electronics

MDPI

Review

A Layered Approach to Threat Modeling for 5G-Based Systems

Muhammad Najmul Islam Farooqui [1], Junaid Arshad [2,*] and Muhammad Mubashir Khan [1]

[1] Department of Computer Science & IT, NED University of Engineering & Technology Karachi, Karachi 75270, Pakistan; itsnajam@gmail.com (M.N.I.F.); mmkhan@neduet.edu.pk (M.M.K.)
[2] School of Computing and Digital Technology, Birmingham City University, Birmingham B4 7XG, UK
* Correspondence: junaid.arshad@bcu.ac.uk

Abstract: The rise of 5G networks promises a wide range of cutting-edge services with the aim of achieving high performance and reliability. Cutting-edge applications facilitated by 5G architecture make use of various enabling technologies, which introduce various new and emerging security threats and attacks. Threat modeling is a proactive approach to identify security requirements, as well as potential threats and vulnerabilities, and prioritize remediation methods. In addition, 5G networks are complex and are usually divided into separate layers to foster the understanding and management of different functionalities. The open nature of 5G envisages that multiple vendors and service providers might be working on network deployment and service provisioning; it is therefore necessary to address and categorize the threats at each layer distinctly. This paper presents a threat model for 5G-based systems. It leverages the layered 5G architecture, identifying threat categories and mapping these to corresponding layers. It also analyzes enabling technologies affected by identified threats along with threat actors, entry points, and the impact of threat categories. Through the development of this threat model, we envisage facilitating further research into specific threats and mechanisms to protect against them.

Keywords: threat modeling; 5G security; threat landscape; threat actors; enabling technologies; network slicing

Citation: Farooqui, M.N.I.; Arshad, J.; Khan, M.M. A Layered Approach to Threat Modeling for 5G-Based Systems. *Electronics* **2022**, *11*, 1819. https://doi.org/10.3390/electronics11121819

Academic Editor: Christos J. Bouras

Received: 18 April 2022
Accepted: 5 June 2022
Published: 8 June 2022

1. Introduction

The Fifth Generation (5G) Mobile Communication Network is the latest 3GPP standard which ensures high bandwidth and ultra-low latency. Such performance guarantees introduce tremendous benefits and facilitate diverse application use-cases leveraging virtualization, edge computing, cloud-based services, network slicing and other emerging technologies [1]. A recent study by Ericsson estimates that USD 31 trillion revenue will be generated due to 5G networks by 2030 [2]. Coupled with the emergence of new application scenarios and increasing use of Internet of Things (IoT), 5G network architecture and services are exposed to ever-increasing security risks and attacks. In order to improve the resilience of future networks against cyber threats, 3GPP has introduced improved security features and flexible policies for 5G including unified authentication and extensible authentication protocols for secure communication [3]. The new services provided by 5G architecture make use of Multi-access Edge Computing (MEC), Network Function Virtualization (NFV), Massive Mulitple–Input Multiple Output (MIMO) and cloud-native, service-based core architecture expanding the attack surface for 5G-based applications [4].

The 5G security architecture consists of different domains which include Network Access Security, Network Domain Security, User Domain Security, Application Domain Security and Service-Based Architecture (SBA) Domain Security [5]. Various security functions such as Authentication Server Function (AUSF), Authentication Credential Repository and Processing Function (ARPF) and Security Anchor Function (SEAF) are introduced in the 5G core network. The 5G security requirements include authentication and authorization, user data and signaling data confidentiality and integrity and subscribers'

privacy. The use of Subscriber Permanent Identifiers (SUPI), Subscriber Concealed Identifiers (SUCI) and Globally Unique Temporary UE Identity (GUTI) ensure privacy in the 5G network. End-to-end security monitoring throughout the 5G architecture including devices, applications and networks must be ensured for desired performance. Some of the key challenges include the security of radio interfaces, user plane integrity, and Denial of Service (DoS) attacks on the infrastructure and end-user devices [6]. Ref. [7] used a bibliographic approach to review the state-of-the-art in the field of 5G security and is the pioneering effort to investigate 5G security. Ref. [8] discuss several threats and present techniques to detect cyber-attacks in 5G networks. Ref. [9] presents the heuristic strategies for assessing wireless sensor network resiliency, whereas [10] investigates and evaluates existing vulnerabilities and security threats in real-world 5G mobile networks. Several other attacks have been identified and reported in the 4G network such as privacy attacks using side-channel information [11], cross-layer impersonation attack [12], desynchronization attack [13] and active IMSI catching and DoS attack [14].

Threat modeling is a systematic way to identify threats that may breach the security of a system or application [15]. Ref. [16] defines threat modeling as *"A process that can be used to analyze potential attacks or threats to a system supported by threat classification or attack taxonomies"*. Ref. [17] emphasizes the importance of understanding the adversary's objectives through threat modeling to be able to design secure systems. Threat modeling has been employed to study threats and attacks on a Software-Defined Network (SDN) [18] and Vehicular AdHoc Network (VANET) [19]; however, a holistic assessment is required to understand the attack surface for a 5G-based system to comprehend the potential cyber risk to such infrastructure and develop appropriate mechanisms to protect against them. Analyzing previous threat modeling work in 5G shows that the studies either focus on a specific layer or are limited to the specific enabling technology. There is not a single publication that discusses the security threats at each layer of the 5G architecture. This paper is focused on achieving a holistic threat modeling for a 5G-based system by taking into account threats at different layers of a typical 5G infrastructure and respective enabling technologies. Our approach is based on identifying the assets at different 5G layers, assessing the risk to each type of asset and then mapping potential threats to threat actors, 5G layers and enabling technologies. We divided 5G security threats into a device layer, radio access network (RAN) layer, edge layer, core network (CN) layer and service layer to create an attack tree that can be applied to 5G networks. Threats have been identified at each layer, and the possible affected components have also been mentioned. This approach provides a model of system security contexts that allows for the creation of a catalog of possible threats to the system and selection of security controls which can be used to address these threats based on the severity of the threat and the risk it poses to the system. It will be helpful in designing secure 5G systems and services. As 5G promises to support open network architecture in which several vendors and service providers may be involved in network and service deployment, it is essential to map threats to each layer. This will help network deployment and software development teams to prioritize fixes for existing network functions and services by anticipating the impact and severity of the threats. This approach ensures that the network can be protected against evolving threats.

In the next section, related work with respect to threat modeling in 5G is discussed, and limitations in earlier studies are identified. The subsequent section presents 5G layered architecture, enabling technologies such as Edge computing, SDN, Network Function Virtualization and Network Slicing along with the potential security challenges for individual layers. Finally, a 5G threat model with respect to each layer, attacks, and threat actors is explained, which includes a detailed analysis of threat classification, mapping between threats and enabling technologies, entry points and potential impact.

2. Related Work

A detailed 5G threat and vulnerability analysis is conducted by ENISA [20], which covers the existing threats and vulnerabilities found in the research material. Threats are

mapped to the assets using the STRIDE [21] threat model. The limitation of the study is that it does not cover all the layers of the 5G system, and the threats to the service-based architecture of the 5G core and the connected devices are not covered at all. As 5G promises to support open network architecture in which several vendors and service providers may be involved in network and service deployment, it is essential to map threats to each layer. It will ensure secure 5G architecture, and each vendor and service provider will only have to take care of the layers they are responsible for. Ref. [22] presented a preliminary threat analysis of the service-based architecture in 5G networks. The authors discuss the risks involved in using web technologies in service-based architecture such as REST, JSON and TLS. The discussion is limited to the web technologies used in the service-based architecture where the vulnerabilities in different core functions are not properly covered. Ref. [23] presented three-dimensional threat taxonomy with respect to NFV security in 5G networks. The authors analyzed the 5G ecosystem and then presented detailed NFV deployment models and their security implications. A threat model is presented involving three dimensions including intra-layer, inter-layer and inter-administrative domains. NFV threats were divided in four categories: namely, virtualization, centralized management, service operation, and communication. The authors also discuss some of the ongoing projects which are related to NFV security. The study only discusses NFV and does not include trust management, security management framework, and cyber threat intelligence with respect to other enabling technologies such as SDN and MEC.

The authors in [24] present vulnerability analysis of a 5G NR physical layer and a survey of available mitigating techniques. The paper assesses physical signals and control channels individually and discusses vulnerabilities especially related to spoofing and jamming attacks. IoT and Wireless Sensor Networks (WSN) are two important applications of 5G, and various studies have analyzed the threats to these use-cases. Ref. [25] uses the layered approach to categorize the threats to the IoT networks. These threats are classified into a perception layer, network layer and application layer. Furthermore, it presents a learning-based approach to defend against perception layer attacks. Ref. [26] discusses the different attacks on the network layer in WSN and presents a novel mechanism to detect DDoS attacks. Ref. [27] analyzed the threats related to network slicing in the 5G core and categorized them using the STRIDE threat modeling methodology. The authors present the network slicing life cycle, which involves the stages of preparation, creation, run time, and termination of a network slice. It then presents the trust boundaries in network slicing with respect to the network operator's perspective involving radio, transport, core and computes the components of a network slice. Threats are divided into STRIDE categories comprising Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Escalation of Privilege. The authors suggest that the detailed future work can be carried out in 5G network slice threat modeling using any other threat modeling strategy such as PASTA [28] to cover future threats and attacks.

In the paper [29], the authors present a review of the research work done in the Cyber-Physical Systems (CPS) and Cyber-Physical Energy Systems security landscape. The paper proposes a threat modeling methodology that comprises the adversary and attack model to system vulnerabilities. The authors provide a risk assessment process which considers the effectiveness of an attack and the components of the targeted system. It then describes a framework to characterize the CPS, which is essential to evaluate several studies in energy, healthcare and transportation sectors. Finally, the authors demonstrate the practical use of a CPS framework with the help of four attack case studies including the application of PCS analysis framework stages. Each attack case is characterized by a threat model, attack setup and risk assessment.

The authors in [30] presented an attack on 5G Authentication and Key Agreement (AKA) protocols and penetrated subscriber privacy. They performed a security analysis of the vulnerability and discussed countermeasures to remedy the attacks. The authors uncovered a new logical vulnerability, requiring dedicated fixes, that the attack exploited. They also used widely available low-cost setups to demonstrate the applicability of the attack.

Table 1 presents a summary of the work done in the field of threat modeling within 5G networks. The comparison is done using parameters such as coverage of layered architecture, threat actors, enabling technologies such as NFV, SDN, MEC and Network Slicing and the impact of the threats within each study. It is evident that the studies either focus on a specific layer or are limited to the specific enabling technology. Ref. [23] only covers the threats to NFV and discusses the role of threat actors. Ref. [24] focuses on the attacks within the 5G radio layer and covers threat actors. The threat modeling study in [22] presents threat attacks with reference to the service-based architecture in the core network. This study covers threats to each layer in 5G architecture and also discusses the threats to the enabling technologies. The impact of each threat is included as well as the role of different threat actors while mapping all the threats to each layer.

Table 1. Analysis of existing literature within 5G threat modeling.

Reference	Journal/ Conference	Year	Layered Architecture Coverage	Threat Actors	SDN	NFV	MEC	Network Slicing	Impact
[20]	ENISA	2020	X	✓	✓	✓	✓	✓	✓
[23]	Computer Networks	2021	X	✓	X	✓	X	X	X
[24]	IEEE ICC Workshops	2018	✓	✓	X	X	X	X	X
[30]	Proceedings on Privacy Enhancing Technologies	2019	✓	X	X	X	X	X	X
[18]	ENISA	2015	X	X	✓	X	X	X	X
[22]	Wireless Personal Communications	2021	X	X	X	X	X	✓	X
This paper	–	–	✓	✓	✓	✓	✓	✓	✓

3. 5G Layered Architecture and Enabling Technologies

In this section, we provide fundamental knowledge about *5G Architecture* and enabling technologies such as Network Function Virtualization (NFV), Software-Defined Networking (SDN), Edge Computing and Network Slicing, which underpin this emerging paradigm. The 5G deployments support open network architecture in which several vendors and service providers may be involved in network and service provisioning, which is why it is essential to map threats to each layer. This will help secure network and deployment by prioritizing fixes for existing network functions and services by anticipating the impact and severity of the threats. This approach ensures that the network can be protected against evolving threats.

3.1. Layered 5G Architecture

The 5th generation mobile network is expected to deliver a multi-Gbps data rate, ultra-low latency, better reliability, increased network capacity and availability. The 5G networks are designed to connect everyone and everything including devices, machines and vehicles. Ref. [31] presents the network architecture and the security issues within the core layer of the 5G network. Figure 1 gives the layered architecture of the 5G network, which includes a device layer, radio layer, edge layer, core layer and service layer. Several innovative use cases and user experiences are proposed to benefit from the improved efficiency and higher performance provided by 5G networks. It is essential to study the architecture and security requirements of each component to design secure network and applications.

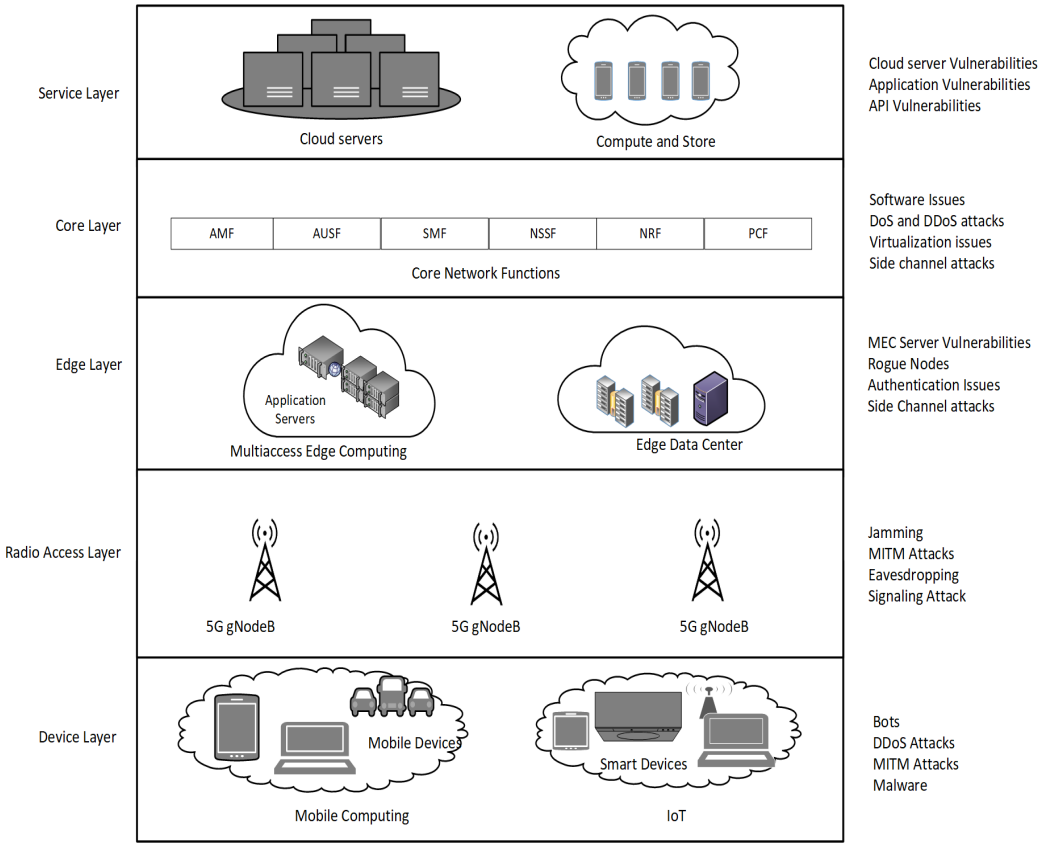

Figure 1. 5G layered architecture.

- **Device layer** This layer consists of the devices which may connect to the 5G network. These devices can range from mobile phones to drones, IoT devices to home appliances and autonomous vehicle to a network access point. The attack surface of these devices is extremely volatile with novel threats emerging regularly such as malware, worms, botnets and in some cases advanced persistent threats [32]. The consequence of a successful breach in this case can range from compromise of user privacy to a potential full-scale attack on the network infrastructure and services.
- **Radio layer** The 5G Radio Access Network (RAN) layer provides wireless connectivity to devices to connect to the 5G core network and services using 5G radio frequencies. Prominent use cases include cloud gaming, AR/VR, autonomous driving, and fixed wireless access. The radio access network consists of transmitters, antennas, base-band (RAN Compute), and RAN software to enable ultra-high speeds and mobility. The 5G network has introduced several improvements in RAN compared to 4G such as multiple antenna arrays, multiple input multiple output (MIMO) and centralized or Cloud RAN (C-RAN). However, these are susceptible to attacks targeting the RAN such as unauthorized access, traffic sniffing, signaling storms, flooding and jamming.
- **Edge layer** The introduction of an edge layer within 5G architecture is envisaged to facilitate use cases such as autonomous vehicles and remote surgery, which require ultra-low latency (1 ms) and are supported by bringing compute capabilities closer to the end-user. Edge computing can be included in WiFi hotspots, radio towers and network routers. As the edge layer uses NFV and SDN, threats and attacks to these enabling technologies are also applicable on the edge layer in a 5G network. Edge nodes are susceptible to Denial of Service attacks, side-channel attacks and VM-based attacks.
- **Core layer** The 5G core is designed as a cloud-native service-based architecture that uses NFV and SDN to provide advanced network functionalities. It has defined several interconnected virtual functions which provide services such as authentica-

tion, session management, mobility and security. These functions include Access and Mobility Management Function (AMF), User Plane Functions (UPF), Session Management Functions (SMF), Data Network (DN), Authentication Server Functions (AUSF), Network Slice Selection Function (SMF) and Unified Data Management (UDM). These functions are divided into the control and user plane and provide an interface to each other so that any function can request service from any other function. The 5G core design principles include Control and User-Plane Separation (CUPS), modular function design, minimizing dependencies between the RAN and Core network and concurrent access to local and centralized services. Several threats to the 5G core layer functions have been identified in [31,33], which need to be assessed while designing any 5G core network. Both control and user planes may be affected by these attacks, which include DoS and spoofing attacks on AMF, routing attacks on AUSF and UPF and SIP relay attacks on IMS AF.

- **Service layer** The service layer provides the application interface to the users. Service providers define the programmable interfaces (APIs), and the architecture of this layer is independent of the underlying 5G architecture. Security at this layer is typically the responsibility of the service provider, and the threats faced by the services have a significant overlap with the contemporary Internet-based applications. Proper security features need to be maintained including authentication, authorization, secrecy and non-repudiation.

3.2. Enabling Technologies

- **Software-Defined Networking (SDN)** is an emerging network architecture that allows decoupling of the control and data plane and adds programmability, making network control flexible. The benefits of SDN include enhanced configuration, improved performance, and innovation. SDN allows the configuration of network devices such as routers, switches, and firewalls automatically from a single point. It helps to add new network devices easily and makes automatic control through software possible. Network optimization using software helps solve challenges such as congestion control, routing, traffic scheduling and quality of service. The high configurability provided by SDN promises more innovative network solutions and use cases to be implemented by the network service providers and telecommunication operators. These benefits make SDN a palpable choice for 5G networks to provide innovative and optimized services to the customers. The use of SDN in 5G networks can lead to attacks such as DoS on the controller, TLS/SSL attacks on the control channel, and flow modification on the data channel [4]. Ref. [18] has identified several threats to SDN including data forging, traffic diversion, side channel attack, flooding attack, DoS attack, identity spoofing and traffic sniffing.
- **Network Function Virtualization (NFV)** NFV architecture was proposed by the European Telecommunications Standards Institute (ETSI), and that also defined the NFV implementation standards. NFV is a way to replace network services and proprietary network devices such as routers, switches, and firewalls with virtual network functions. NFV uses a virtual machine that runs on standard servers instead of proprietary hardware. It allows service providers to provide new on-demand applications and services without requiring specialized hardware. It allows multiple virtual functions to be executed on a single server and flexibility to move from one server to another. The NFV architecture consists of Virtual Network Functions (VNF), Network Functions Virtualization infrastructure (NFVi) and Management, Automation, and Network Orchestration (MANO). VNFs are the virtualized network functions that provide file sharing, network configuration and directory services. NFVi consists of the hypervisor that provides computing, storage, and networking. MANO provides automation support for new VNFs and control of the NFV infrastructure.
  Several threats to NFV and possible attacks have been identified in the literature. Ref. [4] lists security issues related to NFV architecture which include management

and orchestration, virtual network functions, and virtual machines related attacks. Ref. [23] presented a three-dimensional threat taxonomy of NFV-based 5G networks by discussing its benefits, architecture, and design requirements.

- **Multi-access Edge Computing (MEC)** MEC brings computing, store, and networking services closer to the end user or data sources. It solves the latency, bandwidth, and reliability issues of the emerging use cases such as machine learning, AR/VR, IoT, and network functions that require service provisioning closer to users. Edge computing provides computing services at the network edge for real-time processing and cloud-based computing for the operations, which require more powerful computing capabilities. In the absence of edge computing, data processing would be carried out at the centralized cloud servers, resulting in higher latency and increased data transmission costs. With the help of edge computing, decisions can be made quickly near the user end for the emergency services requiring low ultra-low latency. MEC will help achieve 5G objectives such as supporting Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLCC) and Massive Machine-Type Communications (mMTC). The use of enabling technologies such as virtualization, wireless network and distributed architecture within MEC makes it vulnerable to numerous attacks [34]. Mirai botnet attack is an example of a practical attack on IoT and edge devices were later used for DDoS attacks [35].
- **Network Slicing** The 5G network promises to provide ultra-low latency and an ultra-high data rate while supporting mainly three broad application scenarios including Ultra-Reliable and Low-Latency Communications (URLLC), Enhanced Mobile Broadband (eMBB), and Massive Machine-Type Communications (mMTC). These diverse scenarios require extremely dynamic and highly scalable network architecture from mobile operators and network service providers. Extreme (or enhanced) Mobile Broadband (eMBB) supports applications such as HD video streaming and AR/VR and generates huge data and requires really high bandwidth. Massive Machine-Type Communications (mMTC) is also known as the Internet of Things, and it supports billions of connected devices which may not require high bandwidth but need specialized services such as massive MIMO in order to support huge numbers of devices. Ultra-Reliable Low-Latency Communications (uRLC) facilitates use cases such as vehicle-to-X (v2x) communications or remote surgery, which requires ultra-low latency, and mobile network operators need to use mobile edge computing to provide it. Network slicing plays a key role in providing this extreme flexibility in the networks. As a result of recent advancements, network slicing has gained massive popularization in SDN and NFV, but it also gave rise to new inter-slice security threats such as privacy, secure communication, slice isolation, slice-specific authentication, and authorization, which need more research work and appropriate solutions [36,37]. Due to the virtual isolation rather than the physical isolation in 5G network slicing, a number of security attacks are possible. Among them, side channel attack is a very common attack for the slices which are sharing the same infrastructure and require a comprehensive analysis and protection mechanism [4,38].

4. Threat Vectors and Dimensions

The 5G networks are complex and are usually divided into separate layers to understand different functionalities easily. The open nature of 5G envisage that multiple vendors and service providers might be working on network deployment and service provisioning; it is therefore necessary to discuss and categorize the threats at each layer distinctly. Figure 2 shows the 5G threat vector which includes the five layers on which the threats are mapped. We present the threats affecting the specific layer.

- The device layer threat dimension encompasses all the potential attacks that can impact an asset within the end devices connected to the 5G networks.
- The RAN layer threat dimension is concerned with attacks that are initiated at the Radio Access layer in the 5G network.

- The edge layer domain threat dimension incorporates potential attacks which take advantage of any weakness in the edge layer devices.
- The core layer threat dimension covers potential attacks which can include the network functions providing authentication, session management, security of user data and credentials.
- The service/application layer threat dimension include all the threats which can affect the applications running on the cloud.

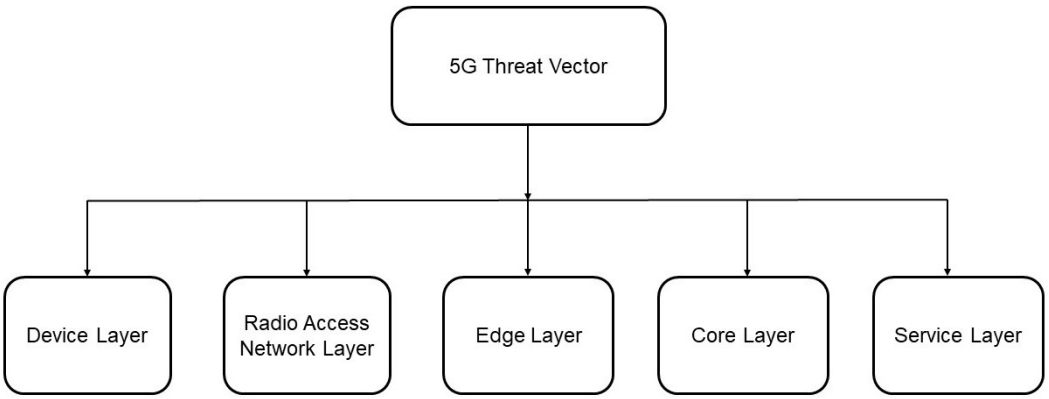

Figure 2. 5G Threat Vector.

4.1. Security Threats

The 5G network threats are studied at separate layers based on the impact these attacks have on different network function and services. Another aspect of security threats is the enabling technologies, which may be affected by the threats. Here, we classify the threats into the categories and also present the same in the form of Tables 2–4 and Figure 3 (https://bit.ly/3uhe4dS, accessed on 7 June 2022). Figure 3 classifies the threats in various categories, whereas Figure 4 (https://bit.ly/3Jp2QIM, accessed on 7 June 2022) maps the threats to each layer and categorizes according to the security requirements of privacy, integrity, authentication and availability.

- **Authentication abuse:** Authentication abuse can result in unauthorized access to network services and can cause integrity violations. Affected services can be AMF, NSSF, AAA and other services. Hyperjacking is an example of such attacks in which a malicious VM performs privilege escalation to gain root access by exploiting the hypervisor's vulnerabilities. It subsequently leads to the control over the host and eventually over all the existing VMs. Edge, core and service layers can all be affected by these types of attacks.
- **Information Leakage**: In case of unauthorized access to user plane or signaling data, sensitive information such as user data, cryptographic keys, monitoring logs and signaling data can be leaked. The core layer, cloud layer and edge layer can be affected. Attacks include security key theft, misuse of security audit tools and access to network traffic. In case of VM hopping attacks to core layer network functions and edge servers, side channels are used by the malicious VM to gain access to cryptographic keys or to establish illicit communication channels.
- **Denial of Service**: These attacks result in the service unavailability of the genuine network users. It may include a host-based DoS attack to target hosts to drain the CPU, memory and bandwidth resource usage. Flooding, jamming network radio and jamming network interface are other examples of DDoS attacks. A bandwidth saturation attack can exploit the bandwidth over-subscription. Overloading the edge node may cause edge routers/switches to become a bottleneck. The 5G network services and components which can be affected are SDN, NFV, RAN, MEC, cloud servers and the core network. The service-based architecture of the 5G core and their

functions such as AMF, SMF and key management servers are also the possible targets. Table 3 shows the layers and services affected by the Denial of Service attack.

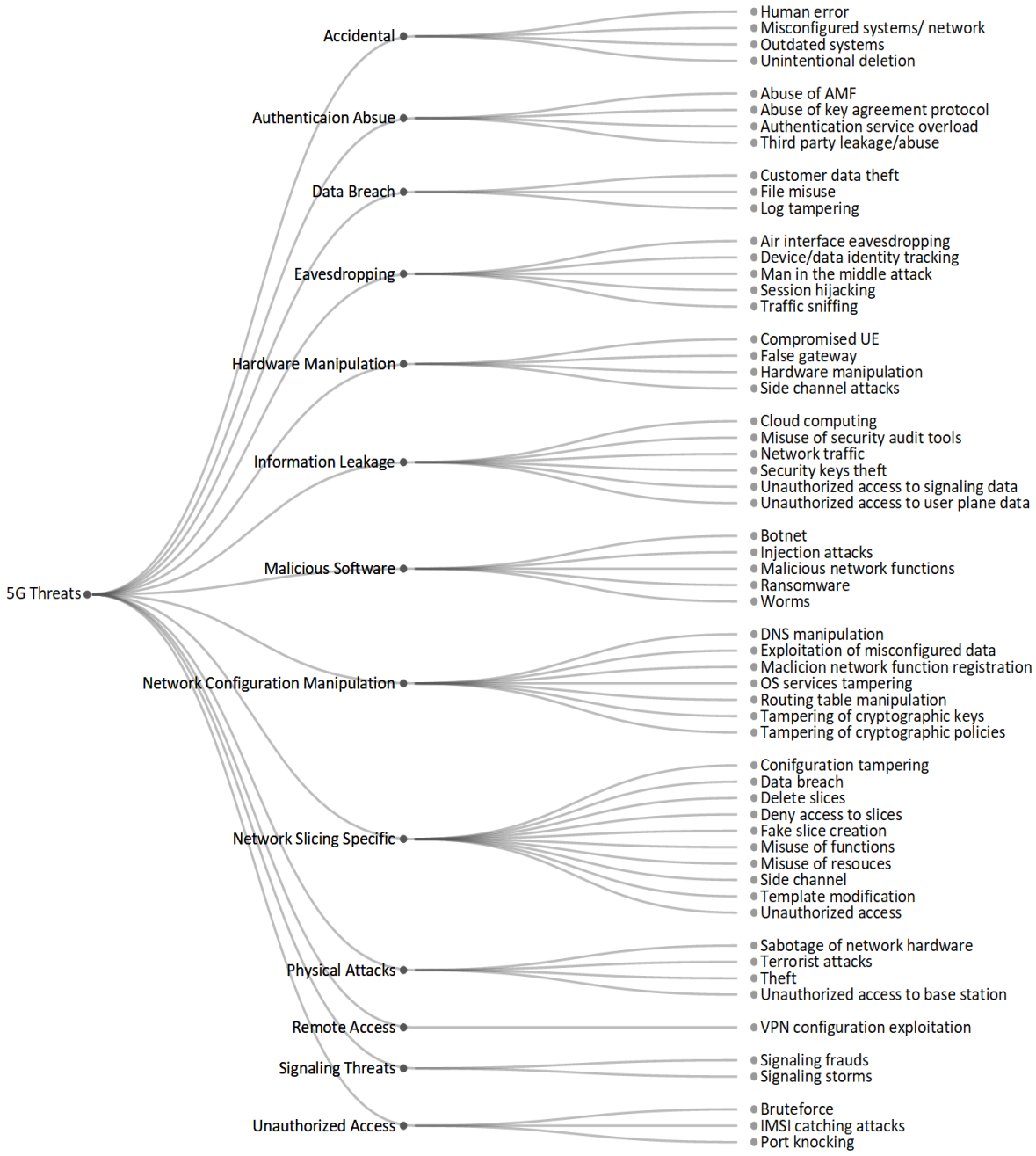

Figure 3. Taxonomy of 5G threat categories.

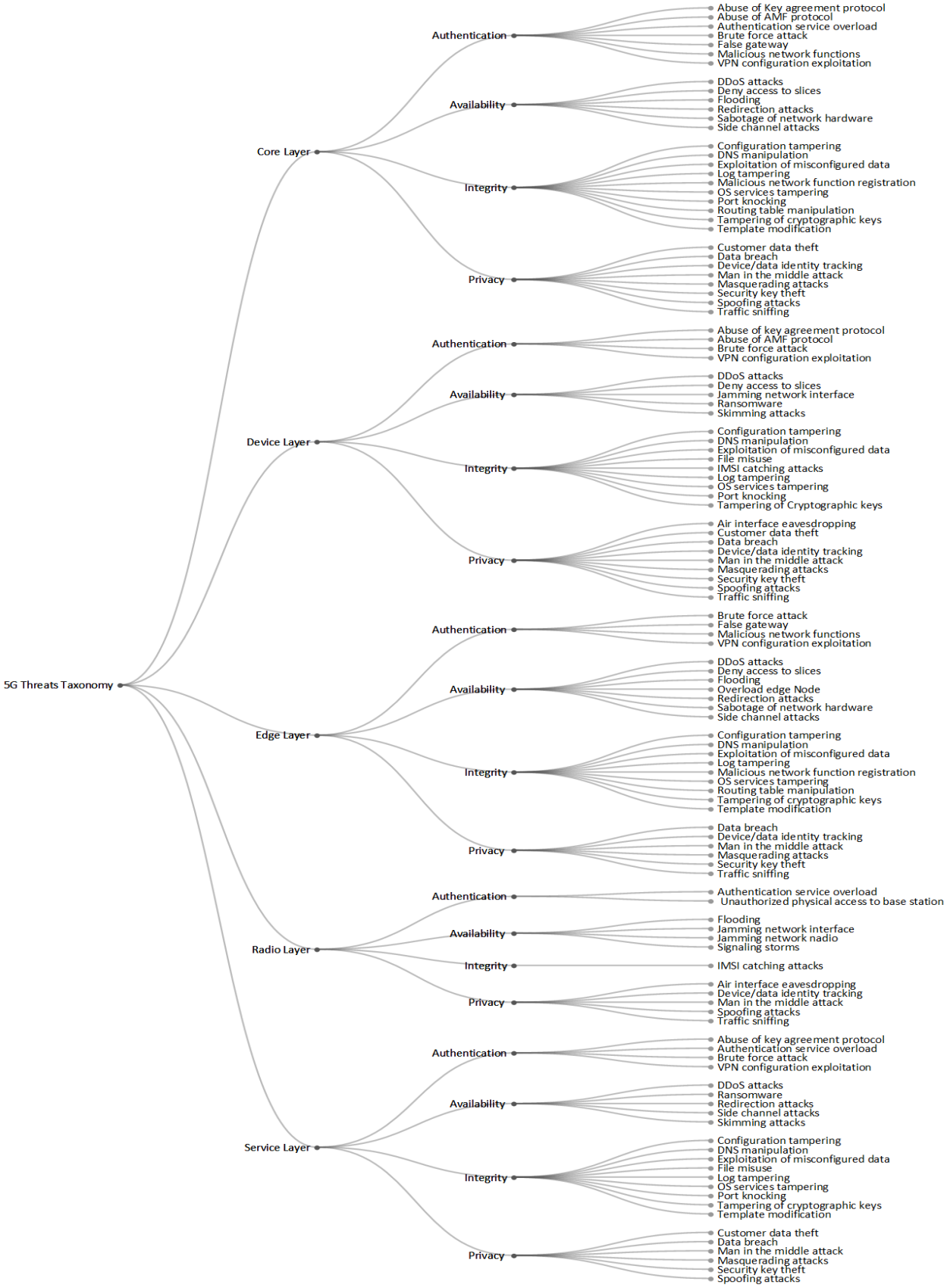

Figure 4. Taxonomy of 5G threat mapped with layers.

- **Network Configuration Manipulation**: A network configuration manipulation attack includes DNS and routing table manipulation, exploiting of misconfigured data and services and tampering of cryptographic keys and policies. These attacks can affect the security of 5G components such as SDN, NFV, MANO, and RAN. The layers affected are the radio, core, and edge, where the SDN controller, network functions such as PCF, AMF, network orchestrator, and DNS servers can be attacked.
- **Malicious Software**: Attacks that can be included in this category are injection attacks, worms, ransomware, malicious network functions and botnet. These attacks can cause service unavailability, information destruction and integrity violations at the device layer, MEC layer, core layer and service layer.
- **Hardware Manipulation**: Hardware attacks can be launched on the user and MEC equipment, and the radio unit can cause unavailability and information destruction.
- **Signaling Threats**: Malware or apps can launch signaling storms which in turn overload the signaling server, cell bandwidth and cloud servers and can also drain the mobile device battery [39]. It affects the device, core and cloud layers of the 5G architecture. Signaling frauds can also affect the integrity and confidentiality of the system.
- **Eavesdropping**: It is an attack in which the attacker stealthily listens to the network communication to gain access to the secret information such as the sensitive data, encryption keys and other personal information. Attacks include traffic sniffing, man in the middle attack, session hijacking, and device or user tracking. It affects data confidentiality and authentication.

Table 2. Categories of 5G threats mapped with layers.

Attack Categories	Core Layer	Device Layer	Edge Layer	Radio Access Network Layer	Service Layer
Network Configuration Manipulation	Routing table manipulation Malicious network function registration Tampering of Cryptographic keys and policies	Exploitation of misconfigured data OS services tampering	Routing table manipulation Malicious network function registration	N/A	DNS manipulation Exploitation of misconfigured data Exploitation of misconfigured service Tampering of Cryptographic keys and policies OS services tampering
Malicious Software	Malicious network functions	Worms Ransomware Botnet	Malicious network functions	N/A	Worms Ransomware Botnet Injection attacks
Remote Access	N/A	VPN configuration exploitation	N/A	N/A	VPN configuration exploitation
Hardware Manipulation	Side channel attacks	N/A	Side channel attacks	N/A	Side channel attacks
Unauthorized Access	N/A	N/A	N/A	IMSI catching attacks	Port Knocking Brute force
Information Leakage	Security keys theft Unauthorized access to user plane data Unauthorized access to signaling data	N/A	N/A	Network traffic Unauthorized access to signaling data	Misuse of security audit tools

Table 2. *Cont.*

Attack Categories	Core Layer	Device Layer	Edge Layer	Radio Access Network Layer	Service Layer
Authentication Abuse	Authentication service overload Abuse of AMF and key agreement protocol	N/A	N/A	N/A	Third party leakage/abuse
Data Breach	Log tampering Customer data theft	File misuse Customer data theft	N/A	N/A	Log tampering File misuse Customer data theft
Eavesdropping	N/A	Session hijacking Device/data identity tracking	N/A	Traffic sniffing Man in the middle attack Air interface eavesdropping	Session hijacking
Physical Attacks	N/A	Theft	Sabotage of network hardware Terrorist attacks	Sabotage of network hardware Terrorist attacks Unauthorized physical access to base station	N/A
Accidental	Human error	Human error Misconfigured systems/ network Unintentional deletion	N/A	N/A	Human error Unintentional deletion
Network Slicing Specific	Template modification Configuration tampering Fake slice creation Deny access to slices Data breach Delete slices	N/A	Unauthorized access Misuse of resources and function Side channel	Misuse of resources and function Side-channel	Unauthorized access Misuse of resources and function Side channel
Signaling Threats	Signaling storms Signaling frauds	N/A	N/A	Signaling Storms Signaling Frauds	N/A

Table 3. Threat categories mapped with threat actors.

Threat Actors/Attack Categories	Cyber Criminal	Hacktivist	Cyber Terrorist	Cyber Warfare	Insider Mal-Actor	Script Kiddies
Network Configuration Manipulation	✓	X	✓	✓	✓	✓
Hardware Manipulation	X	X	✓	✓	✓	X
Unauthorized Access	✓	✓	✓	✓	✓	✓
Authentication Abuse	✓	✓	✓	✓	✓	✓
Data Breach/ Eavesdropping	✓	✓	✓	✓	✓	✓
Physical Attacks	X	X	✓	✓	X	X
Accidental	X	X	X	X	✓	✓

Table 4. Attack categories for 5G-based system mapped with layers.

Attack Categories	Attack Types	Impact	Affected Components	Affected Layer	Entry Point
Denial of Service Attacks	DDoS attacks Flooding, Jamming network radio, Jamming network interface, Overloaded edge node	Service Unavailability Outage	SDN, NFV, RAN, MEC, Cloud, Network services	Radio, Core	Servers/Virtual functions MEC Server, AMF, SMF
Network Configuration Manipulation	Routing table manipulation, Malicious network function registration, DNS manipulation, Exploitation of misconfigured data, Tampering of cryptographic keys and policies, OS services tampering	Integrity violation information destruction Unavailability	SDN, NFV, MANO, RAN, Configuration data (System, Network, Security)	Radio, Core, MEC	SDN controller, Network functions, PCF, DNS servers, AMF, Network orchestrator
Malicious Software	Injection attacks worms, Ransomware, Malicious network functions, Botnet	Service Unavailability Information Integrity Information destruction	Data Network, Applications, Cloud, Application data, services	Core, MEC	Database server, Network functions
Remote Access	VPN configuration exploitation	Integrity, Confidentiality	SDN, NFV, Cloud	Core, Cloud	SDN Controller, Network functions, Cloud servers, Network Orchestrator
Hardware Manipulation	Side channel attacks, False gateway, Compromised UE, Hardware manipulation	Unavailability Integrity Information Destruction	Cloud equipment, UE, Radio Unit SDN, NFV, RAN, Virtualization Network services, data	Radio, Transport	Virtual machines, Network functions, SDN controller, User device
Unauthorized Access	IMSI catching attacks, Brute force, Port knocking	Information Integrity System Integrity	UE, Network Services Data services	Core, Radio	Virtual machines, Network functions, SDN controller, User device
Information Leakage	Network traffic, Cloud computing, Misuse of security audit tools, Security keys theft, Unauthorized access to user plane data, Unauthorized access to signalling data	Confidentility Integrity Information Destruction	Data storage, User data, Cryptographic keys, Monitoring logs, Signaling data	Core, Cloud, MEC	Storage Area Network, SMF, Network servers, Databases
Authentication Abuse	Authentication service overload, Third party leakage/abuse, Abuse of AMF and key agreement protocol	Integrity violation Unauthorized access	User data, Service data, Configuration profiles	Device, Edge, Core, Service	AMF, AAA servers
Data Breach	Log tampering, File misuse, Customer data theft	Integrity, Authorization Confidentiality	Network equipment, User data, Configuration data, Cloud	Core, Cloud	Network servers, Databases
Signaling Threats	Signaling storms, Signaling frauds	Unavailability Integrity, Confidentiality	Network services, Radio equipment, Signaling servers, Cloud servers	Radio	Servers, Network functions

Table 4. *Cont.*

Attack Categories	Attack Types	Impact	Affected Components	Affected Layer	Entry Point
Eavesdropping	Traffic sniffing, Man in the middle attack, Session hijacking, Air interface eavesdropping, Device/data identity tracking	Confidentiality violation, Integrity violation	User data, Cryptographic keys, Profile data	Radio, Core	Radio interface, SMF
Physical Attacks	Sabotage of network hardware theft, Terrorist Attacks, Unauthorized physical access to based station	Unavailability, Confidentiality violation	UE, Radio equipment, Edge devices	Radio, MEC	Network equipment
Accidental	Misconfigured systems/network outdated systems, Human error, Unintentional deletion	Integrity violation, Service unavailability		Radio, Core	Network functions, Cloud Servers
Network Slicing Specific	Template modification, Configuration tampering, Fake slice creation, Deny access to slices, Data breach delete slices, Unauthorized access, Misuse of resources and functions, Side channel attacks	Integrity violation, Confidentiality violation, Service unavailability	Network slicing orchestrator, NFV, SDN, RAN, API	Core, Radio, Transport	NSSF, AMF, Slice orchestrator, SDN controller

4.2. Threat Actors

A threat actor is a person, organization or a nation state which carries out a malevolent act against another person, organization or enemy state. This section first defines the most common type of threat actors and they give a detailed description of the threats each type of actor may pose.

- **Organized hackers**: These are professional hackers whose goal is to attack systems for profit.
- **Hacktivist**: These are the individuals who use hacking to promote their political or social agenda by defacing websites or disabling services and interfaces.
- **Cyber terrorist**: These are expert individuals who are motivated by political or religious beliefs and use their wide-ranging skills to create fear of large-scale disruption of telecommunication services.
- **Cyber warfare**: They are employed by governments to infiltrate to damage the information system and gain the confidential information of other governments.
- **Insider Mal-actors**: These are threats that originate from people within the organization, such as disgruntled and terminated employees and under-trained staff.
- **Script Kiddies**: These are amateur hackers who run software and scripts developed by real hackers to compromise systems.

Table 3 shows the mapping between the threat actors and the type of threats, as different types of actors have different motives. For example, a cybercriminal wants monetary benefits and would like to gain unauthorized access over businesses and users of all types. The data they steal will be put up for sale in the dark net to the highest bidders. They would sometimes just do it for fun and may also remove it from the user's accounts and servers. Hacktivism has been on rise for several years, and hacktivists perform hacking in order to increase awareness, exposing corporate secrets and whistle blowing. Wikileaks

is the most obvious example of hacktivism, which was initiated to expose state secrets and changing perceptions of government activities. Cyber terrorists want to create the state of fear and unrest across a targeted country or community. They utilize all possible tools and cyber weapons to achieve their goals. They like to attack critical infrastructure and services such as power grids, energy resources and communication systems. They can attack organizations, businesses, and state agencies to achieve their goals. Cyber warfare or state-sponsored actors target specific nation states to steal state secrets and sensitive information. Their goal is to spy to further the interests of a rival state. Most of the cyber attacks are carried out from within the perimeter of the targeted organization or businesses. An insider Mal-actor would infiltrate a workplace and use criminal activities to express grievances or gain financial benefits, as the insiders have privileged access over the secret information or resources. Former employees can also a source of these attacks on their own or external actors. Script kiddies can also be as dangerous as any other actor having limited knowledge or skills to design sophisticated tools. They would purchase or use the tools of other actors to attack the targeted system or network. They can take advantage of the known vulnerabilities published online by other actors and cause damage to the resources.

Table 2 maps the threats to each layer of 5G architecture, whereas Table 4 lists the type of attacks which can exploit the threats. Furthermore, the impact of these attacks are also presented as well as the affected components of the system and the entry points that can be used to launch the attacks. Figure 3 classifies the threats in various categories, whereas Figure 4 maps the threats to each layer and categorizes them according to the security requirements of privacy, integrity, authentication and availability.

5. Analysis and Future Directions

We have presented a brief overview of different security threats to the 5G networks and the enabling technologies. With the introduction of numerous new cases such as the Internet of Things, smart cars, Virtual/Augmented reality, high-definition video streaming and remote surgery, new and advanced types of threats are also inevitable and need to be considered and studied. To develop a threat model for 5G, we need to define the user and network assets that are at risk and must be protected. The identification of threat actors for the assets is also another important requirement. Then comes the need to identify the threats these actors pose and attacks which can be launched. The treats should be categorized both in terms of types and the assets and layers these attacks can affect. The paper first gives the background and discusses the layered architecture of a 5G network, presenting the services provided by each layer and their security considerations. Later on, the security issues of enabling technologies are discussed, such as Edge computing, Software-Defined Networking, Network Function Virtualization and Network Slicing. Detailed related work is given, which discusses the previous work in this field and presents different threat modeling techniques. Related work is presented with respect to threat modeling in 5G, and finally, the 5G threat model with respect to each layer, attacks, and threat actors is explained. Threats are classified and mapped to each enabling technology and 5G layers.

Future work in 5G threat modeling can be extended toward real-time attacks in private 5G networks. Private 5G networks work on a smaller scale as compared to public networks and use micro cells to provide coverage in a limited area. These networks can be used to deploy novel Internet of Things use cases such as automated industrial process, connected vehicles, smart cities, telehealth etc. These types of applications are susceptible to Denial of Service attacks, interception, man-in-the-middle attack and DNS spoofing [40]. Another direction is to map the identified threats in this study to known weaknesses and patterns databases such as common weakness enumeration (CWE), common attack pattern enumeration and classification (CAPEC) and MITRE ATT&CK framework.

Author Contributions: Conceptualization, J.A.; methodology, M.N.I.F., J.A. and M.M.K.; validation, J.A. and M.M.K.; Writing—original draft preparation, M.N.I.F.; Writing—review and editing, M.N.I.F., J.A. and M.M.K.; Project administration, M.M.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Agyapong, P.K.; Iwamura, M.; Staehle, D.; Kiess, W.; Benjebbour, A. Design considerations for a 5G network architecture. *IEEE Commun. Mag.* **2014**, *52*, 65–75. [CrossRef]
2. Ericsson. Harnessing the 5G Consumer Potential. 2021. Available online: https://www.ericsson.com/en/reports-and-papers/consumerlab/reports/harnessing-the-5g-consumer-potential (accessed on 17 January 2022).
3. ETSI. Security Architecture and Procedures for 5G System. 2018. Available online: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.04.00_60/ts_133501v150400p.pdf (accessed on 6 January 2022).
4. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Commun. Surv. Tutorials* **2019**, *22*, 196–248. [CrossRef]
5. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Gurtov, A.; Ylianttila, M. Security for 5G and beyond. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 3682–3722. [CrossRef]
6. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. Overview of 5G security challenges and solutions. *IEEE Commun. Stand. Mag.* **2018**, *2*, 36–43. [CrossRef]
7. Farooqui, M.N.I.; Arshad, J.; Khan, M.M. A bibliometric approach to quantitatively assess current research trends in 5G security. *Libr. Hi Tech* **2021**, *39*, 1097–1120. [CrossRef]
8. Alshunaifi, S.Y.; Mishra, S.; AlShehri, M.A.R. Cyber-Attack Detection and Mitigation Using SVM for 5G Network. *Intell. Autom. Soft Comput.* **2022**, *31*, 13–28. [CrossRef]
9. Testa, A.; Cinque, M.; Coronato, A.; De Pietro, G.; Augusto, J.C. Heuristic strategies for assessing wireless sensor network resiliency: An event-based formal approach. *J. Heuristics* **2015**, *21*, 145–175. [CrossRef]
10. Park, S.; Kim, D.; Park, Y.; Cho, H.; Kim, D.; Kwon, S. 5G Security Threat Assessment in Real Networks. *Sensors* **2021**, *21*, 5524. [CrossRef]
11. Hussain, S.R.; Echeverria, M.; Chowdhury, O.; Li, N.; Bertino, E. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego, CA, USA, 24–27 February 2019.
12. Rupprecht, D.; Kohls, K.; Holz, T.; Pöpper, C. *IMP4GT: IMPersonation Attacks in 4G NeTworks*; NDSS: New York, NY, USA, 2020.
13. Mathi, S.; Dharuman, L. Prevention of desynchronization attack in 4G LTE networks using double authentication scheme. *Procedia Comput. Sci.* **2016**, *89*, 170–179. [CrossRef]
14. Mjølsnes, S.F.; Olimid, R.F. Easy 4G/LTE IMSI catchers for non-programmers. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 235–246.
15. Marback, A.; Do, H.; He, K.; Kondamarri, S.; Xu, D. A threat model-based approach to security testing. *Softw. Pract. Exp.* **2013**, *43*, 241–258. [CrossRef]
16. Uzunov, A.V.; Fernandez, E.B. An extensible pattern-based library and taxonomy of security threats for distributed systems. *Comput. Stand. Interfaces* **2014**, *36*, 734–747. [CrossRef]
17. Bedi, P.; Gandotra, V.; Singhal, A.; Narang, H.; Sharma, S. Threat-oriented security framework in risk management using multiagent system. *Softw. Pract. Exp.* **2013**, *43*, 1013–1038. [CrossRef]
18. Belmonte Martin, A.; Marinos, L.; Rekleitis, E.; Spanoudakis, G.; Petroulakis, N. *Threat Landscape and Good Practice Guide for Software Defined Networks/5G*; European Union Agency for Network and Information Security: Athens, Greece, 2015.
19. Hamad, M.; Prevelakis, V. SAVTA: A hybrid vehicular threat model: Overview and case study. *Information* **2020**, *11*, 273. [CrossRef]
20. Baroos, M.L.; Marinos, L.; Patseas, L. *ENISA Threat Landscape for 5G Networks*; European Union Agency for Cybersecurity: Athens, Greece, 2020.
21. Hernan, S.; Lambert, S.; Ostwad, T.; Shostack, A. Threat Modeling—Uncover Security Design Flaws Using The STRIDE Approach. *MSDN Mag.* **2006**, 68–75.
22. Køien, G.M. On Threats to the 5G Service Based Architecture. *Wirel. Pers. Commun.* **2021**, *119*, 97–116. [CrossRef]
23. Madi, T.; Alameddine, H.A.; Pourzandi, M.; Boukhtouta, A. NFV security survey in 5G networks: A three-dimensional threat taxonomy. *Comput. Netw.* **2021**, *197*, 108288. [CrossRef]
24. Lichtman, M.; Rao, R.; Marojevic, V.; Reed, J.; Jover, R.P. 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation. In Proceedings of the 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 20–24 May 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
25. Nasralla, M.M.; García-Magariño, I.; Lloret, J. Defenses against perception-layer attacks on iot smart furniture for impaired people. *IEEE Access* **2020**, *8*, 119795–119805. [CrossRef]
26. Khan, M.A.; Nasralla, M.M.; Umar, M.M.; Khan, S.; Choudhury, N. An Efficient Multilevel Probabilistic Model for Abnormal Traffic Detection in Wireless Sensor Networks. *Sensors* **2022**, *22*, 410. [CrossRef]
27. Sattar, D.; Vasoukolaei, A.H.; Crysdale, P.; Matrawy, A. A STRIDE Threat Model for 5G Core Slicing. In Proceedings of the 2021 IEEE 4th 5G World Forum (5GWF), Montreal, QC, Canada, 13–15 October 2021.

28. Shevchenko, N.; Chick, T.A.; O'Riordan, P.; Scanlon, T.P.; Woody, C. *Threat Modeling: A Summary of Available Methods*; Technical Report; Carnegie Mellon University Software Engineering Institute: Pittsburgh, PA, USA, 2018.
29. Zografopoulos, I.; Ospina, J.; Liu, X.; Konstantinou, C. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access* **2021**, *9*, 29775–29818. [CrossRef]
30. Borgaonkar, R.; Hirschi, L.; Park, S.; Shaik, A. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. *Proc. Priv. Enhancing Technol.* **2019**, *2019*, 108–127. [CrossRef]
31. Ahmad, I.; Suomalainen, J.; Huusko, J. 5 G-Core Network Security. In *Wiley 5G Ref: The Essential 5G Reference Online*; Wiley: Hoboken, NJ, USA, 2019; pp. 1–18.
32. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet Things J.* **2019**, *6*, 8169–8181. [CrossRef]
33. Kim, H. 5G core network security issues and attack classification from network protocol perspective. *J. Internet Serv. Inf. Secur.* **2020**, *10*, 1–15.
34. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **2018**, *78*, 680–698. [CrossRef]
35. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A.; Invernizzi, L.; Kallitsis, M.; et al. Understanding the mirai botnet. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 16–18 August 2017; pp. 1093–1110.
36. Li, X.; Samaka, M.; Chan, H.A.; Bhamare, D.; Gupta, L.; Guo, C.; Jain, R. Network slicing for 5G: Challenges and opportunities. *IEEE Internet Comput.* **2017**, *21*, 20–27. [CrossRef]
37. Cunha, V.A.; da Silva, E.; de Carvalho, M.B.; Corujo, D.; Barraca, J.P.; Gomes, D.; Granville, L.Z.; Aguiar, R.L. Network slicing security: Challenges and directions. *Internet Technol. Lett.* **2019**, *2*, e125. [CrossRef]
38. Zhang, H.; Liu, N.; Chu, X.; Long, K.; Aghvami, A.H.; Leung, V.C. Network slicing based 5G and future mobile networks: Mobility, resource management, and challenges. *IEEE Commun. Mag.* **2017**, *55*, 138–145. [CrossRef]
39. Francois, F.; Abdelrahman, O.H.; Gelenbe, E. Towards assessment of energy consumption and latency of LTE UEs during signaling storms. In *Information Sciences and Systems 2015*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 45–55.
40. Ouziel, N. Top 10 Cyber Threats to Private 5G/LTE Networks. 2020. Available online: https://www.firstpoint-mg.com/blog/top-10-cyber-threats-to-private-5g-lte-networks/ (accessed on 13 January 2022).