Cyber Security Threats for 5G Networks

Jaya Preethi Mohan[1], Niroop Sugunaraj[2], Prakash Ranganathan[3]
School of Electrical Engineering and Computer Science (SEECS), University of North Dakota

2022 IEEE International Conference on Electro Information Technology (eIT) | 978-1-6654-8009-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/eIT53891.2022.9813965

Abstract— The fifth-generation mobile network (5G) services have the potential to provide high-speed connectivity to a large user base with excellent benchmarks on low latencies, large capacity, and faster upload/download data rates. The potential for millimeter-wave technologies to sustain enough power for mobile/Wi-Fi connectivity for indoor/outdoor applications provides an additional layer of expansion of 5G services to enhance good user experiences. The probability of threat landscape increases with a significant increase in network connectivity, users, non-existent or non-compliant Internet of Things (IoT) standards, and service types. Network mobility and applications that are planning on deploying 5G services such as Vehicle to Vehicle (V2V), Vehicle to Everything (V2X), Vehicle or Building to Infrastructure (V2I/B2I) Augmented and Virtual Reality (AR/VR), digital twins-based and streaming video services increase vulnerabilities and risk landscape compromising Confidentiality, Integrity, and Availability (CIA) properties. This paper provides a high-level categorization of cyber attacks related to 5G environment into Physical, Remote, and Local. The various benchmarks (latency, bandwidth) for 5G network evaluation across multiple 5G related technologies such as Enhanced Mobile Broadband (eMBB), Massive Machine Type Communication (mMTC), Ultra-Reliable Low Latency Communications (URLLC) are outlined.

Keywords— The Fifth Generation (5G) Network, cyber security, cyber threat, supply chain security, telecommunication threats, eMBB, mMTC, URLLC.

I. Introduction

Rapid demand for bandwidth and high mobile traffic burdening existing 3G/4G network performance to be slower and unreliable to many new emerging services. 5G was introduced by the 3rd Generation Partnership Project (3GPP) to expand the quality of services (QoS) and enhance user experiences. It is designed to support a larger number of networks connected devices with high data volume, and low latencies than 4G network [1]. Fig. 1 represents the different download speeds of the recent 3 cellular network generations [2].

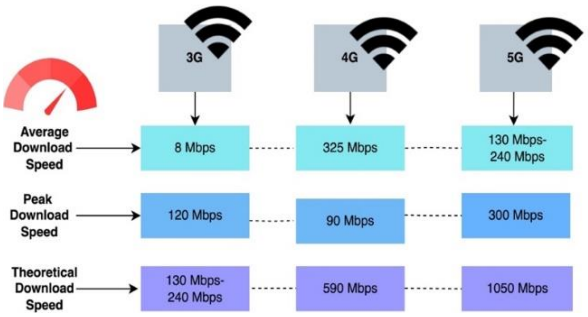

Fig. 1. Download speeds for 3G, 4G, and 5G.

5G can have a download speed is as high as 20 Gbps. Fig. 2 shows the network architecture of the fifth-generation network [3]. In 5G network, the devices such as smartphones are connected through an important part of a cellular network infrastructure called Radio Access Network (RAN) that allows integrating and improving the network utilization of mobile devices [4]. Device to device (D2D) communication is a "network of networks" in which multiple networks are integrated for data services and network communication over radio access technologies [5].

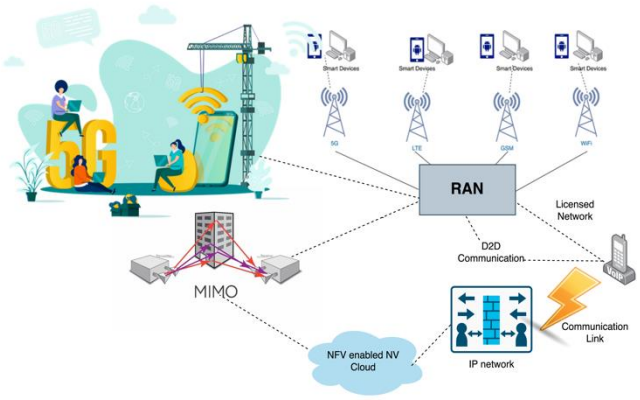

Fig. 2. 5G network architecture.

All of the connection types in 5G network are linked to multiple input multiple output (MIMO), which is a technology to multiply the capacity of radio link by relying on arrays of transmission and receiving antennas to exploit multi-path propagation [6]The network architecture comprises of three different layers: *infrastructure, control, and application* layers. Each layer differs by the type of component placements and varying degree of functionalities. The connectivity components like routers, switches, and base stations are placed in the *infrastructure* layer. The control layer implements the decision-making entities and network control function that is integrated into the application layer. Network services are utilized, and business applications are executed in the application layer [7].

Massive machine-type communication (mMTC) is a communication carried by machine or software platforms for coordinating, sensing, and actuation that are not operated by humans [8]. 5G can reduce the MTC latencies to 1 millisecond (ms) between wireless devices. This is a significant improvement from the latencies of 50 ms and 60 ms for 3G and 4G technologies respectively [9] Machine-type communication enables 5G services to operate securely, reliably and autonomously [10]. AT&T and FirstNet network organizations collaborated to provide public safety or emergency responder-based services using 5G networks [7]. AT&T also experimented several trials using milli-meter-wave (mmWave) technology in Austin, Texas to evaluate network capacity, speed, and latency [11].

[1]Email: jayapreethi.mohan@und.edu
[2]Email: niroop.sugunaraj@und.edu
[3]Email: prakash.ranganathan@und.edu

978-1-6654-8009-3/22/$31.00 ©2022 IEEE

Table 1 highlights the global trends or incidents in the 5G space, observed or predicted consequences, and quantitative findings/projections for the respective trend. The major security issues currently being faced by 5G network operators are supply chain weaknesses, espionage of 5G technology's corporate secrets, high-scale deployment of edge devices, and vulnerabilities in network functions (NFs) such as network slicing.

Table 1. Notable 5G security trends.

Threats/Trend	Consequence(s)	Significance	Reference
4G and 5G Vodafone Networks Exploited by Hackers	**Disruption and Shut Down** of Networks and Network Resources.	4,000,000 Affected for 24+ Hours.	[12], [13]
Cyber Espionage by State Sponsored Cyber Groups Targeted at Telecom Providers	**Data Espionage** of Sensitive or Classified Information	23 Telecom Providers Compromised Across 3 Continents	[14]
High Volume Deployment of Internet of Things (IoT) Devices	Compromised Devices Susceptible to **DDoS and SCA Attacks**	1 Million Devices Projected per Unit Area	[15][16]
Improper Separation of Network Slices using Cloud Technology	**Cloud-based** Vulnerabilities are Transferred to Network Slices	-	[17]
Major Suppliers of Telecom Equipment are Based in China	**Vulnerabilities and Backdoors** for Remote Monitoring	70% of the Chinese Telecom Market is State-owned	[18]

II. 5G Network Requirements and Services

According to ITU-R, 5G comprises of three major services: Enhanced Mobile Broadband (eMBB), Massive Machine Type Communications (mMTC), and Ultra-Reliable and Low Latency Communications (URLLC). Each service supports 5G in various prospective for efficient usage of network resources [19].

A. Enhanced Mobile Broadband (eMBB)

Next-Generation Network (NGN) aims to build a network combining different wireless networks in a complex structure for wide broadband usage. The Long-Term Evolution (LTE) network is the current technology for mobile data communication. LTE is a standardized network that supports 5G services with low latency and high broadband capacity. The eMBB aids in faster data rates (20 Gbps), low latency (in the order of 7 ms), and enhanced user experiences [19][20]. It offers support to various multimedia streaming environments such as augmented reality (AR), virtual reality (VR) technologies, and high-definition video streaming.

B. Massive Machine Type Communication (mMTC)

mMTC aids in the advancement of IoT technology and enables the realization of smart cities, smart grids, autonomous vehicles, smart buildings, transportation, and precision agriculture environments. It also provides low power consumption and high reliability. mMTC can support upto ten years of battery life with a single charge and a coverage density of a million devices in a single sq. kilometer [21]mMTC is applicable in IoT for sensors, transport systems, smart city, manufacturing, and staff control areas.

C. Ultra Reliable Low Latency Communication (URLLC)

URLLC is one of the major services of communication for packet delivery and data transmission. There are strong network requirements such as availability, reliability, and latency for this communication service. The typical applications of URLLC are those in the automation, vehicular communication, and manufacturing sectors. URLCC is fast and can transmit data consistently that are suitable for transportation, manufacturing, and healthcare applications with low probabilities of error (10^{-5} and 10^{-8}) and latency under 3 ms [22][23].

III. 5G Spectral Band Specifications

The spectral bands can be grouped into licensed and unlicensed bands. The radio spectrum band is an important allocation that separates critical (military) and non-critical (civilian) applications for growing wireless communication needs. Telecommunication operators provide high band to a service with broad coverage, selecting appropriate channel coding and high-speed network for many users [24]. 5G produces its own agility and new range of flexibility to satisfy user needs on connectivity and service capability.

a) eMBB Radio Band

Band level: Low-band
The frequency range coverage is extensive in the low-band spectrum of a 5G network. This radio band of eMBB is suitable for the regions that are densely populated or urban environment. The download speed of a low-level radio band is 20 Gbps and 20 times latency network. eMBB is preferred in streaming applications that demand high data rates
Examples of applications include: AR/VR, private broadband services, and high-definition video streaming.

b) URLLC Radio Band

Band level: Mid-band
URLLC services use mid-band spectrum which can support mission-critical systems, services or applications. The end-to-end latency for this band is less than 5ms and it has a 99.9% uptime. Applications for this band include:
Vehicle-to-everything (V2X), automated vehicles, smart grid, unmanned aviation, remote medical procedures, and industry automation.

c) mMTC Radio Band

Band level: High-band
mMTC Radio band is suitable for IoT based applications or devices. This band is suitable to realize applications such as

smart cities, smart grids, smart homes, etc., where there is a need for large collection of low powered embedded sensors or devices need to be connected and supported for network communication [22].

IV. POTENTIAL CYBER ATTACKS

Cyber security properties such as confidentiality, integrity, and availability (CIA) of 5G networks require multi-layered authentication to thwart threats. Cyber threats to 5G infrastructure can broadly be classified into two attack types: passive and active. Passive attacks such as eavesdropping and traffic analyses [25] do not intervene in a network's traffic to modify, insert, or delete data but passively monitor the data being transferred; they do not alter the system states or data [26].

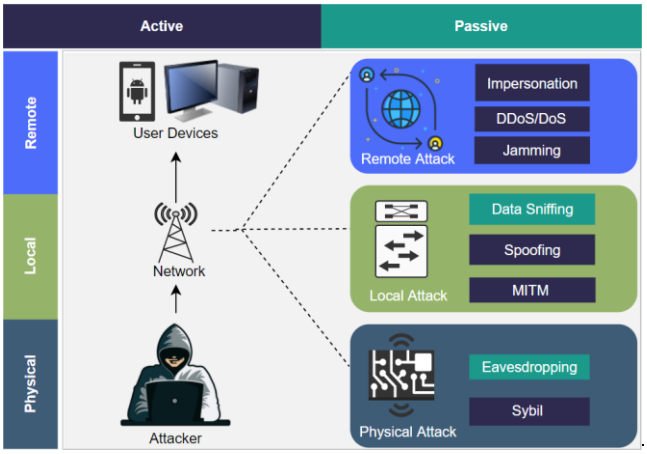

Fig. 3. Cyber threat categories: physical, local, and remote.

Active attacks like jamming, sybil, spoofing, impersonation, man-in-the-middle, and denial of service are carried out to alter systems and their data by compromising the integrity, confidentiality, and availability to cripple operational systems, and to steal or manipulate valuable data. The authors have grouped the potential cyber-attacks into possible likelihood of occurrence and its impact on 5G services. This paper categorizes attacks as follows (please see Fig. 3):

A. Remote Attacks
B. Local Attacks.
C. Physical Attacks.

A. Remote Attacks

- Vulnerabilities in the General Packet Radio Service Tunneling Protocol (GTP), can be exploited by remote threat actors to impersonate users using details such as authentication status, location, and subscriber settings [27]The likelihoods and the associated consequences of remote attacks (i.e., impersonation, DoS/DDoS, jamming) are medium-high as they primarily compromise the availability of a 5G network.
- DDoS and DoS attacks can be launched by a malicious NF against a legitimate NF as there is no authentication mechanism to verify the identity of a NF [28].
- Jamming is an attack that disrupts the signal of the physical devices from input and output transmission. mMTC Scenario: Data transmission in IoT terminals [29].
- Jammers use wireless and cellular 5G networks to attack critical infrastructures and public safety services. Several types of jammers [30] and jamming techniques [31] can be used to attack 5G networks.

B. Local Attacks

- Local area network (LAN) and wireless local area network (WLAN) can be accessed with an open base station through unauthorized users on the network [32]. The likelihoods and associated consequences of local attacks (i.e., data sniffing, spoofing, man-in-the-middle) are medium-high.
- Smart grid applications and network slicing [33] are scenarios that can be exploited.
- A man-in-the-middle attacker can create a fake 5G base station to act as a relay between the user and the 5G core network to intercept sensitive information [34][35].
- Local area network (LAN) and wireless local area network (WLAN) can be accessed with an open base station through unauthorized users on the network [32].

C. Physical Attacks

- Physical attacks refer to damage to property or people, where an intruder (or a malicious actor) takes control of key sensing, or communication or a control equipment. The likelihoods of such attacks and their associated consequences can be considered low-medium. Some common examples for this attack type include: eavesdropping, tampering of physical environment (i.e., cellular towers or associated equipment), and sybil.
- In eavesdropping, an attacker's intercept and analyze the communication traffic without altering any communication link, there by affecting privacy. At a later stage, the attacker may use this process to tamper, or progressively launch local and remote attacks. Mitigation solutions to prevent such attack types are limited and warrant further research [37]. In Sybil attack, malicious actors create fake identities and then proceed to inject false data to gain physical access to the network.
- According to Rahimi and colleagues [36], sybil attacks can be carried out at the connectivity layer that handles the device-network communication or at the physical device layer. Consequences of sybil attacks can propagate to upper layers such as the network management layer that use network function virtualization (NFV) and software defined networks (SDNs).

Based on the extensive literature review, the authors subjectively assess risks levels in terms of Likelihood of Occurrence of Attack (LOA) and its consequence or impact to affect certain 5G service as outlined in Table 2. LOA is shown in arrows (up, down, or double sided) and consequence of attack on a service is categorized as high, low, or medium.

Table 2. Potential cyber threat vectors for 5G networks.

Attack Type and Description	Attack and Loss of CIA Property	Remark(s)	Impacted Service(s)	LOA/ Consequence	References
Remote Attack: Attacks initiated wirelessly or through the Internet	Impersonation (Confidentiality & Integrity)	a) Openness of a wireless channel allows the attacker to perform remote attacks by tracking and controlling the communication channel.	eMBB Scenario: Falsification in network slicing	↔/ Medium	[25][38] [39], [40][41]–[43]
		b) Impersonation attacks can be carried out even without prior knowledge of a user's credentials or if an adequate authentication mechanism is not implemented.	mMTC Scenario: Access denial of legitimate user(s)		
	DDoS/DoS (Availability)	a) High bandwidth and low latency of 5G increase the likelihood of DDoS attacks.	eMBB Scenario: Access denial in network slicing.	↑/ High	[32] [44] [30][37][34] [45], [46] [47], [48][49][50][51]
		b) DDoS attackers target central control units to scale the attack to large servers or networks. This is carried out on the network layer to stop the user services.			
		c) Combination of DDoS and DoS can attack virtual NFs to disrupt host services network.			
	Jamming (Availability)	Jammers use wireless and cellular 5G networks that are majorly implemented in public safety services. Several types of jammers exist for attacking 5G networks.	Scenario: Jamming on IoT devices.	↓/ High	
Local Attack: Attacks within local area networks (LANs)	Data Sniffing (Confidentiality & Integrity)	a) Data sniffing takes place in the virtual local area network (VLAN) of link-layer within LANs.	URLLC Scenario: Smart grid applications and network slicing.	↔/ Low	[22][33] [34][35][52] [29] [53]–[55][46], [56], [57]
	Spoofing (Confidentiality & Integrity)	b) LAN and WLAN can be accessed with an open base station through unauthorized users on the network.		↑/ Medium	
	Man-in-the-Middle (MITM) (Confidentiality & Integrity)	c) User messages are tracked by monitoring communication channels.	URLLC Scenario: IP spoofing.	↔/ High	
		d) The communication data between two legitimate parties are replaced or modified by attackers to obtain confidential data.			
Physical Attack: Attacks requiring physical hardware access	Eavesdropping (Confidentiality & Integrity)	Eavesdropping attacks may happen on the physical layer of the 5G network by intercepting and analyzing traffic to access confidential data (i.e., identity, authentication credentials, location).	eMBB Scenario: SDN and IoT device.	↔/ Low	[58] [30][35] [59][60] [61] [62] [63][64] [65][66][67]
	Sybil (Integrity)	Sybil attacks create fake identities and inject false information to get and maintain access to a physical device.	mMTC Scenario: Data transmission in IoT terminals and Vehicular control.	↓/ Medium	

V. Cyber and non-cyber Risks in 5G networks

5G poses serious cyber risks (if not addressed) regardless of the spectrum band usage in any network type. A recent US Department of Defense (DoD) report shows that the code used for the base station is secure and permitted for telecommunication vendors to access, but the network infrastructure or security equipment (firewalls or routers) is vulnerable to anonymous activity as they come from third-party vendors. Lack of regular maintenance or software updates or patches could expose new vulnerabilities within the infrastructure [36][28]. 5G networks are not only vulnerable to risks that compromise the CIA properties of the infrastructure and communicating parties, but also bring concerns related to power consumption, and supply chain vulnerabilities.

5G network capability plan to support tens of billions of IoT devices worldwide and 7.6 billion smartphone users in the next decade. 5G's network power consumption will exceed exponentially although bits per kilowatt (kW) remains lesser. With the penetration of several small cell technologies, the user capacity demand is to going to surge to accommodate large users and energy or vehicular/building infrastructure networks (V2X, V2I). As portable small cell networks may rely on chargeable lithium-ion batteries, relying on conventional fossil fuel-based electricity is not sufficient. Thus, portable and scalable renewable energy resources are required to address power generation and resource efficiency [68]. Power consumption rates have gradually increased from 3G, 4G, and 5G: there was a 43% increase of power consumption from 3G (4808 W) to 4G (6877 W) and a 68% increase from 4G to 5G (11,577 W) [69]. A significant part of 5G's user equipment (UE) will consist of IoT devices and side-channel attacks (SCA) based on power characteristics pose a threat to user privacy. Timing-based side channel attacks [70] analyze the interference produced during regular device traffic to identify patterns in device behavior. These attacks can probe deeper to gather data such as device type, device-user interactions, and the no. of people using the device(s). Another type of SCA called profiled SCA is regarded as the most dangerous type of SCA as it assumes that a threat actor has access to a cloned IoT device [71].

Supply-chain components used in the development of 5G infrastructure and the policies/standards that are meant to ensure minimum performance and reliability requirements can indirectly or directly contribute to the exploitation of 5G networks. According to CISA's 5G Strategy [72] for the United States, there is a strategic initiative to ensure that "state-influenced" entities do not dominate the 5G market partially because the low upfront costs associated with the procurement and deployment of 5G components will snowball into long-term expenses that will inevitably have to address security flaws in 5G's hardware and software architecture. A report from ETH Zurich [73] highlights the importance of a comprehensive analysis of 5G equipment before deployment. This is due to the economic power shift in the manufacturing of 5G equipment from the US to other countries like China. The UK National Cybersecurity Centre (NCSC) reports that Huawei performs poorly due to sub-par software source codes that are rife with software bugs. Further investigation points out that this observation is not specific to Huawei; European manufacturers like Ericsson and Nokia are also noted for having software vulnerabilities in 5G equipment that can be exploited by malicious actors.

VI. 5G Threat surfaces

5G, at its inception, was expected to build upon existing 3G and 4G/4G (LTE) infrastructure to provide low latency and high-speed services to applications in transportation, aviation, automotive, and energy domains. However, 5G can be exploited by its threat surfaces. A threat surface, as defined by the National Institute of Standards and Technology (NIST) [74], consists of "the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment." For example, disruption to aviation services due to 5G services are emerging and causing mass schedule changes and cancellations. According to FAA [75], as 5G infrastructure uses new frequencies, increased power levels, and warrants closer proximity of flight operations, existing aviation equipment's (e.g., radio altimeter equipment closer to antennas) are noticing disruptions to airport operations, and thus warrants restrictions. Such equipment's could also be attacked by a hacker through side channel attacks by emulating "potential cyber-attacks" as disruptions through any of the attack type (Physical, Local, or Remote) categories. Similar threats exist to other critical infrastructures such as U.S. Power Grid assets [76] (i.e., transmission/distribution lines, substations, circuit breakers, relays, phasor measurement units, Distributed Energy Resource (DER's) controllers), Gas Pipeline Networks (e.g., pumping stations/junctions, switches), and Water/Sewage or Storm Treatment Systems (e.g., key interconnect units or switches). Several IoT devices are being manufactured with no cybersecurity measures and provide several backdoors for vulnerabilities (e.g., man-in-the-middle attacks) to exist. This section classifies three threat surfaces to 5G infrastructure: hardware, operations, and network as shown in Fig. 4.

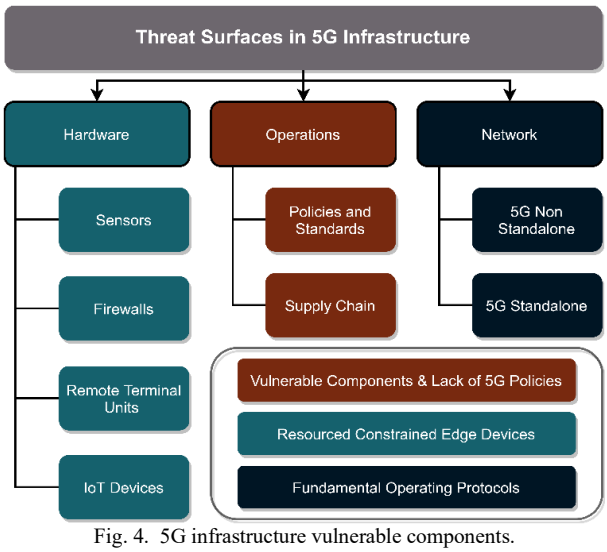

Fig. 4. 5G infrastructure vulnerable components.

A. **Hardware**. The hardware threats can be characterized by endpoint devices such as remote terminal units (RTUs), firewalls, sensors, and power infrastructure. These devices

can be considered part of 5G's hardware ecosystem and rely on 5G services to provide improved and more reliable performance. Additionally, 5G moves its core functions like data storage to edge devices and sub-systems like those within autonomous vehicles in the V2X paradigm to introduce additional attack surfaces [77]. 5G infrastructure is being integrated with current 4G LTE networks [78] and is susceptible to attack vectors such as distributed denial of service (DDoS). Soldani [79] lists assets (anything that is of value to an organization or an individual) in the 5G system, such as firewalls, radio access networks (RAN), and UE to be vulnerable to cloning, hijacking internet of things (IoT) devices to create botnets, and international mobile subscriber identity (IMSI) catching.

B**. Operations.** Operations-side processes include supply chain components used in the design of 5G infrastructure and its policies or standards that are meant to ensure minimum performance and reliability requirements. The Cybersecurity Infrastructure and Security Agency (CISA) [80] highlights the risk of purchasing and deploying components produced by international suppliers: risks such as the insertion of malware and backdoors, and manipulation of sensitive components can expose a nation's broader 5G network to attack vectors. While manufacturers such as Intel, MediaTek, Huawei, and Qualcomm have most of the market share when it comes to proprietary 5G-compatible hardware, it compels customers and vendors to implement features within these technologies that are not standardized by policies and are thus optional. This could introduce new vulnerabilities or attack vectors in the client networks that may be specific to manufacturers.

C. **Network.** According to Positive Technologies [81], most 5G deployments in 2020 were non-standalone (NSA) and used the Diameter protocol (also called Diameter Signaling protocol) and GTP). Diameter is used to exchange subscriber profile information such as location updates, subscriber data, voice, or video sessions, user authentication, quality of service, and mobility requirements. Diameter is an industry-standard protocol used in 4G LTE networks for authentication, authorization, and accounting (AAA) purposes while GTP is used primarily to "tunnel" or route internet protocol (IP) packets initiated from a source IP address (mobile device) to a destination IP address (target webserver) through the cellular network's core segment. Both these protocols have open vulnerabilities that can be exploited. The 5G standalone (SA) architecture accommodates multiple features such as a distributed cloud-based core network, SDN and NFV, and multi-access edge computing (MEC) [15]. While these features offer multiple benefits, security issues can lead to unauthorized access, configuration errors, and exposure to third party vulnerabilities.

VII. Countermeasures

Based on findings in Section IV, the following cyber attacks pose as threats to 5G deployments, namely: impersonation, DoS/DDoS, sybil, eavesdropping, data sniffing, man-in-the-middle, spoofing, and jamming. Table 3 summarizes the countermeasures and subclassifies them as either a prevention or mitigation tactic. Prevention tactics are implemented before the network has been subject to a cyber attack whereas mitigation measures lessen the implications of a cyber attack. Rosenblatt [82] from the Yale Cyber Leadership Forum advises the regular application of "stress-tests": tests that simulate attacks such as DoS/DDoS at various threat surfaces of a 5G network to assess the magnitude of these attacks and implement adequate backup measures.

Table 3. Countermeasures for cyber attacks on 5G networks.

Attack	Countermeasures	Prevention (P)/ Mitigation (M)	Reference
DoS/DDoS	Setting thresholds for transmitted traffic, stress tests, and adequate capabilities to handle peak network requests	P/M	[83][82]
Spoofing	Timing blacklists, authentication mechanisms	P/M	[84]
Man-in-the-middle	Access control policies, symmetric/asymmetric encryption	P	[85]
Jamming	Channel monitoring, jammer timing patterns, relay schemes	P/M	[30]
Eavesdropping and Data Sniffing	Hardware modules (eSIM), symmetric/asymmetric encryption	P	[83][86] [87]
Sybil	Blockchain networks prevent the creation of multiple fake identities, certifying authority to verify identities	P	[88][89]

Spoofing attacks can be mitigated by setting a countermeasure that prevents any suspicious agent from accessing 5G functions. timers can be used to blacklist certain agents from accessing the network if there is no response after predefined periods [84]. Additionally, there should be tactics in place that ensure that the participating parties (base stations and end devices) are legitimate prior to initiating cellular connections and executing certain procedures. Man-in-the-middle attacks can be countered by enforcing adequate access control measures to prevent unauthorized modification [85]. Ensuring that data are encrypted by a strong public key infrastructure (PKI) mechanism will protect relayed data from being decrypted by a man-in-the-middle attacker. Jamming attacks can be detected by monitoring the network for any excess or sudden change in a specific 5G channel by metrics such as bit error rate and setting thresholds to distinguish normal and anomalous channel behaviors. Eavesdropping and data sniffing attacks can be mitigated by using encrypted network data [83]. To complement this measure, it is advised to assign encrypted temporary identities to connecting devices and regularly update this information to prevent user tracking. Preventing sybil attacks

primarily involve methods to ensure the legitimacy of the participants in the network. According to Coin Central [88], using a blockchain to increase the cost associated with creating identities in a 5G network will limit the number of fake or malicious users executing a sybil attack.

VIII. Conclusion

This paper provides a review of potential cyber attacks into three categories: Physical, Remote, and Local. Further, several threat vectors can also be classified into Hardware, Operations, and Network types. As demand for more spectrum will surge, it is natural for the cyber threat landscape to grow. Telecommunication companies and network providers have begun to deploy 5G services and it is important to assess the security exploitations early on across the three categories to avoid expensive re-design/re-installations of 5G infrastructure that may hinder both critical (i.e., energy, aviation, water/sanitary systems, and transportation networks), and non-critical (user authentication and privacy challenges) infrastructures. Futuristic mitigation solutions (e.g., blockchain, encryption mechanisms, multi-layered credential or policy authentication, access privileges to key resources) should be carefully designed and must be robust to track and deter threats as this technology is new and evolving,

ACKNOWLEDGMENTS

The authors acknowledge the support from Grand Forks County's Resilience Study (Grant Award # UND0026784) to carry out this work.

References

[1] H. Fourati, R. Maaloul, and L. Chaari, *A survey of 5G network systems: challenges and machine learning approaches*, vol. 12, no. 2. Springer Berlin Heidelberg, 2021. doi: 10.1007/s13042-020-01178-4.

[2] E. O'Connell, D. Moore, T. N.- Telecom, and undefined 2020, "Challenges associated with implementing 5G in manufacturing," *mdpi.com*, Accessed: Feb. 27, 2022. [Online]. Available: https://www.mdpi.com/2673-4001/1/1/5

[3] A. Gupta, R. J.-I. access, and undefined 2015, "A survey of 5G network: Architecture and emerging technologies," *ieeexplore.ieee.org*, Accessed: Feb. 27, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7169508/

[4] A. Gudipati, D. Perry, L. E. Li, and S. Katti, "Softran: Software defined radio access network," *HotSDN 2013 - Proceedings of the 2013 ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, pp. 25–30, 2013, doi: 10.1145/2491185.2491207.

[5] M. Höyhtyä, O. Apilo, and M. Lasanen, "Review of latest advances in 3GPP standardization: D2D communication in 5G systems and its energy consumption models," *Future Internet*, vol. 10, no. 1, 2018, doi: 10.3390/fi10010003.

[6] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186–195, 2014, doi: 10.1109/MCOM.2014.6736761.

[7] J. A. Khan and M. M. Chowdhury, "Security Analysis of 5G Network," *IEEE International Conference on Electro Information Technology*, vol. 2021-May, pp. 1–6, 2021, doi: 10.1109/EIT51626.2021.9491923.

[8] A. Osseiran, J. F. Monserrat, and P. Marsch, *5G mobile and wireless communications technology*. 2016. doi: 10.1017/CBO9781316417744.

[9] V. G. Nguyen, K. J. Grinnemo, J. Taheri, and A. Brunstrom, "A Deployable Containerized 5G Core Solution for Time Critical Communication in Smart Grid," *2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops, ICIN 2020*, no. Icin, pp. 153–155, 2020, doi: 10.1109/ICIN48450.2020.9059397.

[10] J. Li, K. Nagalapur, E. Stare, … S. D. preprint arXiv, and undefined 2021, "5G New Radio for Public Safety Mission Critical Communications," *arxiv.org*, 2021, Accessed: Feb. 27, 2022. [Online]. Available: https://arxiv.org/abs/2103.02434

[11] M. Patzold, "The Benefits of Smart Wireless Technologies [Mobile Radio]," *IEEE Vehicular Technology Magazine*, vol. 12, no. 4, pp. 5–12, 2017, doi: 10.1109/MVT.2017.2753080.

[12] N. Goud, "https://www.cybersecurity-insiders.com/cyber-attack-disrupts-vodafone-portugal-entire-4g-and-5g-network/," *Cybersecurity Insiders*, 2022. [Online]. Available: https://www.cybersecurity-insiders.com/cyber-attack-disrupts-vodafone-portugal-entire-4g-and-5g-network/

[13] J. Greig, "Vodafone Portugal hit with cyberattack affecting 4G/5G network, TV, SMS services," *ZDNet*, 2022. [Online]. Available: https://www.zdnet.com/article/vodafone-portugal-hit-with-cyberattack-affecting-4g5g-network-tv-sms-services-and-more/

[14] D. Palmer, "Hackers are targeting telecom companies to steal 5G secrets," *ZDNet*, 2021. [Online]. Available: https://www.zdnet.com/article/hackers-are-targeting-telecoms-companies-to-steal-5g-secrets/

[15] H. Kim, "5G core network security issues and attack classification from network protocol perspective," *Journal of Internet Services and Information Security*, vol. 10, no. 2, pp. 1–15, 2020, doi: 10.22667/JISIS.2020.05.31.001.

[16] D. Goodin, "Microsoft catches Russian state hackers using IoT devices to breach networks," *ArsTechnica*, 2019. https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/

[17] A. Jain and T. Singh, "Implementing Security in I O T Ecosystem Using 5G Network Slicing and Pattern Matched Intrusion Detection System : A Simulation Study," vol. 16, pp. 1–38, 2021.

[18] K. Zerrusen, G. Sachs, and C. Council, "The National Security Challenges of Fifth Generation (5G) Wireless Communcations. Winning the Race to 5G, Securely," no. June, 2019, [Online]. Available: https://www.insaonline.org/wp-content/uploads/2019/06/INSA_WP_5G_v5_Pgs.pdf

[19] A. Kostopoulos *et al.*, "Use cases and standardisation activities for eMBB and V2X scenarios," *2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings*, 2020, doi: 10.1109/ICCWorkshops49005.2020.9145377.

[20] A. A. Ateya, A. Muthanna, M. Makolkina, and A. Koucheryavy, "Study of 5G Services Standardization: Specifications and Requirements," *International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, vol. 2018-Novem, pp. 2–7, 2019, doi: 10.1109/ICUMT.2018.8631201.

[21] J. Blackman, "What is mMTC in 5G NR, and how does it impact NB-IoT and LTE-M," *Fundamentals*, 2019. https://enterpriseiotinsights.com/20191016/channels/fundamentals/what-is-mmtc-in-5g-nr-and-how-does-it-impact-nb-iot-and-lte-m

[22] C. Bockelmann, N. Pratas, G. Wunder, … S. S.-I., and undefined 2018, "Towards massive connectivity support for scalable mMTC communications in 5G networks," *ieeexplore.ieee.org*, Accessed: Feb. 27, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8360103/

[23] Z. Li, H. Shariatmadari, B. Singh, and M. A. Uusitalo, "5G URLLC: Design challenges and system concepts," *Proceedings of the International Symposium on Wireless Communication Systems*, vol. 2018-Augus, 2018, doi: 10.1109/ISWCS.2018.8491078.

[24] Cybersecurity and Infrastructure Security Agency, "Overview of Risks Introduced By 5G Adoption in the United States," pp. 1–16, 2019.

[25] S. V Swamy and P. R. R, "Study of Security for 5G Wireless Communication Network," no. July, pp. 3800–3802, 2020.

[26] National Institute of Standards and Technology (NIST), "Computer Security Resource Centre," *Glossary*, 2022. https://csrc.nist.gov/glossary/term/passive_attack

[27] Positive Technologies, "Cybersecurity 2020 - 2021," 2021. [Online]. Available:

https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cybersecurity_20-21.pdf
[28] AdaptiveMobile, "A Slice in Time," 2021. [Online]. Available: https://blog.adaptivemobile.com/5g-network-slicing-vulnerability-denial-of-service-attacks
[29] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019, doi: 10.1109/JIOT.2019.2927379.
[30] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, pp. 1010–1015, 2020, doi: 10.1109/CCWC47524.2020.9031175.
[31] JEM Engineering, "An Introduction to Jammers," 2019. [Online]. Available: https://jemengineering.com/blog-an-introduction-to-jammers/
[32] M. A. Hasnat, S. T. A. Rurnee, M. A. Razzaque, and M. Mamun-Or-Rashid, "Security Study of 5G Heterogeneous Network: Current Solutions, Limitations Future Direction," *2nd International Conference on Electrical, Computer and Communication Engineering, ECCE 2019*, pp. 7–9, 2019, doi: 10.1109/ECACE.2019.8679326.
[33] Q. Qiu, S. Liu, S. Xu, S. Y.-W. C. and Mobile, and undefined 2020, "Study on security and privacy in 5G-enabled applications," *hindawi.com*, Accessed: Feb. 27, 2022. [Online]. Available: https://www.hindawi.com/journals/wcmc/2020/8856683/
[34] A. Shaik, R. Borgaonkar, S. Park, and J. P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols : Exposing device capabilities," in *WiSec 2019 - Proceedings of the 2019 Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 221–232. doi: 10.1145/3317549.3319728.
[35] G. Sahu and S. S. Pawar, "Security Challenges in 5G Network," in *EAI/Springer Innovations in Communication and Computing*, 2022, pp. 75–94. doi: 10.1007/978-3-030-91149-2_4.
[36] H. Rahimi, A. Zibaeenejad, P. Rajabzadeh, and A. A. Safavi, "On the security of the 5G-IoT architecture," *ACM International Conference Proceeding Series*, 2018, doi: 10.1145/3269961.3269968.
[37] G. Holtrup, W. Lacube, D. P. David, A. Mermoud, G. Bovet, and V. Lenders, "5G System Security Analysis," no. August 2021, pp. 1–47, 2021, [Online]. Available: http://arxiv.org/abs/2108.08700
[38] I. ul haq, J. Wang, and Y. Zhu, "Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks," *Journal of Network and Computer Applications*, vol. 161, no. February, pp. 1–11, 2020, doi: 10.1016/j.jnca.2020.102660.
[39] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. J. P. C. Rodrigues, "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges and Future Research Roadmap," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3047895.
[40] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan, and J. H. Park, "Secure D2D communication for 5G IoT network based on lightweight cryptography," *Applied Sciences (Switzerland)*, vol. 10, no. 1, Jan. 2020, doi: 10.3390/app10010217.
[41] B. Yang, T. Taleb, Z. Wu, and L. Ma, "Spectrum Sharing for Secrecy Performance Enhancement in D2D-Enabled UAV Networks," *IEEE Network*, vol. 34, no. 6, pp. 156–163, Nov. 2020, doi: 10.1109/MNET.011.2000093.
[42] H. Huang, J. Chu, and X. Cheng, "Trend Analysis and Countermeasure Research of DDoS Attack under 5G Network," in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy, CSP 2021*, Jan. 2021, pp. 153–160. doi: 10.1109/CSP51677.2021.9357499.
[43] H. A. Alamri, V. Thayananthan, and J. Yazdani, "Machine Learning for Securing SDN based 5G Network," 2021.
[44] B. Ying, A. N.-J. of N. and C. Applications, and undefined 2019, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography," *Elsevier*, Accessed: Feb. 27, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804519300256?casa_token=Xy3pPlLZA9EAAAAA:NDImzMQqNHE7MDXqBU7Y-ADV1rJ84b1pWEQNouIZ3avmHg-dwQloAfcW8lzKdewEdAkGCQ
[45] M. Patzold, "The Benefits of Smart Wireless Technologies [Mobile Radio]," *IEEE Vehicular Technology Magazine*, vol. 12, no. 4, pp. 5–12, Dec. 2017, doi: 10.1109/MVT.2017.2753080.
[46] A. Gupta, R. K. Jha, P. Gandotra, and S. Jain, "Bandwidth Spoofing and Intrusion Detection System for Multistage 5G Wireless Communication Network," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 618–632, Jan. 2018, doi: 10.1109/TVT.2017.2745110.
[47] M. Awais Javed and S. khan Niazi, "5G Security Artifacts (DoS / DDoS and Authentication); 5G Security Artifacts (DoS / DDoS and Authentication)," 2019.
[48] P. Varga *et al.*, "5g support for industrial iot applications – challenges, solutions, and research gaps," *Sensors (Switzerland)*, vol. 20, no. 3, Feb. 2020, doi: 10.3390/s20030828.
[49] J. J.-2020 3rd I. I. C. on and undefined 2020, "Short survey on physical layer authentication by machine-learning for 5G-based Internet of Things," *ieeexplore.ieee.org*, Accessed: May 07, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9318879/
[50] Z. Zhang, N. Li, S. Xia, X. T.-2020 I. Wireless, and undefined 2020, "Fast cross layer authentication scheme for dynamic wireless network," *ieeexplore.ieee.org*, Accessed: May 07, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9120541/
[51] S. Wijethilaka, & M. L.-I. C. S., and undefined 2021, "Survey on network slicing for Internet of Things realization in 5G networks," *ieeexplore.ieee.org*, Accessed: May 07, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9382385/
[52] A. Gupta, R. Kumar Jha, S. Jain, and A. Professor in, "Attack modeling and intrusion detection system for 5G wireless communication network," *Wiley Online Library*, vol. 30, no. 10, Jul. 2016, doi: 10.1002/dac.3237.
[53] IEEE Communications Society and Institute of Electrical and Electronics Engineers, *2017 IEEE Conference on Standards for Communications and Networking (CSCN) : 18-20 Sept. 2017.*
[54] M. Geller and P. Nair, "Whitepaper Cisco Public 5G Security Innovation with Cisco," 2018.
[55] J. Kamasa, "Securing Future 5G-Networks," *Research Collection*, vol. 21, no. 6, pp. 12–19, 2020, [Online]. Available: https://doi.org/10.3929/ethz-a-010025751
[56] Institute of Electrical and Electronics Engineers, *2018 IEEE Global Communications Conference (GLOBECOM) : proceedings : Abu Dhabi, UAE, 9-13 December 2018.*
[57] A. S. Khan, Y. Javed, J. Abdullah, J. M. Nazim, and N. Khan, "Security issues in 5G device to device communication," 2017.
[58] J. Hasneen and K. M. Sadique, "A Survey on 5G Architecture and Security Scopes in SDN and NFV," 2022, pp. 447–460. doi: 10.1007/978-981-16-2008-9_43.
[59] M. Baza, M. Nabil, … M. M.-… on D. and, and undefined 2020, "Detecting sybil attacks using proofs of work and location in vanets," *ieeexplore.ieee.org*, Accessed: May 07, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9091099/
[60] IEEE Communications Society and Institute of Electrical and Electronics Engineers, *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).*
[61] S. Kwon, S. Park, H. J. Cho, Y. Park, D. Kim, and K. Yim, "Towards 5G-based IoT security analysis against Vo5G eavesdropping," *Computing*, vol. 103, no. 3, pp. 425–447, Mar. 2021, doi: 10.1007/s00607-020-00855-0.
[62] E. T. Saglam and S. Bahtiyar, "A Survey: Security and Privacy in 5G Vehicular Networks," in *UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering*, Sep. 2019, pp. 108–112. doi: 10.1109/UBMK.2019.8907026.
[63] M. Baza *et al.*, "Detecting Sybil Attacks Using Proofs of Work and Location in VANETs," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 39–53, 2022, doi: 10.1109/TDSC.2020.2993769.
[64] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks," 2006.

[65] J. M. Batalla *et al.*, "Security Risk Assessment for 5G Networks: National Perspective," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 16–22, Aug. 2020, doi: 10.1109/MWC.001.1900524.

[66] E. Sağlam, Ş. B.-2019 4th I. C. on, and undefined 2019, "A survey: Security and privacy in 5G vehicular networks," *ieeexplore.ieee.org*, Accessed: May 07, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8907026/

[67] S. Kwon, S. Park, H. J. Cho, Y. Park, D. Kim, and K. Yim, "Towards 5G-based IoT security analysis against Vo5G eavesdropping," *Computing*, vol. 103, no. 3, pp. 425–447, Mar. 2021, doi: 10.1007/S00607-020-00855-0.

[68] Q. Wu, G. Y. Li, W. Chen, D. Wing, K. Ng, and R. Schober, "An overview of sustainable green 5G networks," *ieeexplore.ieee.org*, 2016, Accessed: Feb. 27, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8014295/

[69] Huawei Technologies, "5G power whitebook," 2019, [Online]. Available: https://www.huawei.com/minisite/5g-ultra-lean-site-2019/pdf_v1.0/5G-power-cn.pdf

[70] N. Prates, A. Vergutz, R. T. MacEdo, A. Santos, and M. Nogueira, "A Defense Mechanism for Timing-based Side-Channel Attacks on IoT Traffic," *2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings*, 2020, doi: 10.1109/GLOBECOM42002.2020.9322070.

[71] S. Bhasin, A. Chattopadhyay, A. Heuser, D. Jap, S. Picek, and R. R. Shrivastwa, "Mind the Portability: A Warriors Guide through Realistic Profiled Side-channel Analysis," 2020, doi: 10.14722/ndss.2020.24390.

[72] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "CISA 5G strategy: Ensuring the security and resilience of 5G infrastructure in our nation 2020," pp. 1–24, 2020.

[73] J. Kamasa, "Securing Future 5G-Networks," *Research Collection*, vol. 21, no. 6, pp. 12–19, 2020.

[74] National Institute of Standards and Technology (NIST), "Computer Security Resource Centre," *Glossary*, 2022. https://csrc.nist.gov/glossary/term/passive_attack

[75] Federal Aviation Administration, "5G and Aviation Safety," *5G*, 2022. https://www.faa.gov/5g

[76] M. A. Ali and A. A. Mohamed, "5G Cellular Technologies for Supporting Future Power Grid Communication Networks," *IEEE Smart Grid*, 2016. [Online]. Available: https://smartgrid.ieee.org/bulletins/october-2016/5g-cellular-technologies-for-supporting-future-power-grid-communication-networks

[77] K. Mok, "In Defense of 5G: National Security and Patent Rights Under the Public Interest Factors," *The University of Chicago Law Review*, vol. 86, no. 1, pp. 77–142, 2019.

[78] Department of Homeland Security, "5G Introduces New Benefits, Cybersecurity Risks," *Science and Technology Directorate*, 2020.

[79] D. Soldani, "5G and the Future of Security in ICT," *2019 29th International Telecommunication Networks and Applications Conference, ITNAC 2019*, 2019, doi: 10.1109/ITNAC46935.2019.9078011.

[80] National Security Agency, "Potential threat vectors to 5G infrastructure," pp. 1–16, 2021.

[81] Positive Technologies, "Threat vector: GTP. Vulnerabilities in LTE and 5G Networks," 2020.

[82] E. Rosenblatt, "Cybersecurity in 5G," *Yale Cyber Leadership Forum*, pp. 1–6, 2021. [Online]. Available: https://cyber.forum.yale.edu/blog/2021/7/20/cybersecurity-risk-in-5g

[83] G. Horn and P. Schneider, "Towards 5G security," *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, vol. 1, pp. 1165–1170, 2015, doi: 10.1109/Trustcom.2015.499.

[84] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, "5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation," *2018 IEEE International Conference on Communications Workshops, ICC Workshops 2018 - Proceedings*, pp. 1–6, 2018, doi: 10.1109/ICCW.2018.8403769.

[85] F. Liu, J. Peng, and M. Zuo, "Toward a Secure Access to 5G Network," *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, pp. 1121–1128, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00156.

[86] GSM Association (GSMA), "Embedded SIM Remote Provisioning Architecture," pp. 1–113, 2020, [Online]. Available: https://www.gsma.com/esim/wp-content/uploads/2020/07/SGP.01-v4.2.pdf

[87] GSMA, "IoT Security Guidelines Overview," *IoT Security Guidelines*, vol. 2.2, 2020.

[88] B. Garner, "What's a Sybil Attack & How Do Blockchains Mitigate Them?," *Coin Central*, 2018. https://coincentral.com/sybil-attack-blockchain/

[89] J. R. Douceur, "The Sybil Attack," *Microsoft Research*, p. 259, 2002, doi: 10.1145/984622.984660.