho   [State University of Maringá | roger.coelho04@gmail.com]

Ronan Assumpção Silva   [Federal Institute of Paraná | ronan.silva@ifpr.edu.br]

Luciana Andréia Fondazzi Martimiano   [State University of Maringá | lafmartimiano@uem.br]

Elvio João Leonardo   [State University of Maringá | ejleonardo@uem.br]

 Department of Informatics, State University of Maringá (UEM), Av. Colombo, 5790 - Jd. Universitário, CEP 87020-900, Maringá, PR, Brazil

 IT Department, Federal Institute of Paraná (IFPR), Rua Antonio Chemin, 28 - São Gabriel, CEP 8340-3515, Colombo, PR, Brazil

Received: 14 November 2023 • **Accepted:** 11 January 2023 • **Published:** 10 August 2024

Abstract Having an infrastructure capable of exchanging data at high speed is an efficient way to drive the evolution and development of new applications and existing services. The 5G technology has emerged as a trusted source to meet the increased demand of Internet of Things (IoT) devices connected to the network, in addition to enabling Internet connectivity at high broadband speeds. Another important feature of 5G is to allow the use of Software Defined Network (SDN) and Network Function Virtualization (NFV), mechanisms responsible for performing network configurations through software, as well as the control and management of devices using the configuration network functions or device virtualization. The concern with information security in the 5G network is increasing, as cybercriminals try to access important data that is transported over the network, since the demand for connected IoT devices will be greater, allowing for several possibilities of attacks. The understanding of possible threats and attacks is necessary, so that new measures are taken against cybercrimes presented in the 5G and IoT networks. This paper aims to elucidate some conceptions of what 5G technology is and the use of IoT in this network, contextualizing the SDN and NFV paradigms to allow the configuration of the functionality and management of the network by software. In addition, concerns are reported about possible information security attacks that can occur in 5G networks.

Keywords: 5G Network, Internet of Things (IoT), Information Security, Software Defined Network (SDN), Network Function Virtualization (NFV), Link Layer, Physical Layer

1 Introduction

Communication over networks is an essential mechanism for services and products to be quickly accessed and demanded. We see a huge growth in the consumption of data by users, who have expectations of a more technological society, with smarter services and quicker access to information [Varum *et al.*, 2018]. Having an infrastructure capable of transmitting data at high speed is one of the ways to promote the evolution of existing applications and enable new types of activities in data networks.

Users want mobility to access information anywhere with their devices, and for that, a secure, high speed wireless network must provide the means for user demands to be met. With the advent of wireless (mobile) network, it has been possible to offer access to information on personal equipments, such as smartphones and laptops, from anywhere without the need to connect to the Internet through cables [Barona López *et al.*, 2017]. For this to become possible, it has been necessary a constant evolution of wireless data networks that provide better quality in data transport, security, and speed.

The 5G network is not only an evolution of 4G networks, but also a system with many features, such as the use of

SDN and NFV for network configuration that allows for better quality of service and security. It is possible to use it, for instance, in remote health monitoring equipment, in Industry 4.0, in the agricultural sector and in the Internet of Things (IoT) as a whole, with better quality in the information transmission. The 5G network aims to seek lower latency and lower energy consumption, precisely to facilitate the implementation and connection of new devices to the network [Fang *et al.*, 2018].

The IoT is a promising and emerging technology that has the characteristic of revolutionizing the connectivity of various objects transmitting data over the network. IoT deals with low capacity, low power equipments that interact via the Internet. The IoT network connects washing machines, refrigerators, presence sensors, drones, among other devices, through a common interface, allowing data communication over the network. IoT is expected to enable a new business environment with a direct impact on everyday life [Akpakwu *et al.*, 2018]. Thus, it is necessary to ensure the information security to protect the data that is transmitted.

When thinking about information security in new network technologies such as 5G and IoT, some questions arise about how to deal with this challenge, especially when different de-

VICES are connected. With an inadequately developed security project, the entire system is compromised and the limitations stem from inefficient protection, ease of access for people who should not have authorization and the lack of updating of the hardware in the network, among other problems that can be found [Mathew, 2020]. Some techniques, such as network splitting, virtualization, and SDN are used to contribute to information security.

This paper aims to elucidate: SDN and NFV techniques in the 5G network; how IoT devices can be massively used to transmit important information and the necessity of security in data transmission; which are the types of attacks against the 5G and IoT networks; and the security mechanisms that can be used to protect information transmitted in 5G networks.

The remaining of the paper is organized as follows: Sect. 2 describes some related works; Sect. 3 discusses 5G technology, the use of SDN and NFV to enable the software configurations implementation in the network; Sect. 4 covers IoT networks and their connections to the 5G network; in Sect. 5, it is discussed about the security system of the 5G network, the types of attacks that can occur in the physical and link layers; Sect. 6 presents the conclusion.

2 Related Works

This section describes some papers that discuss issues about information security in 5G and IoT networks and the use of SDN, NFV and pattern recognition, among other techniques.

In [Shin *et al.*, 2019], it is established that the security of IoT devices in 5G network must have secure routes. According to the authors, no academic work on secure routes in Distributed IP Mobility Management (DMM) has been established. Therefore, the need to better identify the possibilities of secure routes between IoT devices is essential. Thus, the authors propose a communication protocol for secure routes between devices, whose phases are composed of route optimization initialization and handover, in order to provide authentication, key exchange, routing secrecy and privacy protection. Protocol security is verified using two security analysis tools, Burrows-Abadi-Needham (BAN) logic and Automated Validation of Internet Security Protocols and Applications (AVISPA). According to the authors' demonstration, the proposed protocol ensures better efficiency in the design of secure routes for data transmission from IoT devices, compared to other protocols used.

In [Carrozzo *et al.*, 2020], the authors propose a concept that is called zero-touch security and trust architecture for ubiquitous computing and connectivity to 5G networks. The proposed architecture aims at inter-domain security and the use of reliable orchestration mechanisms through the coupling of Distributed Ledger Technologies (DLT) with operations guided by Artificial Intelligence (AI). All automation of the proposed architecture uses SDN and NFV techniques to secure data communication.

The study carried out by [Li *et al.*, 2023] proposes a framework that integrates Reinforcement Learning (RL) together with an SDN, NFV and Interface for Network Security Functions (I2NSF) architecture, in which the RL agent can select

the Security Functions Chain (SFC) suitable for Distributed Denial-of-Service (DDoS) attack scenario. The DDoS detection problem is modeled using the Markov Decision Process (MDP), and the authors propose an algorithm for detecting the attack. The designed algorithm is compared with other RL algorithms to test its efficiency.

The work presented in [Ravi *et al.*, 2019] aims at the development of security, in 5G networks, through a framework based on deep machine learning to detect and prevent the propagation of attacks. The proposed framework uses decentralized SDN controllers to avoid possible failures in the security management mechanisms. The framework is composed of three main components whose objectives are the monitoring, detection, and mitigation of attacks. Machine learning data is based on observed traffic with previously identified attacks, thus improving efficiency by recognizing patterns of potential security threats.

In [Kabir *et al.*, 2020], an experimental implementation of a Security Policy Management (SPM) system for 5G networks is proposed, which considers the basic principles for the security of end devices. They also propose an overall security architecture, where policies are defined for devices or services on a network slice, providing reliability to access information from those devices. The main aspects of the proposed architecture are the use of SDN techniques, a policy front-end and SPM to resolve the security issues of the end devices connected in the network, while a Customer Edge Switching (CES) firewall at the edge of the network enforces the use of the implemented security policies.

The work presented by [Coelho *et al.*, 2023] discusses the characteristics of SDN, NFV and information security in 5G and IoT networks. The Survey presents classifications of attacks against integrity, availability, centralized policy, privacy, visibility, and authentication. Through this classification, the authors list the types of attacks that each classified element can suffer. Some types of attacks that can occur against 5G and IoT networks are also described, such as radio frequency attacks, battery drain attacks, among others.

The proposal presented in [Abdulqadder *et al.*, 2020b] uses SDN, NFV and AI techniques to implement an approach against security attacks in 5G networks, with the objective of creating an Intrusion Detection System (IDS) based on multi-layers. The five layers used for IDS creation are: data acquisition, switches, domain controllers, smart controller, and virtualization layer. The proposed system allows the verification, mitigation and blocking of different security attacks such as Spoofing, Flow Table Overloading, Denial of Service (DoS), Control Plane Saturation and Host Location Hijacking.

The work in [Zhao *et al.*, 2021] presents the proposal of an algorithm that aims to recommend the privacy requirements of a device connected to 5G and IoT networks through Location-Based Services (LBS). This approach is like identifying trusted endpoints to prevent Man-in-the-Middle (MITM) attacks. The authors present a cross-authentication protocol, which is the basis for using the algorithm. In this protocol, authentications are performed through the physical layer specifying authentication keys between devices and 5G network terminals.

In [Das *et al.*, 2023] a study is presented that offers a

Blockchain-enabled SDN framework to secure transactions that make use of SDN and NFV. The framework proposed by the authors addresses the Man-in-the-Middle attack between the control plane and the data plane in SDN networks. A controller authentication scheme was designed to provide smart contracts. Smart contracts automatically perform controller authentication and controller verification. This framework was designed by the authors to improve the transparency and security of users' data privacy.

The work proposed in [Li *et al.*, 2021] aims to identify threats such as Spoofing, in which the attackers can disguise as legitimate users by modifying their own identity. The authors rely on the use of channel based security technique to identify possible threats from this type of attack. The work presents a new attack detection scheme based on the virtual representation of channels in 5G networks, where two detection strategies are offered, one for static radio environments through the Neyman-Pearson (NP) test and another for dynamic radio where channel correlation is constantly changing. In this case, the detection structure is online based on a neural network feedforward with a single hidden layer.

As can be seen, there are works that deal with information security in 5G and IoT networks. However, many of them aim to exploit and control vulnerabilities found in the network layer and application layer of the TCP/IP model, using SDN, NFV and pattern recognition techniques. However, there is still a wide range of possibilities that can be explored to improve security in these environments.

The data link layer and physical layer have little research on security. With the emergence of new transmission technologies, new protocols are formalized and many of them are not adequately concerned with the security that will be used to transport information. In this way, cybercriminals exploit vulnerabilities in the physical and link layers to compromise data sent and received over the network, affecting the integrity, reliability and availability of information, in relation to these layers and to the upper layers of TCP/IP .

3 5G Technology

3.1 5G new data communication network platform

5G technology has emerged as the newest data communication network. This evolution was necessary due to the growth of more demanding users and new business opportunities that require low latency and higher speed in the information transmission. Much of this is due to the fact of some challenges that the 4G network has been facing, for instance, the connectivity of different IoT devices or because of the increased data consumption by users [Nam *et al.*, 2016].

5G is a multiple access technique through radio technology using existing media from other generations, such as Long-Term Evolution (LTE), from 4G, and the new radio (NR) to 5G, in addition to the Wireless Local Area Network (WLAN) in the design of the new Wi-Fi 6. In addition, 5G has enabled the integration of most emerging network paradigms such as cloud computing, SDN, NFV, spectrum division network and the new concept of cutting-edge computing [Liyan-

age *et al.*, 2018]. The 5G network allows to tackle some problems from previous generations and new opportunities for the applications development and services, such as the massive use of IoT. 5G networks contribute to improve Internet broadband services, providing mechanisms for network operators with more quality in the services provided, contributing to a better user experience in obtaining information at high speed. In this way, the 5G technology features that contribute to the network services improvement can be classified in stages as [Meng *et al.*, 2020]:

- Enhanced Mobile Broadband (eMBB).
- Ultra-Reliable low-latency communications (URLLC) and Machine-Type Communications (MTC).
- Massive Machine Type Communications (mMTC).

This technology implements network virtualization and slicing, so that services are implemented according to their characteristics and demands. Another feature that can be mentioned is that 5G networks are composed of thousands of small cells that provide a dense network for data transmission. The purpose of this feature is for greater efficiency in transmission rates and low data latency. With the use of small cells, it is possible to create subnets that will be able to carry out the necessary services according to user demand. These subnets contribute to the routing of local data traffic for calls from local users sending signaling to the core network [Asif, 2019].

An important advance for radio transmission in 5G technology, consists of geographically distributing several antennas with the massive use of Multiple Input Multiple Output (MIMO). This technique was developed to expand the coverage area of the signal generated by the 5G radio, avoiding the loss of information due to natural obstacles or the penetration of signals on the walls of buildings. It is noteworthy that the use of such a technique provides new opportunities, a user can be in a car or even on a train and have high speed Internet access with guaranteed download and upload transmissions to receive and send data without loss of connection with the towers that are part of the installed architecture [Gupta and Jha, 2015].

Figure 1 shows the architecture of 5G networks, and their geographic distribution of antennas and devices connected to the network.

As can be seen in the **Figure 1**, there is the possibility of interconnecting several different devices to the network and each one with its respective utility. With the network slice technique, services can be allocated in an organized way, providing better demand management for the activities offered. Thus, by implementing a network for vehicular communication devices, for example, the members of this network can communicate with greater efficiency and security, transmitting important data for processing the necessary information for proper decision-making on the service offered.

Furthermore, it can be said that, with the expansion of the use of massive MIMO, the expansion of the connection capacity, through the distribution of hundreds or thousands of antennas, contributes to a better signal reception quality and, consequently, greater data transmission. Speeds are guaranteed and the user can consume large amounts of data with

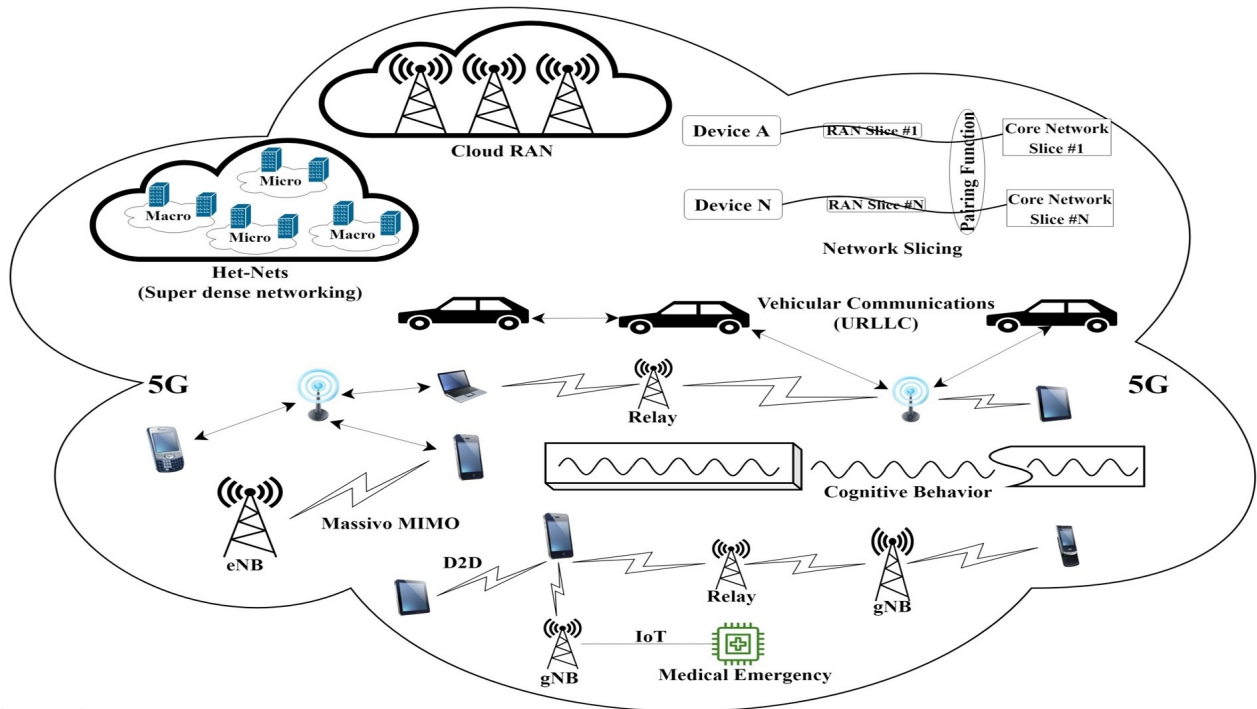


Figure 1. 5G network architecture [Asif, 2019].

quality of service. But, for the management of the 5G network to be carried out efficiently, some techniques such as SDN and NFV were introduced to improve the system, contributing to a greater user experience in terms of agility and information transmission, allowing the networks configuration with unique characteristics.

3.2 Software Defined Network

The SDN system can be used for various possibilities in the 5G network, from the virtualization of physical equipment to the management of information security. A fundamental paradigm for the development of networks with 5G technology is the use of the SDN. This paradigm controls data transmission, virtualizing devices and contributing to network management. SDN is a method to make the network programmable, therefore, basic network functions, such as packet forwarding, are performed virtually by physical devices replicated in software, allowing for customized network configuration [Chahlaoui et al., 2019]. In this way, the 5G network can be used as a heterogeneous data network capable of connecting different devices and carrying out a configuration capable of adapting. However, new challenges arise, especially in security.

Figure 2 shows a scenario using SDN. In this case, the SDN is a central controller used to manage the 5G network, which is divided into scenarios with specific characteristics such as agribusiness, industrial and smart city. In other words, each controller is responsible for managing the network devices found in each network slice.

This leads to better equipment management and allows the network to be programmed according to the business plan for which it was designed. For example, industrial sensor equipments can be controlled through programming performed in

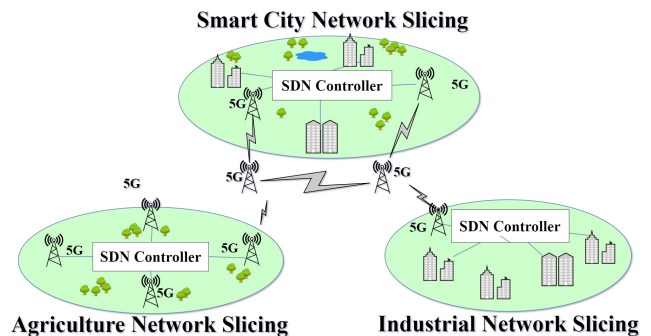


Figure 2. SDN Controller in 5G Network Slicing.

the industry’s SDN controller. In turn, the agro can use crop sensors to monitor forecast information on the use of pesticides, and in the smart city network SDN controller can be used for vehicular traffic monitoring.

SDN allows network control to be performed through a central controller that has the concept of decoupling the control plane from the data plane. This allows a centralized controller to be used to manage the 5G network, providing advantages including solutions for the security of transmitted information. Specifically, regarding security, three attributes can be considered when using SDN [Liang and Qiu, 2016]:

1. Logically centralized intelligence.
2. Programmability.
3. Abstraction.

SDN will centralize the logical use of network control for traffic management as a tool capable of allocating mobile internet resources, performing network slice and promoting revenue improvements after equipment virtualization. It can be said that the 5G technology with the use of SDN allows

several scenarios that are usable for the following purposes [Costa-Requena et al., 2015]:

- Network traffic flow can be segregated by multiple mobile virtual network operators (MVNO) to share available physical resources.
- The data stream can be optimally redirected to a specific service that is available in the network.
- Resource management can be better executed, such as optimizing the power resources of connected devices as well as data resources consumed by users in the network.

With regard to network management, the SDN system can promote better resource management by allowing the control plane to be decoupled from the data plane. With the centralization of the control plane, some types of attacks can be exploited by a cybercriminal, such as denial of service. Intrusion Detection Systems (IDS), using the SDN technique, can verify possible anomalies in the network and predict or block attacks. Another example of using IDS is the implementation of a system that uses reactive routing. In this system, the flow must go through the packet inspection process and make the decision based on the rules configured in the SDN system, thus being able to discard possible malicious packets that travel through the network. A problem with this approach is to perform inspection only on the first received packet, not performing checks on other packets sent by the same sender [Liu et al., 2017].

Consequently, the information security must be guaranteed, from the link layer, of the new transmission technology, to the application layer. Thus, SDN can provide new security mechanisms that aim to verify potential attacks in the link layer of the 5G network, dealing with pattern recognition and preventing information from being stolen or denied by possible attacks from external agents.

3.3 Network Function Virtualization

NFV is another paradigm that can be used in 5G networks. NFV is an important mechanism for implementing network functions as software entities, that is, it performs the virtualization of the infrastructure that is part of the network project, so that some functions are implemented through software. This technique allows the evolution of services such as Voice Over Internet Protocol (VOIP) and IoT, facilitating virtualization and the architectural structure that can be used by any application or service available. This framework facilitates dynamic management of NFV instances, and it also allows the management between the relationships of the NFVs that control the data and other attributes that are necessary for the network management, services and applications that are designed by a software infrastructure [Asif, 2019].

The NFV allows a series of different modalities and services to be executed in the network, promoting advances in new infrastructures and management possibilities. Some of these new trends can be identified as [Yi et al., 2018]:

1. *Physical Network Function (PNF)*: This technique aims to design a block with a specialized function and well

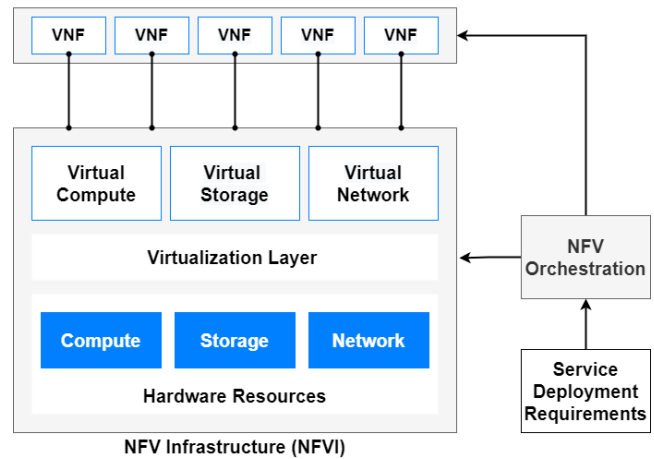


Figure 3. NFV Infrastructure (NFVI) [?].

defined behavior, characterized by a network node or physical device.

2. *Network Function Virtualization Infrastructure (NFVI)*: This technique is responsible for providing a network environment with hardware and software components, in order to manage the assets connected to the network.
3. *Element Management System (EMS)*: This system is responsible for managing the instances of Virtual Network Functions (VNFs).
4. *Management and Orchestration (MANO)*: MANO is responsible for managing and allocating new resources in the network. This technique can be divided into three elements, the Virtualized Infrastructure Manager (VIM), the Virtual Network Function Manager (VNFM) and the NFV Orchestrator (NFVO), responsible for managing NFVI, among other features.
5. *Virtual Network Function (VNF)*: This technique consists of implementing PNF in software, that is, it provides the same functional behaviors as PNF. VNF is only implemented on a virtual machine (VM) and is composed of a single component. If VNF is implemented in multiple VMs, it will be composed of multiple components.
6. *Network Point of Presence (N-PoP)*: It is responsible for indicating the location of the network where the PNF and VNF will be implemented.

Figure 3 is an NFV structure that allows to implement and execute network functions, even allowing the virtualization of some network functions that can be designed via software. Implementation and execution are guided by a management system through metadata that describe the functionalities and characteristics of the network services that will be virtualized. Such a system can be extended to the use of cloud infrastructure, promoting new ways of controlling and managing the network at any location remotely and automatically [?].

Using the NFV technique, network designers are able to produce a certain function for the internet being configured, facilitating the implementation of the business strategy for which the network was designed. Implementing these strategies allows the manager to configure your entire network infrastructure through software. However, as more of these features are implemented, new challenges arise, especially in the field of information security.

3.4 SDN versus NFV

SDN and NFV are paradigms present in the 5G network that can allow the sharing of many properties that complement each other. Both paradigms aim to innovate functionality and services through an ecosystem of Software Based Networks. SDN can serve NFV through programmable network connectivity between VNFs for optimized traffic engineering. In turn, NFV can help SDN to virtualize SDN elements such as the SDN controller, data forwarding entities to run in the cloud, and enable dynamic migration of roles to specific locations on the network. [Nguyen *et al.*, 2017].

The combination of SDN and NFV allows dynamic and flexible deployment of services that can be inserted into the 5G network. These features and characteristics encourage the development of network splitting and new services that can be programmable to give the network greater flexibility. This allows devices with similar performance requirements to be inserted into a specific part of the network [Medhat *et al.*, 2017]. For example, crop monitoring equipment is placed in a 5G spectrum band for agricultural functionality, in the same way that industrial sensors can be grouped together to send specific data for Industry 4.0. Traffic flows can also be routed through an ordered list of functions that can be processed by firewalls or load balancers for better data throughput on the network [Bifulco *et al.*, 2016].

As far as network programming is concerned, there is no need to use the two paradigms together, but when working with network slice and the need to use IoT devices for specific characteristics in 5G implementation, SDN and NFV should work together. Thus, the demand for a programmable network allows the infrastructure to be related specifically to the business plan for which it was designed. It allows the network to not only be programmable, but also it is possible to group together specific functions and services that this subnet of the network can perform in a virtualized way.

4 Internet of Things

The IoT provides several opportunities in different areas such as education, industry 4.0, agriculture, among others. Thus, a comprehensive analysis of the information security of the various devices connected to the network and how to ensure that data is not stolen, modified and denied to legitimate users is required. The contribution of the scientific community helps developers and large companies to design and propose solutions capable of mitigating possible threats that can harm the security of the IoT network, and thus provide reliable services [Saleem *et al.*, 2020].

With the rise of network connected IoT devices and the advent of 5G, the severity of potential security attacks increases. A lot of data will be transported by this new transmission technology and there are still many uncertainties about how security will be established. Although technology advances significantly with each generation, the handling of critical technological issues remains undefined, allowing a vast environment for malicious agents to exploit potential vulnerabilities [Mir *et al.*, 2020].

Studying and improving security techniques and verifying new possibilities to prevent and avoid a potential attack, both

in 5G and IoT networks, are important to ensure the integrity, reliability and confidentiality. Many studies are looking at the application layer, the network and the edge of the network when it comes to IoT and 5G. Traffic monitoring, encryption and anomaly detection are essential to ensure security at this layer. At the application layer, it needs to incorporate secure Applications Programming Interfaces (APIs) for forensic analysis and information verification. Finally, the edge of the network is tied to the performance of the interaction between the IoT environment and the devices at the edge of the network [Saleem *et al.*, 2020].

Many challenges still exist regarding the security of IoT equipment, even when a new data transmission technology such as 5G emerges. There are many works related to information security in the network, transport and application layers, but this area is not studied with emphasis in the link layer of the 5G network. It can be said that the physical and link layers in IoT and 5G networks should be better studied regarding possible risks to information security, because if these layers are attacked, all other layers can be compromised.

4.1 IoT Attacks

IoT devices have allowed the collection of the most varied data types, from medical information from connected equipment on patients, as well as information in smart cities from water meter or vehicle traffic. Information is a very important asset that is transmitted over the network and, due to its value, more and more people are trying to gain undue access.

Poorly configured or designed devices with low processing power allow cybercriminals to access restricted information and execute criminal activities. An example of exploiting flaws in the security of IoT objects is the botnet attack known as Mirai. This attack turns several IoT devices into bots. Through this group of bots, several DDoS attacks were around the world [Abbas *et al.*, 2020].

DDoS or DoS attacks are constantly executed because these devices are easy to control and have unauthorized access. These types of attacks can generate a large amount of traffic in the network and overload routers and other critical infrastructure, causing equipment downtime or service interruptions. Some limitations in IoT devices, such as low power consumption, memory and processing capacity, combined with the lack of firmware updates, can allow cybercriminals to gain unauthorized access and execute attacks [Kaur and Ayoade, 2023].

Many researchers develop studies that focus on DDoS attacks in IoT networks. For example, the study of [Munmun and Paul, 2021] presents DDoS attack mitigation techniques based on SDN, and presents the challenges encountered by researchers when implementing these techniques in SDN networks with IoT devices. Another example of a study is the one developed by [Sharma and Babbar, 2023], which presents an architecture based on the detection of DDoS attacks in IoT networks using different machine learning approaches, such as Decision Tree (DT), Random Forest (RF) and Naive. Bayes (NB). The objective of this study is to analyze the performance and classification of DDoS attacks using machine learning algorithms.

Other types of attacks that can happen in IoT networks are

Man-in-the-Middle and ARP Spoofing. Man-in-the-Middle attacks can be performed passively or actively. In passive, cybercriminals only analyze network traffic and do not take any other action. Active criminals can modify, prevent, and steal information that passes through any IoT device or server that is connected to the network that collects the data involved. The ARP Spoofing attack can be used to generate Man-in-the-Middle [Olazabal *et al.*, 2022] attack. ARP Spoofing is a technique by which a criminal can link his MAC address to the legitimate IP address. As a consequence, information sent by the intended IP is sent to the attacker's MAC address [Rohatgi and Goyal, 2020].

Some research are under development to mitigate, defense and blocking of Man-in-the-Middle and ARP Spoofing attacks in IoT networks. An example is the study presented by [Petrović *et al.*, 2021], where the authors present an IoT educational platform to test security vulnerabilities based on Man-in-the-Middle and ARP Spoofing. Using the platform, students can become familiar with these types of attacks and can create and simulate defense mechanisms.

Due to the large concentration of new devices connected to the network, new opportunities are created, whether good or bad. Various other types of attacks such as brute force, information theft, executed zero-day attacks, among others, can be executed by cybercriminals due to configuration or design flaws in IoT devices.

Given this possibility, new research can be carried out, whether to create algorithms, frameworks, methods, techniques, protocols, AI, among others, as possibilities for contributions to the scientific community, professionals, and companies. Information security is an area where there is a lot to learn, especially in networks where devices do not have large energy, memory, processing capacity and do not have a well-defined standardization for their use. In this sense, concerns about cybersecurity are growing and professionals in this area are increasingly valued.

5 5G Technology Security System

When a new transmission technology is incorporated into the reality of people's lives, it is to be expected that the speed and volume of data will be higher than the previous technology. But just as important as the speed of transmissions and the increased consumption of this information by users is security. Defining and designing a secure environment is essential because a lot of valuable data travels over the network.

SDN and NFV techniques are the main technological precursors of the 5G network to support the applications that run in this network. These two techniques include additional components that allow them to be configured, through software, to provide security [Mir *et al.*, 2020].

Additional algorithms, such as machine learning and management control, can be implemented through SDN and NFV to improve the security efficiency of 5G and IoT networks. Threats can be identified by correlating 5G domains with security standards applied in the 3GPP (Generation Partnership Project) Long Term Evolution Advanced (LTE-A) framework. As for information, criticality is related to network configuration, cyber attacks, data flow, commercial leaks and

other possible attacks against information that travels over the network. With the increasing availability of new radio frequencies for 5G and new data transmission protocols, concerns about security threats will become more evident. A cybercriminal can take advantage of configuration flaws and protocol vulnerabilities, allowing attacks such as Denial of Service (DoS), Distributed Denial of Service (DDoS), Radio Interference, Man-in-the-Middle (MITM) and others that do not have a concrete solution to prevent and block attacks like Zero Day attacks [Dutta and Hammad, 2020].

When running the network slicing, specific authentications are required; in addition to primary authentication, users using a slice gain greater access control and isolation between network segments, which helps prevent cybercriminals from authenticating themselves in the network as if they were legitimate users, preventing attacks such as DoS. Integrity protection, in relation to users, will prevent the injection and manipulation of packets by malicious agents [Javed and Khan Niazi, 2019].

Understanding the anatomy of an attack is critical to data security in any transmission technology. Many attacks are aimed at affecting either the network layer or the application layer of the TCP/IP model. However, many data link and physical layer attacks can be exploited, especially when a new transmission technology is introduced. Understanding how information is gathered and transmitted in the 5G network is important to predict and prevent possible attacks that may occur in these layers.

Once the physical layer is compromised, all layers above it can be compromised as well. It is a fact that many attacks take place at the network and application layers, but overlooking possible attacks at the physical layer of 5G data can open up multiple ramifications for cybercriminals to execute new types of attacks that can affect the entire network. The integrity of the network and the data that travel must be protected at all stages of information transmission, and for this, the use of NFV and SDN with pattern recognition techniques can provide greater security effectiveness in the system.

5.1 Types of attacks against the Physical and Data Link layers

Attacks happen daily on every type of projected network. A major challenge is to identify these attacks, especially zero day ones, which are actions that have never been taken or identified at any given previous time. In 5G and IoT networks the concern with security and the identification of threats are essential for the success of the transmission technology implemented. As IoT devices have characteristics of low energy consumption and processing capacity, they are good targets for cybercriminals.

5G technology is the first mobile architecture designed to allow massive use of IoT and offer multiple possibilities of use in the network. It is critical that cybercriminals do not have access to or execute attacks against this computing infrastructure and access data and make the services inaccessible with DoS or DDoS attacks. Many of the new business opportunities provide loopholes that can be exploited in Zero Day attacks, meaning billions of dollars in losses [Ghosh *et al.*, 2019].

The 5G network is also a technology that can be exploited because it was recently developed, and possible protocol failures can be identified for attacks to be carried out against more specifically at the physical layer. It is worth noting that 3GPP in release 15 defined that the physical layer and the link layer in 5G network are characterized by the name of physical layer.

Faced with the opportunity to explore various vulnerabilities and attacks in 5G and IoT networks, researchers are carrying out studies that aim to contribute to the development of security solutions. One of these studies is a systematic review carried out by Coelho *et al.* [2022] that presents a total of 23 studies that deal with information security at the physical and link layers in 5G and IoT networks. **Table 1** presents some of these studies.

However, as this paper also addresses the IoT network, we characterize the types of attacks at both the physical layer and the link layer based on the TCP/IP model. Given this, attack classifications can be identified in both layers. **Figure 4** shows a scenario of possible attacks in specific 5G networks points, which can be used by cybercriminals.

When analyzing the **Figure 4**, it is correct to state that the threat vector in the 5G network has few limits, and possible attacks can occur from mobile devices to sensor equipment, industry, IoT networks, among other environments in which the 5G is inserted. For example, Man-in-the-Middle (MITM) attacks can be launched in the Cloud Radio Access Network (C-RAN) domain, DDoS can attack the network central part, malware attacks can be launched and compromise the sensor system, among other types of threats that can damage the network [Liyanage *et al.*, 2018]. Given this complex scenario, knowing the attack anatomy is important to identify and prevent security issues and allow the creation of techniques to prevent attacks.

Several threats and attacks are already known and applied in both 5G and IoT networks. Below are some types of attacks that we classified that can occur at the physical and data link layer of 5G and IoT networks:

1. **Radio frequency (RF) jamming:** The main objective of this attack is the introduction of interference or blocking RF signals against wireless IoT devices such as drones, alarms and others.
2. **Attack to drain battery:** This type of attack affects the battery life of LTE-M and Narrow Band IoT (NB-IoT) devices. Threat agents are able to deplete battery power in a way that appears to cause devices to malfunction.
3. **Network slice attacks:** Attacks that can occur in the frequency sub-band used for a certain segment of the 5G network that an IoT service can be running. These types of attacks may be accompanied by others, such as DoS, DDoS, Man-In-The Middle, Radio Frequency, among others, making the attacked network slice insecure.
4. **Zero-day attacks:** Attacks that have no prior knowledge of their structure and damage that can occur in the network at all layers of the TCP/IP model.
5. **Man-in-the-Middle attacks:** In these types of attacks, cybercriminals can impersonate a 5G Radio Base Station (RBS) or a wireless communication device, interrupting communication and being able to see, modify

and steal information exchanges between devices. Information manipulations can be used to attack other devices present on the network or other 5G RBS as they provide information accordingly.

6. **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** In these types of attacks, a cybercriminal overloads the devices or system with interference from Radio Base Stations (RBS) and equipment over a radio link, preventing other users or equipment from connecting with the RBS or other wireless equipment connected to the network. As an example, IoT may have multiples devices interconnected over the Internet that constantly receives packets, and this type of attack reduces the productivity of an IoT device or even make it unproductive.
7. **ARP Spoofing Attacks:** In this type of attack, sends fake Address Resolution Protocol (ARP) messages to trick devices in the network into believing they are connecting with other devices or with Radio Base Stations (RBS). This way, a cybercriminal can intercept and monitor the flow of data between two or more devices in the network.
8. **Botnets:** In this type of attack, the cybercriminal uses a network of compromised systems that can be remotely controlled to execute attacks such as DoS, DDoS and others. For example, IoT devices can be used to execute Botnets attacks.
9. **MAC Table Attacks:** MAC address flooding attacks take advantage of layer 2 equipment of the TCP/IP model. Cybercriminals use spoofed source MAC addresses until the layer 2 equipment MAC address table is full. It is worth mentioning that in the 5G network these devices can be implemented via SDN in their core network.
10. **Spanning Tree Protocol Attacks:** In this type of attack, the cybercriminal can impersonate or assume the identity of a network layer 2 root device, which can lead to scenarios of network unavailability, changes in network traffic, among others. The cybercriminal can break into the 5G core network and configure root switches through SDN, potentially making the entire network unavailable or even all network traffic being monitored.
11. **International Mobile Subscriber Identity (IMSI) Attacks:** IMSI Snatch attacks are a type of privacy threat designed to locate and track specific users via their IMSI. In this type of attack, a cybercriminal can pose as a Radio Base Station (RBS) that has a higher signal incidence as if it was a legitimate RBS. In such case, the user's equipment passes all the IMSI information to the cybercriminal who manages to violate the privacy of the user equipment.

As can be seen in **Table 2**, the classification of attacks and threats was defined according to the layers. For example, Dos and DDoS attacks can be performed at both physical and data link layers; also Man-in-the-Middle attacks can happen at both layers, as a cybercriminal pose as a Radio Base Station (RBS) in 5G networks.

Table 1. Studies Extracted from the Systematic Review [Coelho et al., 2022].

Authors	Title	Publication	Data Base
[Sicari et al., 2020]	5G In the Intrnet of Things era: An overview on Security and Privacy challenges	Computer Networks	Science Direct
[Khan et al., 2020]	A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions	IEEE Communications Surveys and Tutorials	IEEE Xplore
[Zhao et al., 2021]	A fast Physical Layer Security-based Location Privacy Parameter Recommendation Algorithm in 5G IoT	China Communications	IEEE Xplore
[Jaiswal et al., 2021]	Secrecy Rate Maximization in Virtual-MIMO Enabled SWIPT for 5G Centric IoT Applications	IEEE System Journal	IEEE Xplore
[Ferrag et al., 2018]	Security for 4G and 5G Cellular Networks: A survey of Existing Authentication and Privacy Preserving Schemes	Journal of Network and Computer Applications	Science Direct
[?]	Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks	IEEE Access	IEEE Xplore
[Singh et al., 2018]	Physical Layer Security Approches in 5G Wireless Communication Networks	International Conference on Secure Cyber Computing and Communications (ICSCCC)	IEEE Xplore
[Pan et al., 2017]	Physical Layer Security Assisted 5G Network Security	IEEE 86th Vehicular Technology Conference (VTC-FALL)	IEEE Xplore
[Yerrapragada et al., 2021]	Physical Layer Security for Beyond 5G: Ultra Secure Low Latency Communications	IEEE Open Journal of the Communications Society	IEEE Xplore
[Rahimi et al., 2018]	On the Security of the 5G IoT Architecture	Internation Conference on Smart Cities and Internet of Things - SCIOT'18	ACM Digital Library

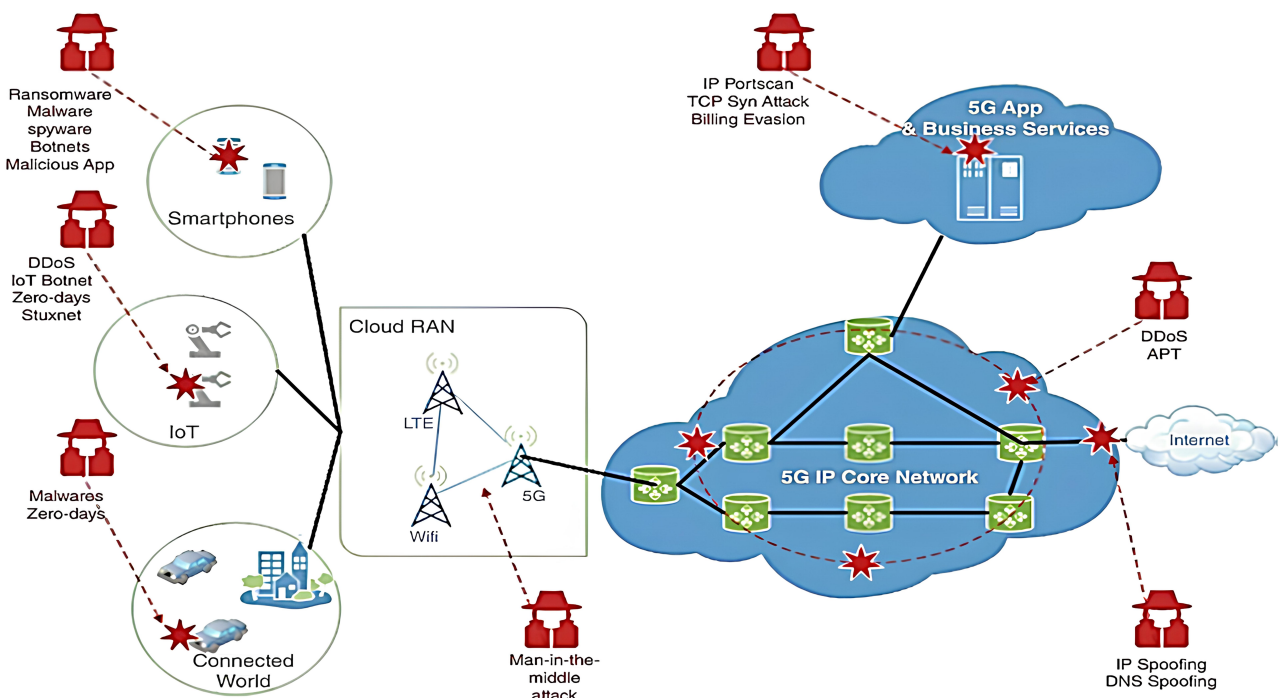


Figure 4. 5G network security threat scenario [Liyanage et al., 2018].

Table 2. Attacks and threats in 5G and IoT Networks

Layer	Types of Attacks and Threats
Physical	International Mobile Subscriber Identity (IMSI)
	DoS and DDoS
	Radio Frequency
	Eavesdropping
	Drain Battery
	Network Slice
	Zero Day
	Man-in-the-Middle
	Brute Force
	Masquerade
	Partial Message Collision
	Side Channel
	Blocking
	Encryption at Application Level
	Stolen Smart-Card
	Misconfiguration and Human errors
	Sniffing
	Leak of Verified
Link	DoS and DDoS
	MAC Table
	Spanning Tree Protocol
	Free-Riddling
	Man-in-the-Middle
	Skimming
	Eavesdropping
	ARP Spoofing
	Brute Force
	Sniffing
	Side Channel
	Blocking
	Misconfiguration and Human errors
	Partial Message Collision
	Masquerade
	Collaborated
	Stolen Smart-Card

5.2 SDN Attacks

SDN and NFV are widely used for configuration and orchestration of network functions, business plan, network slicing, among others, being widely used in the 5G network core configuration. However, new possibilities for attacks can be exploited by cybercriminals who seek to find vulnerabilities so that SDN and NFV can be breached, and information stolen.

SDN, despite offering flexibility and efficient network management at low cost, also introduces new vulnerabilities that can affect the network. SDN separates the data plane from the control plane. The control plane has the policies for forwarding frames and packets. In turn, the data plane implements the decisions where the information will be forwarded. With the centralized control plane, decision-making for network operations can be performed in a single, centralized manner. However, the separation of control and data planes can bring serious security challenges to SDN, such as reliability, scalability, security and interoperability [Abdulkarem and Dawod, 2020].

An SDN controller can be responsible for controlling all network equipment, through software, using OpenFlow chan-

Table 3. Attacks in SDN.

Types of Attacks	Possible Mitigations
DoS and DDoS	Rule implementation
	Machine Learning
	Packet Classification
Zero Day Attacks	Firewall and IDS
	Updating SDN
	Apply Rules
Unauthorized Access	Machine Learning
	Firewall and IDS
	Cryptography
ARP Spoofing	IDS
	Machine Learning
	Static ARP Mappings
Side Channel	Machine Learning
	IDS
	Package Checking
Eavesdropping	Machine Learning
	Deep Learning
	Statistical Error Computation
Botnet	Cryptography
	Machine Learning
	IDS
	Packet Analysis
	Cryptography

nels. OpenFlow channels are used to transmit controller commands or requests. Through this channel, statistics and status of network equipment are transmitted. Much of SDN’s security relies on correctly configuring OpenFlow. If the configuration is not correct, various types of attacks can be launched against the SDN controller, such as DoS, DDoS, Repudiation, Data Modification and Man-in-the-Middle [Mohan *et al.*, 2022].

To prevent DoS or DDoS some SDN-based techniques can be used. Most of them are implemented using the OpenFlow protocol, which include port blocking, network reconfiguration, packet dropping, among others. Some of these techniques are described below [Munmun and Paul, 2021]:

- **Port Block:** This method is used to block the source port of malicious traffic, preventing the source of the DDoS attack from communicating with hosts in the future. By using this technique, legitimate traffic can also be blocked.
- **Redirection:** This technique can be used to redirect legitimate traffic to a new IP address. At the beginning of redirection, all connections are leveled and checked to prevent direct access from bots.
- **Change IP address:** When the attack is detected, the IP of the target or victim machine is changed. When this oc-

Table 4. Some studies of SDN in 5G and IoT networks

Authors	Title	Publication	Data Base
[Sinha <i>et al.</i> , 2023]	DDoS Vulnerabilities Analysis in SDN Controllers: Understanding the Attacking Strategies	2023 International Conference on Wireless Communications Signal Processing and Networking (WiSP-NET)	IEEE Xplore
[Dake <i>et al.</i> , 2021]	DDoS and Flash Event Detection in Higher Bandwidth SDN-IoT using Multiagent Reinforcement Learning	2021 International Conference on Computing, Computational Modelling and Applications (ICCMA)	IEEE Xplore
[Ampririt <i>et al.</i> , 2023]	An intelligent fuzzy-based system for handover decision in 5G-IoT networks considering network slicing and SDN technologies	Internet of Things vol.23	Science Direct
[Javanmardi <i>et al.</i> , 2023]	An SDN perspective IoT-Fog security: A survey	Computer Networks	Science Direct
[Cabaj <i>et al.</i> , 2018]	SDN-based Mitigation of Scanning Attacks for the 5G Internet of Radio Light System	ARES '18: Proceedings of the 13th International Conference on Availability, Reliability and Security	ACM Digital Library
[Alshamrani <i>et al.</i> , 2017]	A Defense System for Defeating DDoS Attacks in SDN based Networks	15th ACM International Symposium on Mobility Management and Wireless	ACM Digital Library

curs, authentic traffic can communicate, and malicious traffic is blocked or dropped.

- **Deep Packet Inspection (DPI):** It is a technique that allows to examine the contents of the packet, including the data part and the packet header. DPI checks the origin of the packet and whether the origin is malicious or not. This technique allows deciding whether a packet will be redirected to another destination or discarded.

Many other types of attacks can occur in networks that use SDN. The **Table 3** presents a classification of some possible attacks.

A so-called “Bot Master” attempts to gain unauthorized access to a device in the network and deploys malware that is spread to take control of other devices. Flaws in the SDN controller could allow the attacker to use malicious code to gain access to network devices and create their bots. Deep learning and Machine Learning techniques can be used in conjunction with SDN to analyze traffic to detect potential inconsistencies and detect abnormal traffic. In this case, researchers execute Machine Learning and Deep Learning training using traffic generated on the network so that the characteristics of the attack can be collected [Nadeem *et al.*, 2023].

Another type of attack that can be executed in SDN networks is ARP Spoofing. As they are networks controlled by exclusive authority or SDN, they exclude a high level of security for their central driver. Attackers can intercept communication between devices using ARP Spoofing and execute passive or active Man-in-the-Middle attacks. One way to check for attackers in the network using this attack is to check the transmitted ARP messages and analyze inconsistencies that may occur after injecting ARP transfers. Algorithms or Machine Learning techniques can be used to ver-

ify, detect, block, and classify this attack [Saritakumar *et al.*, 2023].

The attacks and techniques used by the scientific community are examples of exercises for building security in networks that use the SDN technique. SDN, being programmable, can bring several benefits such as the configuration and control of various devices in the network, from traffic management to blocking and classifying data anomalies, as well as configuration vulnerabilities that can be exploited by cyber-attacks. Faced with concerns about possible attacks, the scientific community is striving to build new techniques, methods, frameworks, and theories for solving problems in SDN networks. The **Table 4** presents some SDN studies in 5G and IoT networks.

5.3 NFV Attacks

NFV has been used to the development of network orchestration and management in terms of improving these functionalities. However, when it comes to working in the security field, little is explored. For example, NFV can be affected by threats to generic virtualization and networking, just as it can be affected by threats specific to the use of NFV. That is, as a VNF is just a network function running on a virtual machine, the set of all threats that can be characterized comprises [Reynaud *et al.*, 2016]:

1. Data link and physical layer threats before virtualization.
2. All generic virtualization threats.
3. New types of attacks that use a technology and virtualization networking combination.

Because it is a software integrated feature, NFV is suscep-

Table 5. Attacks in NFV.

Types of Attacks	Possible Mitigations
Flood Attacks	Firewall
	Machine Learning
	Trust-based Method Congestion Balancing
Routing	Machine Learning
	Routing Algorithm
	Congestion Balancing Smart Routing IDS
Hypervisors	Machine Learning Algorithms
	Encrypting VNF
	Hypervisor Introspection Remote Attestation
Improper Access Attacks	Rule implementation
	Machine Learning
	Packet Classification IDS
Malware	Malicious Traffic Detection
	Machine Learning
	Deep Learning Packet Analysis Classification Algorithms VNF isolation

tible to program related security issues. A virtualized and incorrectly programmed network function allows serious problems to happen. For example, a cybercriminal can invade a virtualized instance and modify the entire flow of data, compromising the availability of a service. **Table 5** presents the classification of some possible attacks that can occur in NFV. The attacks presented are, in many cases, generic attacks that can happen in any type of network, equipment, virtualization of hypervisors, among other functionalities.

NFV can be used to configure methods and techniques so that they can be used to mitigate different types of attacks. One example is the use of NFV to defend against potential DDoS attacks that may occur in the SDN control plane. The work developed by Chen *et al.* [2021] presents a three-stage security scheme for overload control. In the first step, legitimate flows are identified, in the second step the TCP handshake is verified and in the third step the flows eliminated in the first two steps are classified to identify possible attacks.

Another example of the use of NFV is the development of security techniques against Botnet attacks. Some research that aims to detect, block, and mitigate this type of attack proposes intrusion detection techniques to analyze network traffic and implement these virtualized devices in security applications in SDN controller. These solutions assume that all network traffic must first be transferred to the SDN controller. This creates a bottleneck that makes it difficult to correctly detect potential botnet attacks. The overhead generated by this bottleneck can be exploited by bots [Park *et al.*, 2018]. In this sense, developing studies that aim to identify botnet

attacks and that use NFV are good options for developing techniques, algorithms, use of AI, among others.

NFV techniques allow many network functions to be configured, and through an orchestrator these virtualized functions are managed. With the help of other techniques, such as SDN, it is possible to configure and virtualize security functions in the network. This is an area that has great potential for new studies and research. **Table 6** presents some studies that are involved with the use of NFV in the information security area.

In this sense, the protection of information and the strengthening of security in these functionalities should be better explored by security researchers or designers.

6 Conclusion

5G technologies offer new business opportunities and a more connected user to a high speed and quality network. Adding IoT devices to this network opens new possibilities and demonstrates what can be called the Internet of the future. Users can take control of all the information they need from a variety of devices, such as smart watches, smart cars and more, enabling new experiences for increasingly connected people.

Allowing the network to be configured and adapted, according to the user's reality, enables a management model capable of using SDN and NFV techniques to facilitate the configuration of the network through software. These features allow users to have better control of information transferred over the network. However, the lack of unreliable configurations and protocols can lead to security risks in IoT and 5G networks.

Knowing the anatomy of an attack in these networks is essential if potential security events are to be avoided and mitigated. Many attacks, such as DoS and Man-in-the-Middle, aim to damage data or services the network. Thus, techniques capable of managing and mitigating possible threats must be developed.

In the case of the 5G network, because it is a new transmission technology, many attacks can happen in the sense of exploiting protocol vulnerabilities, attacks on the physical layer and on the link layer, and even cybercriminals can execute Zero Day attacks, which are difficult to identify at first. As it is a network in which the use of IoT technologies will be widely used, the flow of data will be greater and with that the guarantee of information protection must be implemented from end to end. AI techniques can be used and programmed at the SDN and NFV level for pattern recognition and attack classification, both at the protocol level and at the TCP/IP data link and physical layers. Therefore, studies must be carried out in this area for the development of new techniques and programming of SDN and NFV that use AI, thus allowing new possibilities to mitigate and prevent attacks against 5G network.

Many works in 5G and IoT network security are developed using SDN and NFV techniques, but the studies are still directed to the network and application layers in the TCP/IP model. However, testing at the physical layer and link layer must be performed so that vulnerable protocols or possible

Table 6. Some studies of NFV in 5G and IoT networks

Authors	Title	Publication	Data Base
[Abdulqadder <i>et al.</i> , 2020a]	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)	IEEE Xplore
[Lioy <i>et al.</i> , 2017]	NFV-based network protection: The SHIELD approach	2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)	IEEE Xplore
[Hakiri and Dezfouli, 2021]	Towards a Blockchain-SDN Architecture for Secure and Trustworthy 5G Massive IoT Networks	Association for Computing Machinery	ACM Digital Library
[Wendland and Banse, 2018]	Enhancing NFV Orchestration with Security Policies	Proceedings of the 13th International Conference on Availability, Reliability and Security	ACM Digital Library
[Yungaicela-Naula <i>et al.</i> , 2023]	SDN/NFV-based framework for autonomous defense against slow-rate DDoS attacks by using reinforcement learning	Future Generation Computer Systems	Science Direct
[Madi <i>et al.</i> , 2021]	NFV security survey in 5G networks: A three-dimensional threat taxonomy	Computer Networks	Science Direct

security breaches are found and fixed, so that they are not exploited by cybercriminals. Therefore, more work must be carried out to verify and create techniques capable of correcting and mitigating vulnerabilities in the physical layer of 5G. Once this layer is damaged, information security is compromised in the upper layers.

Declarations

Acknowledgements

This work is supported by the *Coordenação de Aperfeiçoamento de Pessoal de Nível Superior* (CAPES) (88887.941768/2024-00).

Authors' Contributions

Competing interests

The authors declare that they have no competing interests

Availability of data and materials

Data can be made available upon request

References

- 3GPP (2019). 3rd generation partnership project; technical specification group services and system aspects; release 15 description; summary of rel-15 work items (release 15). *3GPP Release 15*, pages 1–118. Available at:
- Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F., Shah, G. A., and Zafar, K. (2020). Iot-sphere: A framework to secure iot devices from becoming attack target and attack source. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1402–1409. DOI: 10.1109/TrustCom50675.2020.00189.
- Abdulkarem, H. S. and Dawod, A. (2020). Ddos attack detection and mitigation at sdn data plane layer. In *2020 2nd Global Power, Energy and Communication Conference (GPECOM)*, pages 322–326. DOI: 10.1109/GPECOM49333.2020.9247850.
- Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., and Akber, S. M. A. (2020a). Bloc-sec: Blockchain-based lightweight security architecture for 5g/b5g enabled sdn/nfv cloud of iot. In *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, pages 499–507. DOI: 10.1109/ICCT50939.2020.9295823.
- Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., and Akber, S. M. A. (2020b). Multi-layered intrusion detection and prevention in the sdn/nfv enabled cloud of 5g networks using ai-based defense mechanisms. *Computer Networks*, 179:107364. DOI: 10.1016/j.comnet.2020.107364.
- Akpakwu, G. A., Silva, B. J., Hancke, G. P., and Abu-Mahfouz, A. M. (2018). A survey on 5g networks for the internet of things: Communication technologies and challenges. *IEEE Access*, 6:3619–3647. DOI: 10.1109/ACCESS.2017.2779844.
- Alshamrani, A., Chowdhary, A., Pisharody, S., Lu, D., and Huang, D. (2017). A defense system for defeating ddoS attacks in sdn based networks. In *Proceedings of the 15th*

- ACM International Symposium on Mobility Management and Wireless Access*, MobiWac '17, page 83–92, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3132062.3132074.
- Ampririt, P., Higashi, S., Qafzezi, E., Ikeda, M., Matsuo, K., and Barolli, L. (2023). An intelligent fuzzy-based system for handover decision in 5g-iot networks considering network slicing and sdn technologies. *Internet of Things*, 23:100870. DOI: 10.1016/j.iot.2023.100870.
- Asif, S. (2019). *5G Mobile Communications Concepts and Technologies*, volume 1. CRC Press. Book.
- Barona López, L. I., Valdivieso Caraguay, Á., Maestre Vidal, J., Sotelo Monge, M., and García Villalba, L. J. (2017). Towards incidence management in 5g based on situational awareness. *Future Internet*, 9(1):3. DOI: 10.3390/fi9010003.
- Bifulco, R., Matusiuk, A., and Silvestro, A. (2016). Ready-to-deploy service function chaining for mobile networks. In *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, pages 175–183. DOI: 10.1109/NETSOFT.2016.7502411.
- 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. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES '18, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3230833.3233248.
- Carrozzo, G., Siddiqui, M. S., Betzler, A., Bonnet, J., Perez, G. M., Ramos, A., and Subramanya, T. (2020). Ai-driven zero-touch operations, security and trust in multi-operator 5g networks: a conceptual architecture. In *2020 European Conference on Networks and Communications (EuCNC)*, pages 254–258. DOI: 10.1109/Eu-CNC48522.2020.9200928.
- Chahlaoui, F., El-Fenni, M. R., and Dahmouni, H. (2019). Performance analysis of load balancing mechanisms in sdn networks. In *Proceedings of the 2nd International Conference on Networking, Information Systems & Security*, NISS19, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3320326.3320368.
- Chen, K.-Y., Liu, S., Xu, Y., Siddhau, I. K., Zhou, S., Guo, Z., and Chao, H. J. (2021). Sdnshield: Nfv-based defense framework against ddos attacks on sdn control plane. *IEEE/ACM Trans. Netw.*, 30(1):1–17. DOI: 10.1109/TNET.2021.3105187.
- Costa-Requena, J., Guasch, V. F., and Santos, J. L. (2015). Software defined networks based 5g backhaul architecture. IMCOM '15, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/2701126.2701180.
- Coelho, R. W., Leonardo, E. J., Martimiano, L. A. F., and Silva, R. A. (2023). A survey of the characteristics of sdn, nfv and information security in iot and 5g networks. *Revista Brasileira de Computação Aplicada*, 15(3):96–105. DOI: 10.5335/rbca.v15i3.14645.
- Coelho, R. W., Leonardo, E. J. a., Martimiano, L. A. F., and Silva, R. A. a. (2022). Segurança da informação nas camadas física e de enlace em redes 5g e iot: Uma revisão sistemática. DOI: 10.14209/sbrt.2022.1570822822.
- Dake, D. K., Gadze, J. D., and Klogo, G. S. (2021). Ddos and flash event detection in higher bandwidth sdn-iot using multiagent reinforcement learning. In *2021 International Conference on Computing, Computational Modelling and Applications (ICCA)*, pages 16–20. DOI: 10.1109/IC-CMA53594.2021.00011.
- Das, D., Banerjee, S., Dasgupta, K., Chatterjee, P., Ghosh, U., and Biswas, U. (2023). Blockchain enabled sdn framework for security management in 5g applications. In *Proceedings of the 24th International Conference on Distributed Computing and Networking*, ICDCN '23, page 414–419, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3571306.3571445.
- Dutta, A. and Hammad, E. (2020). 5g security challenges and opportunities: A system approach. In *2020 IEEE 3rd 5G World Forum (5GWF)*, pages 109–114. DOI: 10.1109/5GWF49715.2020.9221122.
- Fang, D., Qian, Y., and Hu, R. Q. (2018). Security for 5g mobile wireless networks. *IEEE Access*, 6:4850–4874. DOI: 10.1109/ACCESS.2017.2779146.
- Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., and Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, 101(August 2017):55–82. DOI: 10.1016/j.jnca.2017.10.017.
- 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. DOI: 10.1109/ACCESS.2019.2939938.
- Gupta, A. and Jha, R. K. (2015). A survey of 5g network: Architecture and emerging technologies. *IEEE Access*, 3:1206–1232. DOI: 10.1109/ACCESS.2015.2461602.
- Hakiri, A. and Dezfouli, B. (2021). Towards a blockchain-sdn architecture for secure and trustworthy 5g massive iot networks. In *Proceedings of the 2021 ACM International Workshop on Software Defined Networks & Network Function Virtualization Security*, SDN-NFV Sec'21, page 11–18, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3445968.3452090.
- Jaiswal, A., Kumar, S., Kaiwartya, O., Kumar, N., Song, H., and Lloret, J. (2021). Secrecy Rate Maximization in Virtual-MIMO Enabled SWIPT for 5G Centric IoT Applications. *IEEE Systems Journal*, 15(2):2810–2821. DOI: 10.1109/JSYST.2020.3036417.
- Javanmardi, S., Shojafar, M., Mohammadi, R., Alazab, M., and Caruso, A. M. (2023). An sdn perspective iot-fog security: A survey. *Computer Networks*, 229:109732. DOI: 10.1016/j.comnet.2023.109732.
- Javed, M. A. and Khan Niazi, S. (2019). 5g security artifacts (dos / ddos and authentication). In *2019 International Conference on Communication Technologies (ComTech)*, pages 127–133. DOI: 10.1109/COMTECH.2019.8737800.
- Kabir, H., Bin Mohsin, M. H., and Kantola, R. (2020). Implementing a security policy management for 5g customer edge nodes. In *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, pages 1–8. DOI: 10.1109/NOMS47738.2020.9110321.
- Kaur, K. and Ayoade, J. (2023). Analysis of ddos at-

- tacks on iot architecture. In *2023 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, pages 332–337. DOI: 10.1109/EECSI59885.2023.10295766.
- 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 and Tutorials*, 22(1):196–248. DOI: 10.1109/COMST.2019.2933899.
- Li, M., Zhou, H., and Qin, Y. (2023). Qlsfc: An intelligent security function chain with q-learning in sdn/nfv network. In *Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering, ICECC '23*, page 125–131, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3592307.3592327.
- Li, W., Wang, N., Jiao, L., and Zeng, K. (2021). Physical layer spoofing attack detection in mmwave massive mimo 5g networks. *IEEE Access*, 9:60419–60432. DOI: 10.1109/ACCESS.2021.3073115.
- Liang, X. and Qiu, X. (2016). A software defined security architecture for sdn-based 5g network. In *2016 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC)*, pages 17–21. DOI: 10.1109/IC-NIDC.2016.7974528.
- Lioy, A., Gardikis, G., Gaston, B., Jacquin, L., De Benedictis, M., Angelopoulos, Y., and Xylouris, C. (2017). Nfv-based network protection: The shield approach. In *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 1–2. DOI: 10.1109/NFV-SDN.2017.8169869.
- Liu, C., Raghuramu, A., Chuah, C.-N., and Krishnamurthy, B. (2017). Piggybacking network functions on sdn reactive routing: A feasibility study. In *Proceedings of the Symposium on SDN Research, SOSR '17*, page 34–40, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3050220.3050225.
- Liyanage, M., Ahmad, I., and Abro, A. B. (2018). *A Comprehensive Guide to 5G Security*, volume 1. Wiley. Book.
- Madi, T., Alameddine, H. A., Pourzandi, M., and Boukhtouta, A. (2021). Nfv security survey in 5g networks: A three-dimensional threat taxonomy. *Computer Networks*, 197:108288. DOI: 10.1016/j.comnet.2021.108288.
- Mathew, A. (2020). Network slicing in 5g and the security concerns. In *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, pages 75–78. DOI: 10.1109/ICCMC48092.2020.ICCMC-00014.
- Medhat, A. M., Taleb, T., Elmangoush, A., Carella, G. A., Covaci, S., and Magedanz, T. (2017). Service function chaining in next generation networks: State of the art and research challenges. *IEEE Communications Magazine*, 55(2):216–223. DOI: 10.1109/MCOM.2016.1600219RP.
- Meng, Y., Naeem, M. A., Almagrabi, A. O., Ali, R., and Kim, H. S. (2020). Advancing the state of the fog computing to enable 5g network technologies. *Sensors*, 20(6). DOI: 10.3390/s20061754.
- Mir, A., Zuhairi, M. F., Musa, S., Syed, T. A., and Al-rehaili, A. (2020). Poster: A survey of security challenges with 5g-iot. In *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, pages 249–250. DOI: 10.1109/SMARTTECH49988.2020.00063.
- Mohan, K. V. M., Kodati, S., and Krishna, V. (2022). Securing sdn enabled iot scenario infrastructure of fog networks from attacks. In *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, pages 1239–1243. DOI: 10.1109/ICAIS53314.2022.9742727.
- Munmun, F. A. and Paul, M. (2021). Challenges of ddos attack mitigation in iot devices by software defined networking (sdn). In *2021 International Conference on Science & Contemporary Technologies (ICSCT)*, pages 1–5. DOI: 10.1109/ICSCT53883.2021.9642640.
- Nadeem, M. W., Goh, H. G., Aun, Y., and Ponnusamy, V. (2023). Detecting and mitigating botnet attacks in software-defined networks using deep learning techniques. *IEEE Access*, 11:49153–49171. DOI: 10.1109/ACCESS.2023.3277397.
- Nam, T. L., Mohammad, A. H., Amirul, I., Do-yun, K., Young-June, C., and Yeong, M. J. (2016). Survey of promising technologies for 5g networks. *Mobile Information Systems*, 2016:1–25. DOI: 10.1155/2016/2676589.
- Nguyen, V.-G., Brunstrom, A., Grinnemo, K.-J., and Taheri, J. (2017). Sdn/nfv-based mobile packet core network architectures: A survey. *IEEE Communications Surveys & Tutorials*, 19(3):1567–1602. DOI: 10.1109/COMST.2017.2690823.
- Olazabal, A. A., Kaur, J., and Yeboah-Ofori, A. (2022). Deploying man-in-the-middle attack on iot devices connected to long range wide area networks (lorawan). In *2022 IEEE International Smart Cities Conference (ISC2)*, pages 1–7. DOI: 10.1109/ISC255366.2022.9922377.
- Pan, F., Jiang, Y., Wen, H., Liao, R., and Xu, A. (2017). Physical Layer Security Assisted 5G Network Security. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pages 1–5, Toronto, ON. IEEE. DOI: 10.1109/VTC-Fall.2017.8288343.
- Park, Y., Kengalahalli, N. V., and Chang, S.-Y. (2018). Distributed security network functions against botnet attacks in software-defined networks. In *2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 1–7. DOI: 10.1109/NFV-SDN.2018.8725657.
- Petrović, R., Simić, D., Stanković, S., and Perić, M. (2021). Man-in-the-middle attack based on arp spoofing in iot educational platform. In *2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*, pages 307–310. DOI: 10.1109/TELSIKS52058.2021.9606392.
- Rahimi, H., Zibaenejad, A., Rajabzadeh, P., and Safavi, A. A. (2018). On the security of the 5G-IoT architecture. *ACM International Conference Proceeding Series*, pages 1–8. DOI: 10.1145/3269961.3269968.
- Ravi, N., Rani, P. V., and Shalinie, S. M. (2019). Secure deep neural (seden) framework for 5g wireless networks. In *2019 10th International Conference on Computing,*

- Communication and Networking Technologies (ICCCNT)*, pages 1–6. DOI: 10.1109/ICCCNT45670.2019.8944654.
- Reynaud, F., Aguessy, F.-X., Bettan, O., Bouet, M., and Conan, V. (2016). Attacks against network functions virtualization and software-defined networking: State-of-the-art. In *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, pages 471–476. DOI: 10.1109/NETSOFT.2016.7502487.
- Rohatgi, V. and Goyal, S. (2020). A detailed survey for detection and mitigation techniques against arp spoofing. In *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pages 352–356. DOI: 10.1109/I-SMAC49090.2020.9243604.
- 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. DOI: 10.1109/ACCESS.2020.3046325.
- Saritakumar, N., Anusuya, V. K., and Krishnakumar, S. (2023). Detection of arp spoofing attacks in software defined networks. In *2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)*, pages 422–426. DOI: 10.1109/ICISCoIS56541.2023.10100567.
- Sharma, A. and Babbar, H. (2023). Bot-iot: Detection of ddos attacks in internet of things for smart cities. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 438–443. Available at: <https://ieeexplore.ieee.org/abstract/document/10112310>.
- 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. DOI: 10.1109/ACCESS.2019.2943929.
- Sicari, S., Rizzardi, A., and Coen-Porisini, A. (2020). 5G In the internet of things era: An overview on security and privacy challenges. *Computer Networks*, 179:107345. DOI: 10.1016/j.comnet.2020.107345.
- Singh, P., Pawar, P., and Trivedi, A. (2018). Physical Layer Security Approaches in 5G Wireless Communication Networks. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pages 477–482, Jalandhar, India. IEEE. DOI: 10.1109/ICSCCC.2018.8703344.
- Sinha, M., Bera, P., and Satpathy, M. (2023). Ddos vulnerabilities analysis in sdn controllers: Understanding the attacking strategies. In *2023 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, pages 1–5. DOI: 10.1109/WiSPNET57748.2023.10134518.
- Varum, T., Ramos, A., and Matos, J. N. (2018). Planar microstrip series-fed array for 5g applications with beamforming capabilities. In *2018 IEEE MTT-S International Microwave Workshop Series on 5G Hardware and System Technologies (IMWS-5G)*, pages 1–3. DOI: 10.1109/IMWS-5G.2018.8484697.
- Wendland, F. and Banse, C. (2018). Enhancing nfv orchestration with security policies. In *Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES '18*, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3230833.3233253.
- Yerrapragada, A. K., Eisman, T., and Kelley, B. (2021). Physical Layer Security for Beyond 5G: Ultra Secure Low Latency Communications. *IEEE Open Journal of the Communications Society*, 2(August):1–1. DOI: 10.1109/ojcoms.2021.3105185.
- Yi, B., Wang, X., Li, K., Das, S., and Huang, M. (2018). A comprehensive survey of network function virtualization. *Computer Networks*, 133:212–262. DOI: 10.1016/j.comnet.2018.01.021.
- Yungaicela-Naula, N. M., Vargas-Rosales, C., and Pérez-Díaz, J. A. (2023). Sdn/nfv-based framework for autonomous defense against slow-rate ddos attacks by using reinforcement learning. *Future Generation Computer Systems*, 149:637–649. DOI: 10.1016/j.future.2023.08.007.
- Zhao, H., Xu, M., Zhong, Z., and Wang, D. (2021). A fast physical layer security-based location privacy parameter recommendation algorithm in 5g iot. *China Communications*, 18(8):75–84. DOI: 10.23919/JCC.2021.08.006.