Revista Brasileira de Computação Aplicada, November, 2023

DOI: 10.5335/rbca.v15i3.14645
Vol. 15, Nº 3, pp. 96–105
Homepage: seer.upf.br/index.php/rbca/index

ORIGINAL PAPER

A survey of the characteristics of SDN, NFV and information security in IoT and 5G networks

Roger William Coêlho [1], Elvio João Leonardo [1], Luciana Andréia Fondazzi Martimiano [1], Ronan Assumpção Silva [2]

[1]State University of Maringá (UEM), [2]Federal Institute of Paraná (IFPR)

*roger.coelho04@gmail.com; ejleonardo@uem.br; lafmartimiano@uem.br; ronan.silva@ifpr.edu.br

Received: 2023-04-06. **Revised:** 2023-11-01. **Accepted:** 2023-11-20.

Abstract

The 5G technology has emerged as a trusted source to meet the increased demand of Internet of Things (IoT) devices, in addition to enabling Internet connectivity at high broadband speeds. Another important feature of 5G is the use of techniques such as Software Defined Networking (SDN) and Network Functions Virtualization (NVF), mechanisms responsible for performing network configurations through software, in addition to massive control and management of devices using the network configuration 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, thus 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 techniques to allow the configuration of the functionality and management of the network by software. In addition, concerns will be reported about possible information security attacks that may occur in 5G.

Keywords: Information Security; Internet of Things (IoT); Network Function Virtualization (NFV); Software Defined Network (SDN); 5G network.

Resumo

A tecnologia 5G surgiu para atender à crescente demanda por dispositivos de Internet das Coisas (IoT), além de permitir conectividade à Internet em altas velocidades de banda larga. Outra característica importante do 5G é a utilização de técnicas como Rede Definida por Software (SDN) e Virtualização de Função de Rede (NFV), mecanismos responsáveis por realizarem configurações de rede por meio de software, controle e gerenciamento de dispositivos utilizando as funções de configuração de rede ou virtualização de dispositivos. A preocupação com a segurança da informação na rede 5G é cada vez maior, à medida que os cibercriminosos tentam acessar dados importantes que são transmitidos pela rede, já que a demanda por dispositivos IoT conectados será maior, permitindo assim diversas possibilidades de ataques. A compreensão de possíveis ameaças e ataques é necessária, para que novas medidas sejam tomadas contra os cibercriminosos nas redes 5G e IoT. Este artigo tem como objetivo elucidar algumas concepções do que é a tecnologia 5G e o uso da IoT, contextualizando as técnicas SDN e NFV para permitir configurações de funcionalidades e gerenciamento da rede por software. Além disso, serão relatadas preocupações sobre possíveis ataques à segurança da informação que podem ocorrer no 5G.

Palavras-Chave: Internet das Coisas (IoT); Rede Definida por Software (SDN); Rede 5G; Segurança da Informação; Virtualização de Função de Rede (NFV).

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 quick access to information (Varum et al., 2018). Having an infrastructure capable of transmitting data at high speed is the best way to promote the evolution of existing applications and new types of activities.

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 demand 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 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 feature rich system, which allows the use of SDN and NFV for network configuration that allows for better quality of service and security. It is possible to use 5G, for instance, in remote health monitoring equipment, in Industry 4.0, in the agricultural sector and in the Internet of Things (IoT), 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 Internet of Things (IoT) is an 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 in IoT networks to protect the data that is transmitted over the 5G network.

When we think about information security, some questions arise such as: what is the adequate protection of the network?; when do we apply network configuration techniques through software?; and how to deal with this challenge, especially when different devices are connected? Answering these questions allows the security project to meet the requirements of the strategic plan that was developed. With an inappropriate 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 network security on 5G technology and connected IoT devices.

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

The remaining of the paper is organized as follows: Section 2 discusses 5G technology, the use of SDN and NFV to enable the software configurations implementation in the network; Section 3 covers IoT networks and their connections to the 5G network; in Section 4, the types of attacks against 5G and IoT are presented and some works related to implementing information security in these networks are discussed; Section 5 presents the conclusion.

2 5G Technology

2.1 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 (Le 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, Software Defined Networking (SDN), Network Function Virtualization (NFV), spectrum division network and the new concept of cutting edge computing (Liyanage 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 (Meng et al., 2020). In this way, the 5G technology features that contribute to the network services improvement can be classified in stages as:

- Enhanced Mobile Broadband (eMBB).
- Ultra-reliable low-latency communications (URLLC) or ultra-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 demand. Also, interconnected small-cell networks provide a dense data transmission network for 5G. The purpose of this feature is for greater

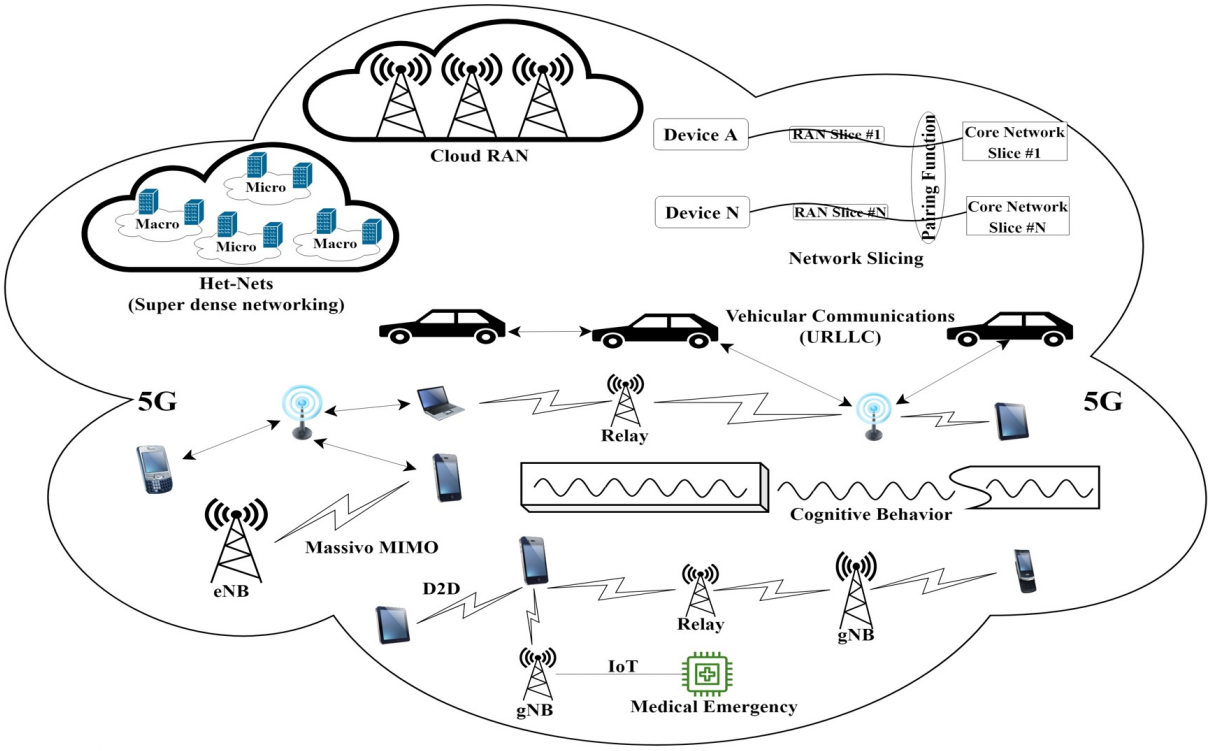

Figure 1: 5G network architecture

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 their 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). Fig. 1 shows the 5G network architecture and their geographic distribution of antennas and devices connected to the network presented by Asif (2019).

As can be seen in Fig. 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 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.

2.2 Software Defined Network (SDN)

A fundamental tool for the development of networks with 5G technology is the use of the Software Defined Network (SDN) paradigm. 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.

SDN is the future of 5G technology in mobile phone network evolution. 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, in addition to improving security. 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) in order 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 done, such as optimizing the power resources of connected devices as well as data resources consumed by users in the network.

With regard to network security, the SDN system can promote better resource management, allowing for the risk management of some types of attack that can be exploited by a threat agent that aims to carry out a certain intrusion in the system. Intrusion Detection Systems (IDS), using the SDN technique, is capable of verifying possible anomalies in the network and predicting or blocking attacks. Another example of using this technique 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).

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 programmed network can meet the needs of any user, enabling new possibilities for applications and businesses. However, new challenges arise, especially in security. As a consequence, 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.

2.3 Network Function Virtualization (NFV)

Network Function Virtualization (NFV) is another paradigm of 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. It is also allowed 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):

i. ***Physical Network Function (PNF):*** This technique aims to design a block with a specialized function and well-defined behavior, characterized by a network node or physical device.
ii. ***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.
iii. ***Element Management System (EMS):*** This system is responsible for managing the instances of Virtual Network Functions (VNFs).
iv. ***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 VNF Manager (VNFM) and the NFV Orchestrator (NFVO), responsible for managing NFVI, among other features.
v. ***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.
vi. ***Network Point of Presence (N-PoP):*** It is responsible for indicating the location of the network where the PNF and VNF will be implemented.

Fig. 2 is an NFV structure in Li and Chen (2015). It is noteworthy that such architecture contributes to the network functions implementation.

As can be seen in Fig. 2, the structure of the NFV architecture allows network functions to be implemented and executed, even allowing the virtualization of some network functions that can be designed via software. The implementation and execution are guided by a management system through metadata that describes 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 to control and manage the network at any location remotely and automatically (Li and Chen, 2015).

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

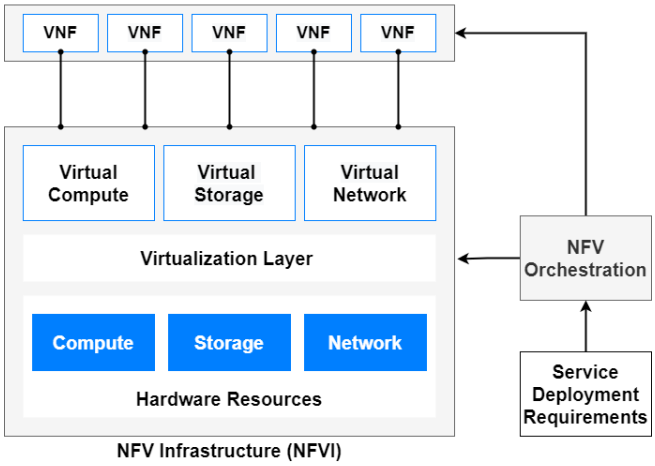

Figure 2: NFV Infrastructure

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 Internet of Things (IoT)

The IoT is expected to enable an environment capable of impacting and influencing the lives of the population, providing new business possibilities and application implementations in various areas such as agriculture and industry 4.0. With the network's modernization, new application possibilities emerged to connect different types of devices to the network, with high data transmission and reception speed, allowing users to access information from these devices at any time and remotely (Akpakwu et al., 2018).

With the connection of several devices in the network and the growing concern with information security, a broad discussion is necessary for the development of new methods that mitigated possible threats to the network. This concern arises, since the devices offer low processing capacity and energy, allowing technical deficiencies to be exploited to carry out attacks. Providing a secure network is essential for the successful deployment of IoT devices connected to the 5G network. New transmission technology must ensure that IoT devices can transmit information securely and at high speed. To do this, 5G radio operators need to incorporate powerful and robust security standards.

3.1 Information Security Challenges for IoT Networks

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). One problem with this approach is that it requires less authentication. This fact is crucial because the data generated from the edge is critical and confidential.

Many challenges still exist in relation to 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 link layer in IoT and 5G networks should be better studied in terms of possible risks to information security, since, if this layer is attacked, all other layers can be compromised.

4 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 for information is essential, not least because a lot of valuable data travel over the network, and if this information falls into the wrong hands, the damage to the user or service provider can be great, not only in the financial area, but also in the reputation of these individuals or business conglomerates.

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. In addition to these two, other techniques such as Mobile Edge Cloud (MEC)

and Network Slicing (NS) allow the sharing of resources and low latency applications. However, these features can lead to additional security risks (Dutta and Hammad, 2020).

Additional algorithms, such as those used in 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. Much concern about 5G security threats will come from the greater availability of data in the network, which means that more bandwidth means more transmitted data that can be attacked by malicious agents. 5G wireless channels can provide easy accessibility to exploit the attacks that cause network interference, such as denial of service (DoS) and distributed denial of service (DDoS), and there are still no concrete solutions to prevent these types of attacks, like other attacks that can be classified as zero-day (Javed and khan Niazi, 2019).

Security features in the 5G network will contribute to significantly increase the adoption of connected IoT devices. When running the network slicing, specific authentications are required; in addition to primary authentication, users using slice gain greater access control and isolation between network segments, which helps prevent cybercriminals from authenticating themselves on 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 (Ghosh et al., 2019).

Faced with a complex scenario of IoT and 5G networks, new measures are taken to enable the implementation of a secure environment. In (Ghosh et al., 2019), some of the key security features of 3GPP Version 15 are specified as:

- Unified authentication framework and access-agnostic authentication.
- Primary and secondary authentication in public and non-public networks.
- Increased Heme Control (IHC), for authentication and steering of roaming.
- Enhanced subscriber privacy.
- Enhance Security for Radio Resource Control (RRC) and Non-Access Stratum (NAS) signaling.
- Support for user plane integrity protection.
- Secure service-based architecture and inter-Public Land Mobile Network (PLMN) interconnection.
- Security for interworking between the 5G and the Envolved Packet System (EPS) of 4G.

Understanding the anatomy of an attack is essential for data security in any transmission technology. Many attacks aim to affect the network layer or the application layer of the TCP/IP model. However, many data link layer attacks can be exploited, especially when a new transmission technology is introduced. Understanding how the frame link is assembled in the 5G network is important to predict and prevent possible attacks that might occur at this layer.

Once the link layer is compromised, all others above can consequently be compromised as well. It is a fact that many attacks occur at the network and application layers, but neglecting potential attacks at the 5G data link layer can open up multiple ramifications for threat actors to execute new types of attacks that affect the entire system. The integrity of the system and the data that travels in the network must be protected at all of stages of transmission, and for this, using NFV and SDN with pattern recognition techniques can provide greater security effectiveness in the system as a whole.

4.1 Types of attacks against the 5G and IoT network

Attacks against information security happen daily on every type of projected network. A major challenge is identifying these attacks, especially zero-day ones, which are actions that have never been taken or identified at any given 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 carry out 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 (Americas, 2019). The 5G network is also a technology that can be exploited because it was recently developed and possible protocol flaws can be identified for attacks to be carried out against data security.

Several threats and attacks are already known and applied in both the 5G network and the IoT network. Below are some types of attacks (Ahmad et al., 2020):

i. ***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.
ii. ***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.
iii. ***Social engineering:*** IoT devices collect a lot of important information from users. The data collected is used to assist users in their needs. Such data may be requested by threat agents who use users' good faith to provide critical personal data. In this way, users send information to threat agents because they believe that the applications are legitimate.
iv. ***Data and Identity:*** With smart devices widely used in the networks, cybercriminals can gain access to personal and confidential information that are important to users. All information can be used to spoof

identity and carry out attacks in a way that the attacker does not appear to be actually presenting himself.

v. ***Man-in-the-Middle atacks:*** In these types of attacks, the threat agent can impersonate a 5G tower or a wireless communication device, interrupting communication and can see, modify and steal the exchanges of information between the devices. Information manipulations can be used to attack other IoT devices or 5G towers as they progressively share information.

vi. ***Denial of Service (DoS) and Distributed Denial of Service (DDoS):*** In these types of attack, a threat agent overloads the device or system with packages and makes the device inaccessible to the user. Since the IoT has multiple devices interconnected over the Internet and constantly receive packets, such an attack will reduce the productivity of an IoT device and can render it unproductive. In an industry 4.0 environment, unavailability of devices can lead to production delays and, as a result, serious financial losses.

vii. ***Ransomware:*** In this attack, the threat agent uses malware to block users' access to devices by encrypting data. The attacker only provides the access key to the encrypted data via a cash ransom performed by the victim.

viii. ***Botnets:*** In this type of attack, the cybercriminal uses a network of compromised systems that can be remotely controlled to carry out mass attacks such as DoS, DDoS and others. By using the 5G network and connected IoT devices, criminals will have a vast arsenal of bots to carry out attacks.

Table 1 is an adaptation of Mir et al. (2020), referring to the classification of possible attacks that can occur in IoT and 5G networks.

The protection of information on 5G networks is essential, as the massive use of IoT devices will lead to a greater amount of information transmitted over the network, which can lead to possible attacks, whose information can be acquired by cybercriminals. With the advancement of security techniques and knowledge of possible attacks, the quality of the service provided improves, allowing the user to be sure that their data is safe. Therefore, technological means such as SDN, NFV and artificial intelligence allow the configuration of the network, so that threat patterns are recognized and the network is automated for a more effective management of information security.

Table 1: Types of Attacks in 5G and IoT Networks

Attacks Classification	Types of Attacks
Against Availability	DoS and DDoS Free-Riddling Skimming Redirection
Against Integrity	Spam Cloning Tempering Message Blocking
Against Centralized Policy	Network Manipulation Traffic Diversion DoS and DDoS Traffic Sniffing ARP Spoofing API Exploitation Brute Force Side Channel
Against Privacy	Masquerade Collaborated Man-in-the-Middle Impersonation Spoofing Stalking Tracing
Against Visibility	VM Migration Distributed Control Privacy Issues Orchestration Issues Misconfiguration and Human errors Encryption at Application Level Eavesdropping
Against Authentication	Password Reuse Partial Message Collision Dictionary Leak of Verifier Brute Force Forgery Stolen Smart-Card

4.2 Papers related to security in the 5G and IoT networks

This subsection 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 the 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 ensured 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. All automation of the proposed architecture uses SDN and

NFV techniques to secure data communication.

The work presented in Zhao et al. (2021), presents the proposal of an algorithm that aims to recommend the privacy requirements of a device connected to the 5G and IoT network through Location-Based Services (LBS). This approach identifies trusted terminals for connection to the network as a measure to prevent MITM type attacks. The authors present a cross-authentication protocol, which is based on the use of the algorithm. In this protocol, authentications are performed through the physical layer by specifying authentication keys between devices and terminals in the 5G network.

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.

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

In Djigal et al. (2022) a comprehensive research is presented, through a survey, which shows how the allocation of resources for Multiaccess Edge Computing (MEC) in IoT devices present in 5G network, using machine learning and deep learning techniques. The initial part of the study presents a tutorial that shows the advantages of applying machine learning and deep learning in MEC. As a second stage of the study, an in-depth survey of recent works that used machine learning and deep learning methods for resource allocation in MEC is presented. The authors list three aspects: (1) methods based on machine learning and deep learning for offloading tasks; (2) methods based on machine learning and deep learning for task scheduling, and (3) methods based on machine learning and deep learning for joint resource allocation.

In Kabir et al. (2020), an experimental implementation of a Security Policy Management (SPM) system for 5G networks was proposed, which considers the basic principles for the security of end devices. They also proposed 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 Zhou et al. (2022) is an investigation of the use of blockchain in 5G networks. This technique consists of the services decentralization, with the purpose of guaranteeing the network reliability. The authors also carry out an investigation to support blockchain solutions based in 5G Radio Access Network (RAN) architecture. The authors explain in their study that blockchain is a decentralized and privacy-protected system and that it is a tool capable of storing reliable data that travels in 5G network through the decentralization of information. This type of technology operates at the edge of the network and the advantage presented by the authors is that the storage of information is distributed, with high security and high immutability. Each blockchain block consists of a hash value from the previous block that are connected to create a chain of correlated blocks used to search and add new information blocks. Some applications use the blockchain technique, cited by the authors, are: Vertical Industry and Network Sharing.

As can be seen, there are works that deal with information security in 5G and IoT environments. 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 is poorly researched for security. With the emergence of new transmission technologies, new protocols are formalized and many of them are not adequately concerned with the security of the frame that will carry the information. In this way, cybercriminals can exploit link layer vulnerabilities to compromise all data sent and received over the network, thus affecting the integrity, reliability and availability of information, in relation to this layer and to the higher layers of the TCP/IP model.

5 Conclusion

5G transmission technologies offer new business opportunities and a more connected user to a high-speed and quality network. Adding IoT devices to this network opens up 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.

Many works in the area of 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, extensive testing at the link layer must be performed so that vulnerable protocols or possible 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 link layer of 5G transmission technology. Once this layer is damaged, information security is compromised in the upper layers of the TCP/IP model.

Acknowledgments

This work is supported by the Coordination for the Improvement of Higher Education Personnel (CAPES) (88887.668985/2022-00).

References

Ahmad, A., Bhushan, B., Sharma, N., Kaushik, I. and Arora, S. (2020). Importunity & evolution of iot for 5g, pp. 102–107. https://doi.org/10.1109/CSNT48778.2020.9115768.

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. https://doi.org/10.1109/ACCESS.2017.2779844.

Americas, G. (2019). *The Evolution of Security in 5G: A Slice of Mobile Threats*, Vol. 1, 5G Americas.

Asif, S. (2019). *5G Mobile Communications Concepts and Technologies*, Vol. 1, CRC Press.

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. https://doi.org/10.3390/fi9010003.

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, pp. 254–258. https://doi.org/10.1109/EuCNC48522.2020.9200928.

Chahlaoui, F., El-Fenni, M. R. and Dahmouni, H. (2019). Performance analysis of load balancing mechanisms in sdn networks. https://doi.org/10.1145/3320326.3320368.

Costa-Requena, J., Guasch, V. F. and Santos, J. L. (2015). Software defined networks based 5g backhaul architecture. https://doi.org/10.1145/2701126.2701180.

Djigal, H., Xu, J., Liu, L. and Zhang, Y. (2022). Machine and deep learning for resource allocation in multi-access edge computing: A survey, **24**(4): 2449–2494. https://doi.org/10.1109/COMST.2022.3199544.

Dutta, A. and Hammad, E. (2020). 5g security challenges and opportunities: A system approach, pp. 109–114. https://doi.org/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. https://doi.org/10.1109/ACCESS.2017.2779146.

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. https://doi.org/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. https://doi.org/10.1109/ACCESS.2015.2461602.

Javed, M. A. and khan Niazi, S. (2019). 5g security artifacts (dos / ddos and authentication), pp. 127–133. https://doi.org/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, pp. 1–8. https://doi.org/10.1109/NOMS47738.2020.9110321.

Le, N. T., Hossain, M. A., Islam, A., Kim, D.-Y., Choi, Y.-J. and Jang, Y. M. (2016). Survey of promising technologies for 5g networks, *Mobile Information Systems* **2016**: 2676589. https://doi.org/10.1155/2016/2676589.

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. https://doi.org/10.1109/ACCESS.2021.3073115.

Li, Y. and Chen, M. (2015). Software-defined network function virtualization: A survey, *IEEE Access* **3**: 2542–2553. https://doi.org/10.1109/ACCESS.2015.2499271.

Liu, C., Raghuramu, A., Chuah, C.-N. and Krishnamurthy, B. (2017). Piggybacking network functions on sdn reactive routing: A feasibility study, p. 34–40. https://doi.org/10.1145/3050220.3050225.

Liyanage, M., Ahmad, I. and Abro, A. B. (2018). *A Comprehensive Guide to 5G Security*, Vol. 1, Wiley.

Mathew, A. (2020). Network slicing in 5g and the security concerns, pp. 75–78. https://doi.org/10.1109/ICCMC48092.2020.ICCMC-00014.

Meng, Y., Naeem, M., Almagrabi, A., Ali, R. and Kim, H. S. (2020). Advancing the state of the fog computing to enable 5g network technologies, *Sensors* **20**: 1754. https://doi.org/10.3390/s20061754.

Mir, A., Zuhairi, M. F., Musa, S., Syed, T. A. and Alrehaili, A. (2020). Poster: A survey of security challenges with 5g-iot, pp. 249–250. https://doi.org/10.1109/SMART-TECH49988.2020.00063.

Ravi, N., Rani, P. V. and Shalinie, S. M. (2019). Secure deep neural (seden) framework for 5g wireless networks, pp. 1–6. https://doi.org/10.1109/ICCCNT45670.2019.8944654.

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. https://doi.org/10.1109/ACCESS.2020.3046325.

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. https://doi.org/10.1109/ACCESS.2019.2943929.

Varum, T., Ramos, A. and Matos, J. N. (2018). Planar microstrip series-fed array for 5g applications with beamforming capabilities, pp. 1–3. https://doi.org/10.1109/IMWS-5G.2018.8484697.

Yi, B., Wang, X., Li, K., k. Das, S. and Huang, M. (2018). A comprehensive survey of network function virtualization, *Computer Networks* **133**: 212–262. https://doi.org/10.1016/j.comnet.2018.01.021.

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. https://doi.org/10.23919/JCC.2021.08.006.

Zhou, Y., Gao, Y., Chen, J., Li, D., Liu, Z., Wei, Y. and Ma, Z. (2022). Blockchain for 5g advanced wireless networks, pp. 1306–1310. https://doi.org/10.1109/IWCMC55113.2022.9825182.