Wiley
Security and Communication Networks
Volume 2024, Article ID 2883082, 23 pages
https://doi.org/10.1155/2024/2883082

WILEY

Review Article

An Extensive Classification of 5G Network Jamming Attacks

Shreya Savadatti, Sakshi Kuldeep Dhariwal, Shruthi Krishnamoorthy, and Radhakrishnan Delhibabu

Department of Computer Science and Engineering, Vellore Institute of Engineering, Vellore, India

Correspondence should be addressed to Radhakrishnan Delhibabu; rdelhibabu@vit.ac.in

Received 24 February 2024; Revised 18 May 2024; Accepted 22 May 2024

Academic Editor: Vincent O. Nyangaresi

The paper introduces a pioneering taxonomy for 5G jamming attacks, meticulously crafted through diverse research methodologies, including literature review, case studies, incident database analysis, and network architecture assessment. This taxonomy is based on six dimensions: attack classification, attack techniques, jammer characteristics, impact and target analysis, countermeasure strategies, and security layers. It gives a full picture of what is needed to protect 5G networks from new security threats, especially jamming attacks. Real-world case studies from regions like Ukraine, the South China Sea, and Cuba validate the taxonomy's efficacy in analyzing varied jamming scenarios and offer practical insights into cyber threats and mitigation strategies. By looking closely at attack details, network effects, countermeasure strategies, and security layers, this research makes a big difference in improving the security of 5G networks. It gives everyone involved, the tools and knowledge they need to protect themselves from jamming attacks and make networks more resilient in a world where technology and connectivity are changing quickly. The key findings of this research include identifying key 5G network vulnerabilities to jamming attacks and presenting a detailed six-dimensional taxonomy: attack classification, techniques, jammer characteristics, impact analysis, countermeasures, and security layers. It emphasizes the need for strong security strategies to improve 5G network resilience against evolving threats, which case studies from Cuba, the South China Sea, and Ukraine have validated.

1. Introduction

Consider a critical situation in which emergency personnel use 5G networks to coordinate a rescue mission. Suddenly, all communication is disrupted, and a malicious actor is jamming the signal. This scenario demonstrates the susceptibility of 5G networks to jamming attacks, which take advantage of their reliance on open-air communication. Unlike wired networks, 5G's reliance on radio waves renders it vulnerable to jamming attacks, which use this open communication channel to disrupt legitimate transmissions. To understand this vulnerability better, let us explore the concept of wireless network.

In its widest sense, a wireless network is any network that connects devices wirelessly, that is, without requiring any form of cable, by using radio waves, microwaves, or infrared waves, and this connection can be used to transmit data, giving users the desired mobility and ease. Decades of innovation have transformed wireless communications, culminating in the provision of high-speed mobile broadband services through the deployment of 4G long-term evolution (LTE) networks [1].

The fifth generation of wireless cellular networks, 5G, promises faster data rates and reliable service delivery. 5G's evolution towards high-speed, low-latency connectivity relies on millimetre-wave technology, small cell deployment, D2D communication, M-MIMO with beamforming, and other innovations for intelligent wireless systems [2]. D2D communication and IoT technologies, including smart sensors, RFID, and M2M, are pivotal components of 5G networks, with a focus on emerging IoT architectures suited for future-generation 5G systems [3]. There are many interesting things about 5G, such as the potentially disruptive move to the millimeter wave (mm-wave) spectrum, new market-driven ways to allocate and reassign bandwidth, and the significant virtualization currently underway in the core

network that may eventually extend to the edges. The emergence of a billion-strong "Internet of Things" (IoT) composed of varied devices, along with the growing integration of old and new cellular technologies, creates a complex communications landscape. As a result of the 5G public-private partnership, it is expected that 7 trillion things or devices will be connected, and service delivery time can be reduced from 90 hours to 90 minutes due to advanced privacy technology [4]. This fifth generation of wireless technology, which will support the development of new technologies like the Internet of Things (IoT), driverless cars, augmented reality, and much more, is set to revolutionize the way people live and work. A general view of the 5G mobile network jammer attack is shown in Figure 1.

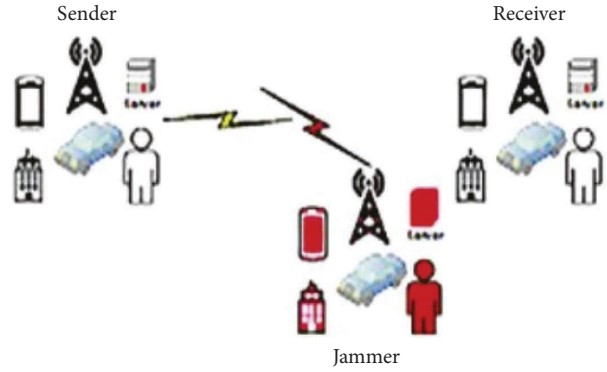

Figure 1: Jammer 5G mobile networks' attack.

5G networks are designed to be highly flexible and scalable, with a wide range of potential applications. To achieve this, 5G networks are structured into several internal function layers, each with a specific purpose: radio access network (RAN), core network (CN), network function virtualization (NFV), software-defined networking (SDN), and network orchestration [5–7]. 5G networks change over time to meet the needs of multimedia users. They do this by using network slicing through SDN and NFV for a variety of purposes, including meeting service needs, standardization, technology enablers, industry efforts, management, orchestration, and future research. 5G networks change over time to meet the needs of multimedia users. They do this by using network slicing through SDN and NFV for different purposes. These uses include meeting service needs, standardization, technology enablers, industry efforts, management, orchestration, and future research [8]. 5G research and development aims to provide various advanced characteristics, such as higher capacity than current 4G, denser users, support for device-to-device (D2D), and massive machine-type communication [9].

There are eight advanced features of 5G wireless systems, such as 1–10 Gbps connections to endpoints in the field, 1-millisecond latency, 1000% bandwidth per unit area, 10 to 100 times as many connected devices, 99.999% availability, 100% coverage, 90% reduction in network energy consumption, and up to ten years of battery life for low-power devices [10]. For 5G systems to meet these performance standards, many different technologies are used. These include heterogeneous networks (HetNet), massive multiple-input multiple-output (MIMO), millimeter wave (mmwave) [11], direct-to-device communications [12], software-defined networks (SDNs) [13], network function virtualization (NFVs) [14], and networking slices. For B5G authentications, a protocol is created that uses message authentication codes, symmetric cryptography, and elliptic curve cryptography to show that it is safe based on the Dolev–Yao model. Performance evaluation indicates that it has minimal execution time and bandwidth requirements, making it suitable for B5G networks [15]. A hash signature-based AKA protocol is developed for mutual authentication between user equipment and 5G base station (gNB), with independently computed session keys to ensure message confidentiality and integrity. Security evaluation confirms its resilience against common 5G attack vectors, while performance evaluation demonstrates minimal computation and communication costs for the protocol [16]. A trusted authority-based authentication scheme is developed for secure IoT packet exchanges, featuring stochastic token generation and message source authentication to prevent attacks like session hijacking and man-in-the-middle. Security analysis confirms key agreement and mutual authentication, with performance metrics showing low communication and computation costs [17]. A pseudonym-based authentication protocol is designed for 5G network elements, showing resilience against various attacks, including ephemeral leakages, man-in-the-middle (MitM), impersonation, and offline guessing. Performance evaluation indicates that the protocol has the lowest execution time and bandwidth requirements compared to similar protocols [18].

Despite the ease of use of wireless networks, they are vulnerable to security threats as air is used to transmit data, making them susceptible to jamming [19]. The free space serves as the communication channel for 5G networks, like other wireless cellular networks. This makes wireless networks more susceptible to interference, which leads to a decline in their performance. The enhanced EAP-AKA protocol, vital for authentication in 5G networks, encounters security hurdles like simulated attacks, man-in-the-middle (MitM) attacks, and inadequate user identity privacy measures. Strengthening cellular network security requires robust authentication that can withstand conventional attacks such as privileged insider threats, desynchronization issues, password guessing, and impersonation attempts [20]. In 5G HetNets, an improved handover protocol uses dynamic sequence numbers and timestamps to stop replay attacks. It also provides mutual authentication, privacy, key secrecy, and protection against many attacks, such as MitM and impersonation [21]. In the event of significant blocking, receivers cannot decipher broadcast signals. Malicious nodes could take advantage of this flaw to obstruct legitimate users' wireless communications. These attacks are called jamming attacks. In a jamming attack, radio signals are transmitted that reduce the signal-to-interference-plus-noise ratio (SINR) of communications [22]. When dividing the signal power by all other interfering signals, including noise, a ratio greater than 1 generally denotes a desirable state of more signal than noise [19]. Jamming attacks can be carried out

using a variety of devices, including simple radios, high-powered transmitters, and even software-defined radios.

Inducing denial of service (DoS) attacks with wireless signal jamming devices is probably the most common use for these devices. Wireless networks heavily rely on radio channels, and jamming attacks consequently interrupt transmission by injecting semivalid packets into those channels [23]. Models of varying complexity, such as intelligent jammers that sense and calculate in real time or steady sources of wave interference, can increase the attack's effectiveness and covertness. In industries such as transportation and healthcare, such attacks can have a wide range of negative effects, including disruptions of services, invasions of privacy, and even deaths.

Communication disruptions caused by jamming attacks can have serious effects, particularly for real-time data sharing applications like the Internet of Things (IoT) and Big Data analytics. Sensors and devices in an IoT-Big Data system are constantly collecting and transmitting data, which is then analyzed for insights. Jamming attacks can disrupt this data flow, preventing real-time analytics and perhaps creating delays or mistakes in insights generated from big data. From smart grids and industrial automation to remote healthcare monitoring and driverless vehicles, this disruption may have a domino effect on a number of applications. The emergence of reactive jammers has increased the threat even further. Unlike traditional jammers that simply broadcast noise, reactive jammers can exploit their sensorial capability to sense the surrounding wireless environment. This allows them to intelligently determine their jamming strategy in real time, aiming to inflict maximum damage. Because reactive jammers can effectively stop secure communications in IoT networks even with little power, it is very important to look into ways to protect these important data flows from being jammed [24–26].

Jamming attacks on IoT and Big Data systems can have adverse effects. For example, an attack on a remote healthcare monitoring system could cause delays in vital medical care, while an attack on a smart grid could result in power outages. Disrupted data flow may lead to data loss or corruption, endangering the integrity of massive data collected by IoT devices and rendering it unsuitable for analysis. This can eventually reduce the overall effectiveness of IoT-Big Data systems by delaying processing and analysis.

Fortunately, various ways exist for preventing or mitigating the impact of jamming attacks. These techniques include frequency hopping: jamming communication gets more difficult when frequencies are switched quickly. Spread spectrum techniques: data transmissions are less vulnerable to jamming when they are dispersed over a larger frequency band. Encryption: adding an extra layer of protection to data transmissions makes it more difficult for adversaries to impede communication. Intrusion detection systems (IDS): these systems are capable of recognizing possible jamming attempts and notifying network administrators of them. Network hardening: implementing security best practices to harden the network infrastructure might make it more resistant to jamming attacks. Additionally, recent research proposes a machine learning-based approach to detect and counter jamming attacks in real time, specifically tailored to the IoT domain [27].

While existing research underscores the significance of 5G network security, there is a lack of comprehensive taxonomy to categorize 5G jamming attacks. Current taxonomies may not fully capture the subtle characteristics of these attacks, especially in the context of developing 5G technologies. This limitation underscores the importance of the novel approach, which seeks to overcome the unique challenges posed by jamming attacks on 5G networks. The lack of a systematic framework makes it difficult for network managers, security specialists, and legislators to understand and efficiently mitigate the subtleties of jamming attacks. This paper aims to bridge this gap by proposing a comprehensive taxonomy that categorizes the diverse spectrum of jamming attacks targeting 5G networks.

The proposed taxonomy goes beyond existing frameworks by incorporating novel dimensions for identifying 5G-specific jamming attacks. Jamming attacks were methodically categorized across multiple dimensions, including attack types, techniques, targets, impacts, sources, and vectors. By incorporating these unique dimensions, the taxonomy provides a more sophisticated understanding of 5G jamming attacks, allowing for more effective defense strategies against these emergent threats. By providing a structured framework for investigating and categorizing 5G jamming attacks, the aim is to equip stakeholders with the knowledge they need to design efficient defenses against these threats. In line with this objective, the paper makes the following contributions.

Motivation for research: the crucial necessity is to recognize and categorize 5G jamming attacks, underscoring the need for strong security measures in the face of changing wireless communication paradigms. Identification of research gaps: the absence of a comprehensive taxonomy for 5G jamming attacks as a key gap in the existing literature, emphasizing the importance of methodical frameworks to address rising security concerns, was identified. Proposal of taxonomy: the proposed structured taxonomy offers a thorough framework for researching and countering 5G jamming attacks by methodically classifying them according to several dimensions. Contribution to knowledge: the taxonomy provides insights important for network administrators, security specialists, and lawmakers to comprehend the complexities of 5G jamming attacks and design effective defense tactics, thus ensuring the integrity.

Through the research, the aim is to establish a foundational framework for addressing the critical security issues that arise in 5G networks, supporting the safe and robust development of wireless communication technologies. The major objectives are as follows:

(i) Introduce a pioneering taxonomy for 5G jamming attacks.

(ii) Craft the taxonomy through diverse research methodologies including literature review, case studies, incident database analysis, and network architecture assessment.

(iii) Structure the taxonomy around six dimensions: attack classification, attack techniques, jammer characteristics, impact and target analysis, countermeasure strategies, and security layers.

(iv) Validate the taxonomy's efficacy through real-world case studies from regions like Ukraine, the South China Sea, and Cuba.

(v) Contribute significantly to strengthening the security landscape of 5G networks by equipping stakeholders with tools and knowledge to defend against jamming attacks and enhance overall network resilience amid rapid technological progress and connectivity advancement.

The major contributions include

(i) Introduces a comprehensive taxonomy for 5G jamming attacks.

(ii) Structured around key dimensions such as attack classification and countermeasure strategies.

(iii) Validated through case studies from Ukraine, the South China Sea, and Cuba. • Considers technical, sociopolitical, and economic factors.

(iv) Provides valuable insights into jamming attack specifics and countermeasures.

(v) Lays groundwork for expanding the taxonomy and integrating AI/ML.

(vi) Highlights the need for ongoing collaboration among stakeholders.

Section 1 of the paper describes the literature review encompassing 5G Networks, jamming attacks on wireless networks, and taxonomies in network security. A methodology was devised to develop a detailed taxonomy for classifying these attacks, integrating insights from literature reviews, case studies, incident databases, network architecture analysis, and protocol analysis in Section 2. Section 3 provides a detailed methodology for the research, including a thorough literature search on 5G networks and jamming attacks, examination of case studies, analysis of incident databases, scrutiny of network architecture, and protocol analysis. It lays the groundwork for understanding and categorizing jamming attacks on 5G networks, contributing to a comprehensive taxonomy essential for developing effective defense strategies. Section 4 provides the taxonomy which delves into attack techniques, jamming characteristics, impact and target analysis, countermeasures, and security layers, providing a structured understanding of the subject. Implementation and evaluation are followed in Section 5, applying the taxonomy to case studies on the Jamming of Drone Communication in Ukraine (2022), GPS Signals in the South China Sea (2019), and Cellular Networks in Cuba (2021), validating its real-world efficacy. The discussion and results in Section 6 present numerical and thematic analyses of the case studies, demonstrating the taxonomy's utility in addressing jamming attacks. Section 7 is the conclusion which provides key findings, contributions, and future research directions, bolstered by a comprehensive reference list.

2. Literature Review

The rapid deployment of 5G networks (Table 1) has heightened security concerns, with jamming attacks emerging as a significant threat. These attacks pose severe consequences, from disrupting critical infrastructure services to compromising national security. This literature review provides an overview of existing research on 5G networks and jamming attacks, addressing the unique challenges posed by the increased reliance on wireless communication.

2.1. 5G Networks. The research conducted delves into the technical aspects of 5G, emphasizing millimeter-wave frequencies, massive MIMO configurations, and low-latency communication. While millimetre-wave frequencies enhance data transfer rates, they are susceptible to targeted jamming attacks due to signal attenuation. Massive MIMO, contributing to increased network capacity and coverage, introduces complexity in signal processing, making the network vulnerable to coordinated jamming attacks. Low-latency communication, crucial for applications like enhanced reality and autonomous vehicles, also renders the network susceptible to timing disruptions caused by jamming attacks [28].

Another study explores frequency jittering (FJ) schemes for securing ultrareliable low-latency communication (URLLC) in 5G. Their adaptive FJ schemes, applied to technologies like beamforming, MIMO, and IoT networks, offer security without taxing device resources [29].

Research conducted also highlights smart jamming attacks targeting 5G NR networks, classifying them into deceptive, reactive, and cognitive types. Mitigation techniques include frequency hopping, spread spectrum, jamming detection, beamforming, and adaptive transmission schemes [30].

Another study extensively explores jamming attacks and countermeasures in wireless sensor networks (WSNs), covering various attack types, their impacts, and a wide range of countermeasure strategies. Their discussions on countermeasures like machine learning, user-centric approaches, and dynamic frequency hopping provided valuable insights into securing network communications. This comprehensive survey inspired research on cybersecurity strategies in complex network environments, particularly in preemptively identifying and countering jamming attempts in 5G networks. Their work served as a foundational understanding, guiding the exploration of enhancing the overall resilience of 5G networks against potential security vulnerabilities [31].

Table 1: Comparative study of prior research potential criteria.

Title/author	Year	Research focus/objective	Methodology	Types of attack	Targeted systems	Finding conclusion
Friendly jamming schemes to secure ultrareliable low-latency communications in 5G and beyond communications	2021	Survey of friendly jamming (FJ) for IoT security, considering various wireless tech and networks	Literature review	Friendly Jamming	IoT, beyond 5G	Integration with diverse tech improves security efficiency. Future research directions outlined
Smart jamming attacks in 5G new radio: A review	2020	Explore 5G NR vulnerabilities to jamming, propose solutions	Literature review, analysis	Regular, delusive, random, responsive, go-next, control channel	5G new radio (NR)	Despite 5G NR's resilience, vulnerabilities persist. Future research needed for deeper antijamming techniques
Jamming attacks and antijamming strategies in wireless networks: a comprehensive survey	2021	Examine jamming threats and defenses in wireless networks	Literature review, analysis	Jamming attacks	WLANs, cellular networks, CRNs, ZigBee, Bluetooth, vehicular networks, LoRa, RFID, GPS	Despite tech progress, wireless networks remain vulnerable to jamming and research gaps for securing networks against jamming
What will 5G be?	2014	Provide a comprehensive overview of 5G technology	Literature review, analysis	5G networks	Not applicable	5G is a significant shift, featuring high frequencies, large bandwidths, and dense device deployments. Seamless integration with LTE and WiFi is vital for universal coverage and user experience
Online schedule randomization to mitigate timing attacks in 5G periodic URLLC communications	2023	Develop countermeasure for timing attacks on periodic real-time URLLC flows in 5G	Proposal, analysis, evaluation	5G, ICSs	Timing	PerRand strategy counters selective jamming, ensuring deadlines. It uses Kullback–Leibler divergence for randomness
Smart jamming attacks in 5G new radio: a review	2020	Focuses on their implications and strategies within 5G NR technology	Literature review, analysis	Smart jamming attacks in 5G new radio (NR)	5G new radio (NR)	A comprehensive review of smart jamming attacks in 5G new radio (NR), highlighting their potential threats and implications
Jamming attacks on wireless networks: classification, countermeasures, and challenges	2013	To provide a comprehensive analysis of jamming attacks on wireless networks, including classification, countermeasures, and challenges	Literature review, analysis	Jamming attacks on wireless networks	Wireless networks	Importance of robust classification and countermeasures against jamming attacks to enhance the security of wireless networks
The evolution of jamming attacks in wireless networks	2016	Investigate the evolution of jamming attacks in wireless networks	Literature review, analysis	Continuous wave jamming, noise jamming, and smart jamming	Wireless networks susceptible to jamming attacks, encompassing a range of communication protocols and technologies	Summarizes the evolution of jamming attacks in wireless networks

Table 1: Continued.

Title/author	Year	Research focus/objective	Methodology	Types of attack	Targeted systems	Finding conclusion
Towards security and privacy preservation in 5G networks	2021	Security and privacy preservation in 5G networks	Literature review, analysis	Disrupting the security and privacy of 5G networks	5G networks	The conclusion likely addresses the importance of robust security measures
A taxonomy of attack mechanisms in the automotive domain	2021	Categorize and classify various attack mechanisms relevant to the automotive domain	Literature review, analysis	Remote exploits, physical intrusions, denial-of-service (DoS) attacks	Automotive systems, including in-vehicle networks, electronic control units (ECUs), connected car technologies, and other components within modern vehicles	Summarizes the key findings of the taxonomy and highlights the importance of securing automotive systems against cyber threats
A survey on jamming attacks and countermeasures in WSNs	2009	Provides a comprehensive overview of jamming attacks targeting wireless sensor networks (WSNs)	Literature review, analysis	Continuous wave jamming, random noise jamming, selective jamming, and protocol-specific attacks targeting WSN communication protocols	Wireless sensor networks (WSNs)	Summarizes the key insights gained from the survey and highlights the prevalence and impact of jamming attacks on WSNs
Selective jamming attacks in wireless networks	2010	To investigate and analyze selective jamming attacks targeting wireless networks	Literature review, analysis	Selective jamming attacks	Wireless networks, which encompass various types of communication systems such as Wi-Fi, cellular networks, and ad hoc networks	Summarizes the findings related to selective jamming attacks and highlights the challenges in detecting and mitigating
Signal characteristics of civil GPS jammers	2011	Investigate and analyze signal properties of civil GPS jammers	Literature review, analysis	Focus on GPS disruption by civil GPS jammers, impacting navigation and location-based services	GPS navigation system, disrupted by civil GPS jammers aiming to interfere with satellite signals	Summarizes findings on civil GPS jammer signal traits
The impact of international economic sanctions on Iranian cancer healthcare	2015	Evaluate the effects of international economic sanctions	Literature review, analysis	Analyze the negative impacts of economic sanctions on healthcare services	Iranian cancer healthcare infrastructure	Discusses the detrimental effects of economic sanctions on cancer healthcare in Iran

Table 2: A comprehensive categorization of jamming attack aspects, including intentionality, scope, signal targets, duration, legal implications, and attribution complexity.

Aspect	Category	Description
Intentionality	Financial gain	Attackers disrupt operations to cause financial losses
	Ideological motives	Jamming attacks driven by ideological beliefs
	Competitive advantage	Jammers target competitors to gain an unfair advantage
Scope	Localized	Attacks limited to a specific area
	Regional	Attacks target a wider region, such as a state or province
	National	Attacks affect an entire country
	Global	Attacks disrupt 5G networks worldwide
Signal target	Mobile data	Jammers disrupt cellular connectivity and Internet access
	IoT devices	Jamming attacks cause disruptions in connected applications
	Critical infrastructure networks	Attacks disrupt power grids, transportation system
Additional aspects	Duration	Attacks can be short-term, prolonged, or persistent
	Coordination	Attacks can be coordinated or uncoordinated
	Legal implications	Jamming attacks may violate laws and lead to legal consequences
	Reversibility	Attacks may allow for quick recovery or cause lasting damage
	Complexity	Attacks can be simple or advanced, requiring technical expertise
	Attribution difficulty	Attributing attacks can be challenging due to anonymity
	Collateral damage	Attacks may cause unintended damage beyond the intended target
	Motivation transparency	Attacker's motivation may be clear or unclear
	Innovation	Jammers may employ static or innovative attack methods
	Environmental impact	Attacks may disrupt ecological monitoring systems
	Geographical focus	Attacks can have a global or localized focus
	Frequency of occurrence	Attacks can occur frequently or be rare events
	Scalability	Attacks may be scalable or limited in their scalability
	Targeted information	Jammers may target general or specific information
	Social engineering involvement	Attacks may involve social engineering tactics
	Resilience to countermeasures	Attacks can be designed to be resilient to countermeasures
	Financial resources required	Attacks can be low-resource or high-resource attacks

Another study addresses security challenges in 5G networks, covering issues such as access control, data confidentiality, and privacy. Mitigation strategies involve network slicing, encryption, authentication, IDS/IPS, and privacy-preserving data collection. Recent advancements focus on security protocol innovations, integrated security in network management, and machine learning for security analytics [32].

Another study provided a thorough analysis of selective jamming attacks on wireless networks, focusing on targeted disruptions to specific packets. It proposed detection and mitigation techniques to counter these attacks, including statistical analysis, adaptive modulation, and cooperative detection methods. This paper inspired research on cybersecurity strategies in complex network environments by highlighting the importance of understanding and defending against targeted disruptions like jamming attacks. It helped shape the approach by stressing the need for organized security layers and full defenses at physical, network, application, and other levels to make advanced network infrastructures like 5G networks more resistant to attacks [33].

Research on civil GPS jammers provided insights into jammer properties like power levels, mobility, intelligence, and adaptiveness. This understanding inspired the research on cybersecurity strategies in 5G networks, leading to a taxonomy dimension focused on jammer capabilities and intentions. Leveraging this insight enabled the development of proactive countermeasures against potential jamming attacks [34].

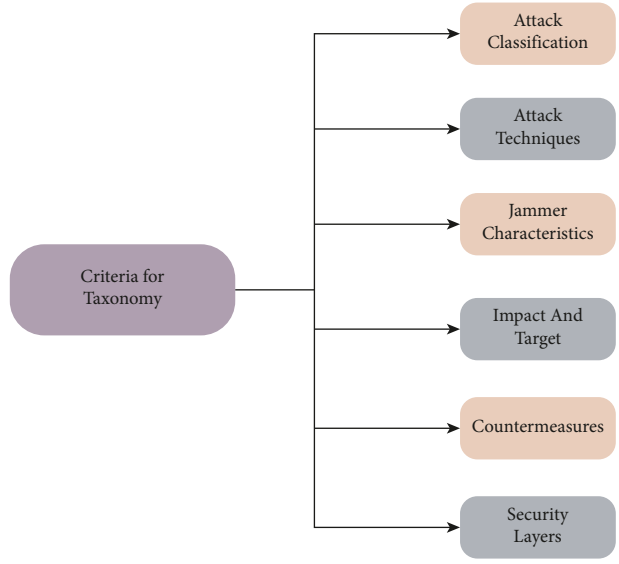

Figure 2: The essential criteria for developing the taxonomy.

A study on economic sanctions' impact on Iranian cancer healthcare inspired the research on 5G jamming attacks' effects. Just as they analyzed sanctions' consequences on healthcare, the paper delved into jamming attacks' ramifications on public safety, data integrity, and network

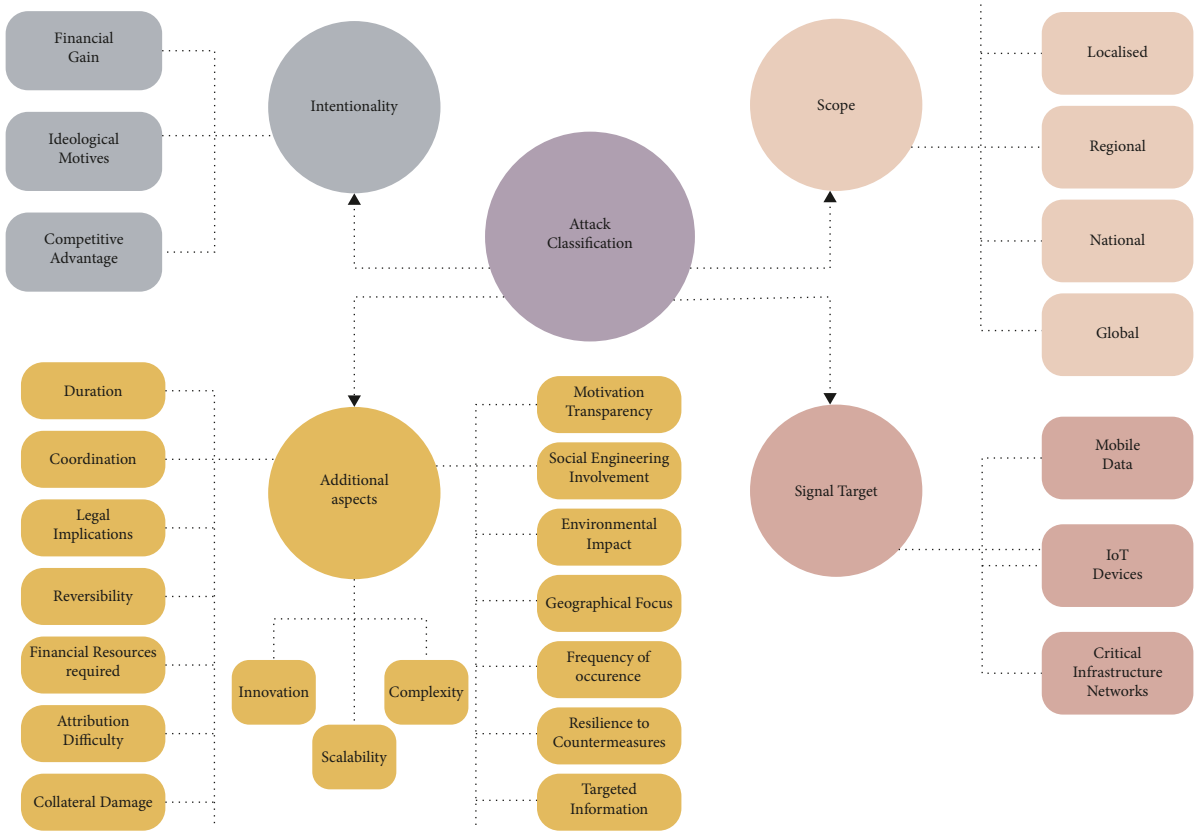

Figure 3: The classification of 5G jamming attacks based on intentionality, scope, signal target, and other factors.

functionality. The taxonomy, "Impact and Target," categorizes and comprehends 5G jamming's unique impacts, aiding in the development of effective countermeasures [35].

2.2. Jamming Attacks on Wireless Networks

2.2.1. Evolution of Jamming Research. Jamming attacks have a long history, with early research examining vulnerabilities and ways of interference in previous network generations [36, 37]. These studies provide useful insights into the fundamental concepts of jamming attacks, laying the groundwork for understanding their use in 5G networks.

2.2.2. Unique Challenges of 5G. However, the shift to 5G creates new complexities. According to research by [38], using an online schedule randomization technique can stop timing assaults that target 5G ultrareliable low-latency communication (URLLC). This demonstrates how 5G's distinct properties, such as its emphasis on exact timing, demand different protection techniques against jamming attacks.

2.2.3. Examining Specific Attacks and Mitigation Techniques. Hardware-based jamming: a research study [39] looks at a hardware-based jamming attack that lowers user equipment throughput by interfering with 5G's Physical Uplink Shared Channel (PUSCH). This is a prime example of how serious jamming attacks can be and how effective mitigation techniques are required. Detection and classification: research by [40] suggests a multistage method for accurately detecting and categorizing jamming attacks using supervised and deep learning classifiers. Although this holds potential for automated defense systems, further research is required to comprehend the processing requirements and possible drawbacks of these techniques in practical network deployments. Leveraging network design: As investigated by [41], the open radio access network (O-RAN) design has the ability to detect downlink jamming in 5G. This highlights the need to take network architecture into account while creating defense mechanisms. However, the effectiveness of this strategy may vary depending on the deployment scenario and the sophistication of the jamming attack.

2.2.4. Connecting Research to Taxonomy Development. The research presented here provides useful insights into the various types of jamming attacks targeting 5G networks. It draws attention to the necessity of a thorough taxonomy that takes into account different attack kinds, target components, and potential impact. Through a thorough examination of current research on jamming attacks and countermeasures, key characteristics are identified that will serve as the foundation for creating a comprehensive taxonomy tailored especially for 5G networks.

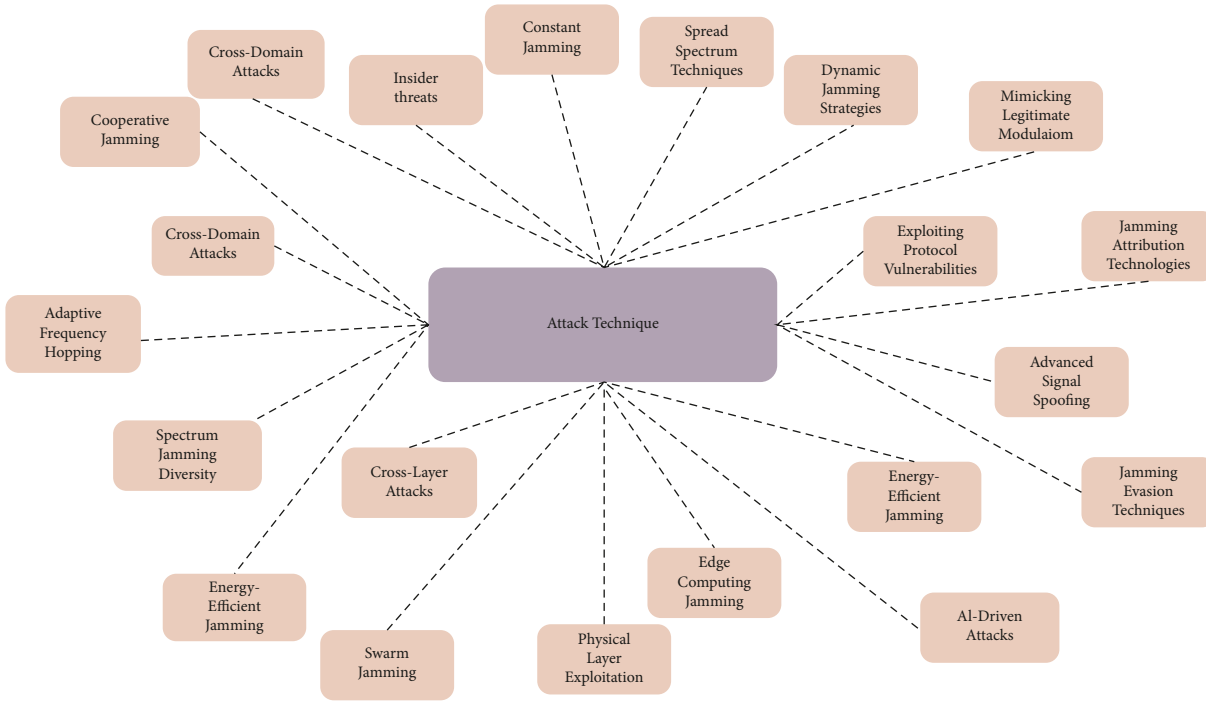

Figure 4: Visual representation of various jamming techniques disrupting wireless signals, highlighting the vulnerabilities of modern communication systems.

Table 3: A comprehensive taxonomy categorizing various jamming attack types and techniques in 5G networks, providing insights into their characteristics and key attributes.

Attack type	Description
Constant jamming	The attacker continuously transmits a powerful signal on the same frequency as the 5G network (attack type: continuous jamming)
Spread spectrum techniques	Attackers employ spread spectrum techniques to distribute the jamming signal across a wide range of frequencies (attack type: discontinuous jamming)
Mimicking legitimate modulation	Sophisticated jammers mimic the legitimate modulation schemes used by the 5G network (attack type: deceptive jamming)
Exploiting protocol vulnerabilities	Attackers exploit vulnerabilities in SG protocols, injecting deceptive signals (attack type: deceptive jamming)
Advanced signal spoofing	Techniques that involve more sophisticated signal spoofing (attack type: deceptive jamming)
Al-driven attacks	Investigation into the potential use of artificial intelligence in crafting and adapting jamming strategies (attack type: to be determined based on the specific AI application)
Physical layer exploitation	Attacks that specifically target vulnerabilities in the physical layer of SG infrastructure (attack type: varies depending on the specific vulnerability)
Cross-layer attacks	Coordinated attacks that exploit vulnerabilities across multiple layers of the 5G network simultaneously (attack type: varies depending on the specific layers targeted)
Spectrum jamming diversity	Utilizing a diverse range of frequencies for jamming, beyond the traditional target frequencies (attack type: continuous or discontinuous jamming depending on the specific technique)
Dynamic jamming strategies	Jamming techniques that dynamically adapt based on real-time changes in the 5G network environment (attack type: varies depending on the specific strategy)
Cooperative jamming	Collaborative efforts where multiple jammers coordinate their attacks to amplify the disruption (attack type: continuous or discontinuous jamming depending on the specific technique)
Cross-domain attacks	Attacks that extend beyond the digital domain, targeting both digital and physical aspects of the 5G infrastructure (attack type: varies depending on the specific combination of techniques)
Insider threats	Jamming attacks orchestrated by individuals with insider knowledge or access to 5G infrastructure (attack type: varies depending on the specific technique used)
Swarm jamming	Coordinated attacks involving a large number of jammers operating in a swarm-like fashion (attack type: continuous or discontinuous jamming depending on the specific technique)

Table 3: Continued.

Attack type	Description
Adaptive frequency hopping	Dynamic adjustment of jamming frequencies to match the target's frequency-hopping patterns (attack technique)
Energy-efficient jamming	Jamming techniques designed to optimize energy consumption while maintaining disruption effectiveness (attack technique)
Jamming evasion techniques	Techniques employed by jammers to evade detection or circumvent countermeasures actively (attack technique)
Burst mode jamming	Short bursts of jamming signals interspersed with periods of silence to evade detection (attack technique)
Quantum jamming considerations	Exploring potential jamming techniques leveraging principles from quantum mechanics (attack type: to be determined based on the specific application)
Edge computing jamming	Jamming attacks that specifically target edge computing nodes in 5G networks (attack type: varies depending on the specific impact)
Jamming attribution technologies	Technologies or techniques used to attribute jamming attacks to their source

2.3. Taxonomies in Network Security. Building upon the exploration of jamming attacks in 5G networks, this section delves into the crucial role of taxonomies in network security. The area of network security relies significantly on well-defined taxonomies to categorize and comprehend cyber threats. Previous studies by [29, 42] highlight the significance of classifying data methodically, and their taxonomies encompass a wide variety of attack vectors according to target, intent, and techniques. These broad classifications provide a valuable foundation for understanding threats, but they may not capture the specific nuances of emerging attack types.

2.3.1. The Gap in 5G Jamming Taxonomy. There is currently no comprehensive taxonomy primarily focused on 5G jamming attacks. This gap hinders effective defense strategies, as a clear classification system is crucial for identifying patterns and trends. A clear taxonomy makes it easier to analyze jamming attacks more methodically, which makes it easier to spot patterns and trends in attack strategies and targets. Developing targeted defense systems: by categorizing different types of jamming attacks, researchers and security professionals can develop more targeted mitigation techniques and defense mechanisms tailored to specific attack characteristics. Enhancing communication and collaboration: a unified taxonomy can improve communication and collaboration among researchers, network operators, and security specialists when dealing with 5G jamming concerns.

2.3.2. Connecting Research to Building a 5G Jamming Taxonomy. The research discussed in the previous section on "Jamming Attacks on Wireless Networks" provides useful insights that can help establish a strong taxonomy for 5G jamming attacks. Here is how this research contributes to taxonomy development: attack types: research like those by [30, 38] indicates the existence of varied attack types, such as timing attacks and hardware-based jamming. The taxonomy allows for the classification of attacks according to their mechanism (e.g., time manipulation and disruption of signals). Target components: studies reveal weaknesses in particular network components, such as the Physical Uplink Shared Channel (PUSCH) [30]. Target components are one kind of classification factor that the taxonomy can include. Impact on network: the impact of jamming attacks on a network can vary, ranging from a reduction in throughput [30] to the total loss of communication. The taxonomy may take into account how seriously an attack affects network performance. Attack source: another possible classification feature in the taxonomy may be the origin of the jamming attack (e.g., malicious actor and accidental interference).

A comprehensive taxonomy for 5G jamming attacks can be created by examining these variables in light of recent findings and continuing developments in the area. This taxonomy will serve as a valuable tool for researchers, security professionals, and network operators in understanding, mitigating, and preventing these evolving threats in the 5G ecosystem.

3. Methodology

This ground-breaking research represents a critical investigation into the flaws present in 5G networks, concentrating on the terrifying threat that jamming attacks pose. As the fifth generation of wireless technology heralds a new era of connectivity with its revolutionary features, the heightened risk of security breaches, particularly through jamming attacks, underscores the urgency for comprehensive understanding and strategic defense mechanisms. Central to this research is the development of a detailed taxonomy, meticulously categorizing jamming attacks based on a spectrum of parameters. This sophisticated classification system encompasses types, tactics, targets, impacts, sources, and vectors. This systematic approach goes beyond a mere academic exercise; it serves as the foundational knowledge required to craft potent defenses against potential security vulnerabilities in 5G networks. The taxonomy emerges as a powerful resource for various stakeholders, including network managers, security specialists, and legislators. Providing a structured framework for understanding jamming attacks empowers these professionals to design strategic defense mechanisms tailored to the specific intricacies of the 5G environment.

The ability to classify and comprehend these attacks with granularity enables a proactive stance in fortifying networks

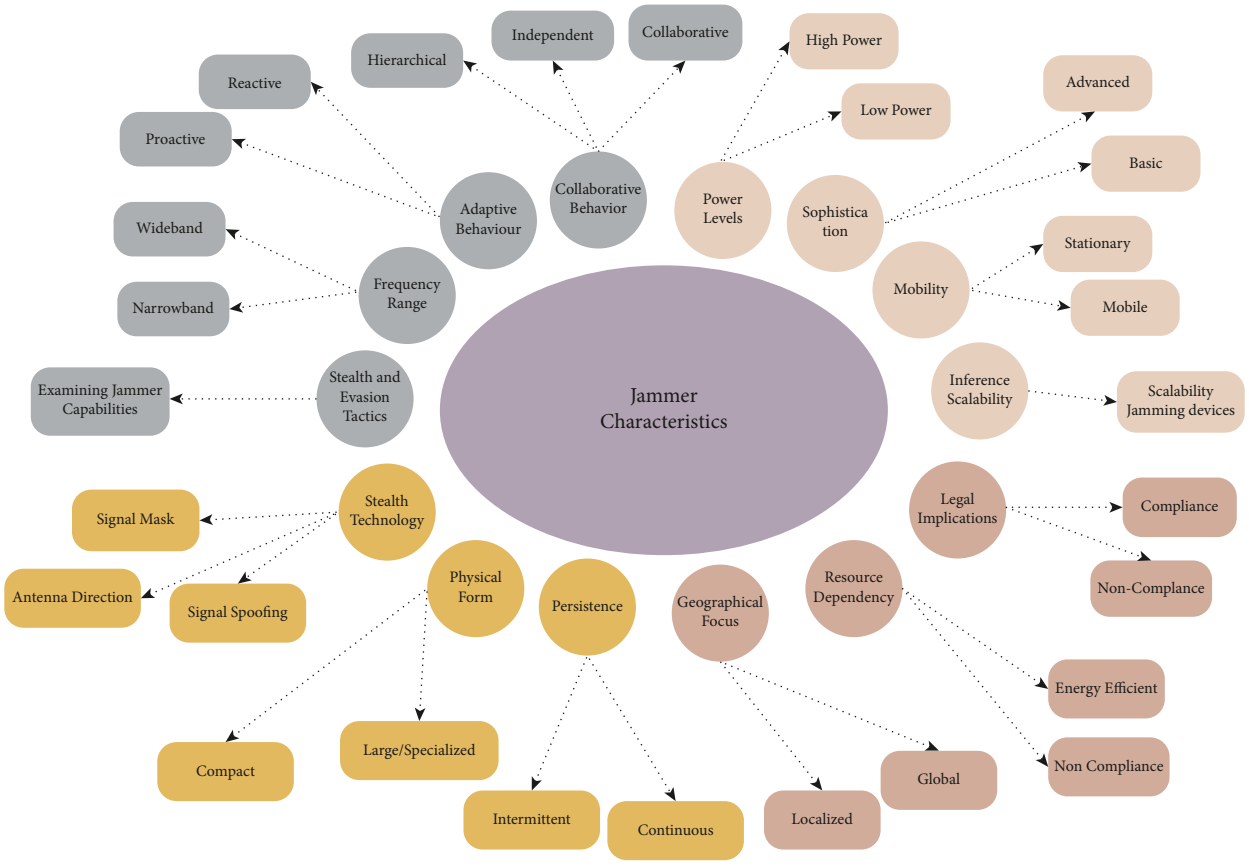

Figure 5: The various features and capabilities of different types of jammers.

Table 4: A comprehensive taxonomy categorizing jammer characteristics in 5G networks, including power levels, mobility, sophistication, and other key attributes.

Jammer characteristics	Description
Power levels	High power Low power
Mobility	Stationary Mobile
Sophistication	Basic Advanced
Adaptive behavior	Reactive adaptation Proactive adaptation
Stealth and evasion tactics	Examining jammers' capabilities to evade detection or employ stealth strategies to prolong their effectiveness
Interference scalability	Considering the scalability of jamming devices, from individual devices to distributed networks of jammers
Frequency range	Narrowband Wideband Multiband
Collaborative behavior	Coordinated Independent Hierarchical
Stealth technology	Signal masking Antenna directionality Signal spoofing
Physical form	Compact Large/specialized

Table 4: Continued.

Jammer characteristics	Description
Persistence	Intermittent Continuous
Legal implications	Compliance Noncompliance
Resource dependency	Energy-efficient Resource-intensive
Geographical focus	Localized Global

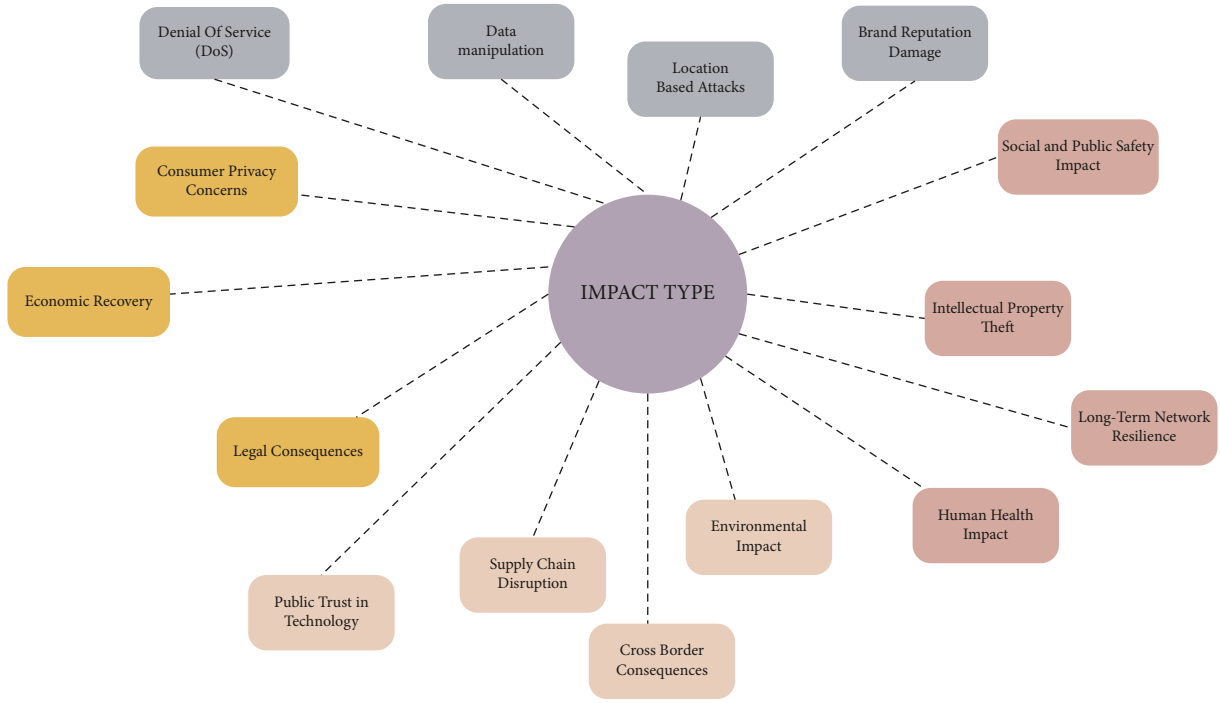

Figure 6: A visualization of the diverse effects of jamming attacks across various domains.

against potential threats. To bridge theoretical insights with practical applications, the research delves into real-world scenarios through insightful case studies. These case studies, set in diverse geopolitical contexts such as Ukraine, the South China Sea, and Cuba, serve as tangible demonstrations of the taxonomy's utility. They highlight the adaptability and effectiveness of the taxonomy in the face of varied and complex scenarios, reinforcing its practical relevance in safeguarding 5G networks. Moving beyond classification, the research scrutinizes the nuanced aspects of jamming attacks, encompassing attack techniques, jammer characteristics, impacts, and targets.

This holistic examination provides a comprehensive view of the intricacies involved in these security threats. By understanding the diverse tactics employed by attackers and the potential impacts on network infrastructure, stakeholders can develop countermeasure strategies that are not only reactive but also anticipatory. Furthermore, the research delves into the intricate layers of security involved in safeguarding 5G networks. It examines possible countermeasure tactics to lessen the risks that jamming attacks pose. This multifaceted exploration contributes to a profound understanding of the dynamic 5G security paradigm. Table 2 presents a comprehensive taxonomy of jamming attack types and techniques in 5G networks, offering insights into their characteristics and key attributes. This research not only identifies and analyzes vulnerabilities but also provides a robust taxonomy and strategic tools for defense against jamming attacks on 5G networks. Through real-world case studies and a nuanced examination of attack techniques, impacts, and countermeasures, this research makes a substantial contribution to fortifying the security landscape in an era where connectivity and technological innovation are paramount.

This research unveils a comprehensive taxonomy addressing jamming attacks on 5G networks. As the fifth generation promises revolutionary features, its vulnerability to security threats, particularly jamming attacks, poses a significant risk. The taxonomy classifies attacks based on types, tactics, targets, impacts, sources, and vectors. It

Table 5: A taxonomy of 5G jamming attack impact types, offering a systematic classification.

Impact type	Description
Denial of service (DoS)	Overwhelming the 5G network with interference
Data manipulation	Tampering with data packets within the 5G network
Location-based attacks	Strategically targeting 5G signals in specific locations
Brand reputation damage	Loss of customer trust and damage to brand image
Social and public safety impact	Risks to public safety and panic
Intellectual property theft	Unauthorized data access and manipulation
Long-term network resilience	Lingering vulnerabilities and diminished trust
Human health impact	Direct health effects of jamming signals
Environmental impact	Impact on wildlife, ecosystems, and environmental monitoring systems
Cross-border consequences	Impact on diplomatic relations and lack of international cooperation
Supply chain disruption	Vulnerability of the 5G supply chain to disruption
Public trust in technology	Negative impact on public perception and adoption rates
Legal consequences	Noncompliance with regulations and legal gaps
Economic recovery	Extended recovery time and impact on future investments
Consumer privacy concerns	Unauthorized data access and exposure

provides a structured understanding crucial for safeguarding networks, enabling network managers, security specialists, and legislators to develop potent defenses. The paper further explores case studies, applying the taxonomy to real-world scenarios in Ukraine, the South China Sea, and Cuba, demonstrating its practical utility. The taxonomy focuses on attack classification, techniques, jammer characteristics, impact and targets, countermeasure strategies, and security layers. It gives a thorough look at the changing 5G security paradigm, making it easier to stay safe as technology changes quickly.

3.1. Literature Search. We conducted a thorough literature review on 5G networks and jamming attacks using databases like IEEE Xplore and Google Scholar. Employed targeted keywords such as "5G Network," "Jamming Attacks," and "Taxonomy of 5G" to ensure a comprehensive exploration of the subject.

3.2. Case Studies. We examined case studies of 5G jamming attacks, applying selection criteria based on attack severity, geographical diversity, and relevance to research questions. We employed comparative and temporal analyses to identify patterns and changes in tactics. Figure 2 illustrates the fundamental criteria for developing the taxonomy.

3.2.1. Incident Databases. Utilized incident databases like CRAWDAD and the Wi-Fi jamming attack dataset to investigate real-world and simulated scenarios of jamming attacks on wireless networks.

3.2.2. Examination of Network Architecture. We conducted a detailed investigation of 5G network architecture, analyzing components like user equipment, base stations, core network, NFV, SDN, network slicing, fronthaul, backhaul, and edge computing. We examined vulnerabilities and interdependencies through simulations and scenario analysis.

3.2.3. Protocol Analysis. We examined communication protocols in 5G networks, including NR, PDCP, RLC, Ethernet, PPP, MAC, LLC, SDAP, NGAP, RRC, NAS, S1AP, TCP, UDP, SCTP, L2TP, HTTP/2, WebSocket, RESTful APIs, Diameter, GTP, GTP-U, NG-U, TLS, and IPsec. We analyzed protocol documentation, applied modelling methods, simulated scenarios, and conducted protocol stack analysis to identify potential vulnerabilities.

4. Taxonomy

The paper presents a comprehensive taxonomy framework, shown in Figure 2, that examines the multifaceted realm of 5G network security from six pivotal dimensions. To begin with, the framework excels in attack classification, which categorizes and classifies diverse 5G attacks based on their origin, nature, and intended impact. As a result, it provides a foundation for understanding the intricate threat landscape that the 5G ecosystem faces.

In the Attack Techniques section, the taxonomy delves into the specific techniques used by attackers to compromise 5G networks' integrity, availability, or confidentiality. Additionally, the taxonomy encompasses jammer characteristics, meticulously examining the various traits and attributes of jammers. Through an analysis of their capabilities, intentions, and technologies, a comprehensive understanding of jamming attacks can be gained. As part of the framework, a comprehensive impact and target analysis is conducted, which evaluates the repercussions of 5G attacks and identifies their specific targets. The results shed light on how 5G systems might affect network functionality, data integrity, and overall reliability.

Additionally, the taxonomy explores countermeasure strategies, systematically analyzing the array of strategies and technologies deployed to combat 5G security threats. This dimension reveals proactive measures taken to mitigate the impacts of potential attacks and fortify network resilience. In addition, the taxonomy defines security layers, which is the understanding of security measures implemented across sections of the 5G architecture. In this dimension, security mechanisms are viewed holistically, from the physical to the

Table 6: A comprehensive taxonomy of 5G jamming countermeasures, elucidating each method's description for a holistic understanding of network security strategies.

Countermeasure	Description
Jamming detection	Identify the presence of jamming signals
Dynamic frequency hopping	Dynamically change frequencies during communication
Physical layer security	Encrypt communication channels and authenticate devices
Machine learning for adaptive countermeasures	Adapt countermeasures based on evolving attack patterns
User-centric countermeasures	Involve and empower end-users in detecting and mitigating jamming effects
Deceptive technologies	Mislead and confuse jammers regarding the actual network configuration
Network resilience enhancements	Improve the overall resilience of the 5G network against jamming attacks
Collaborative defense	Coordinate and collaborate among different entities to defend against jamming attacks
Regulatory measures	Implement regulatory frameworks and policies to deter and penalize jamming attacks
Jammer attribution technologies	Trace and attribute jamming attacks to their source
Behavioral analytics	Analyze patterns of network behavior to detect anomalies and potential jamming activities
Public awareness and education	Educate the public and relevant stakeholders about the risks of jamming attacks
Edge computing security	Protect data processed at the network edge
Cross-domain collaboration	Pool resources and expertise from different domains
Human-in-the-loop security	Combine automated systems with human decision-making
Open source security tools	Enhance transparency, auditability, and collaborative development
Supply chain security	Prevent infiltration of malicious components and vulnerabilities
Threat hunting and forensics	Proactively search for signs of jamming threats and conduct forensic analysis
Environmental monitoring	Monitor and protect against environmental impacts of jamming
Cross-border cooperation	Mechanisms address cross-border jamming incidents and promote global cybersecurity collaboration
Economic impact assessment	Evaluate the economic impact of 50 jamming incidents
Policy and regulation evolution	Ensure policies and regulations address emerging jamming threats

application level. Combined, this taxonomy enables researchers to explore 5G security in a nuanced manner. The framework facilitates a comprehensive understanding of the dynamic and complex 5G security paradigm by systematically organizing and analyzing the many elements that make up the threat landscape and countermeasure ecosystem.

4.1. Attack Classification. In this research, the "attack classification" dimension within the taxonomy serves as a foundational pillar for methodically categorizing and comprehending the multifaceted landscape of 5G jamming attacks. By carefully grouping these attacks by their goal, range, signal target, and other important factors, as shown in Figure 3 and Table 2, the framework not only makes it easier to understand cyber threats, but it also makes it possible to spot new trends, their underlying causes, and their possible effects in the 5G ecosystem. Researchers learn a lot about the complicated cybersecurity problems caused by jamming attacks by using a detailed categorization method that tells the difference between things like signal disruption, data interception, device manipulation, and targeting network infrastructure. The taxonomy shows how this structured analysis not only helps in creating effective defenses but also makes it possible for strategic actions to be taken to make 5G networks more resistant to new threats and weaknesses.

4.2. Attack Techniques. The taxonomy's "attack classification" dimension serves as a cornerstone for systematically categorizing and understanding the diverse spectrum of 5G jamming attack types. The attack classification is shown in Figure 4 and is explained in more detail in Table 3. Attacks are carefully looked at based on their intended purpose, scope, targeted signals, and other important factors. This methodical organization enables researchers to discern patterns, underlying drivers, and potential ramifications of these attacks. By gaining a structured view of the attack landscape, this classification framework provides crucial insights into the intricacies of cyber threats faced by the ecosystem. It makes it possible to look into all the different ways that jamming attacks can happen on 5G networks. This helps people come up with strong defenses and countermeasures that can be used against specific types of attacks and holes in the 5G infrastructure.

4.3. Jammer Characteristics. The taxonomy dimension "jammer characteristics" is useful in giving a detailed study of the numerous qualities and attributes displayed by jammers in the context of 5G networks. This dimension rigorously investigates elements such as power levels, mobility, intelligence, adaptive behavior, and more, as seen in Figure 5 and summarized in Table 4. Taxonomy provides researchers and security professionals with vital insights into the different capabilities and intentions of jammers by categorizing and comprehending these properties. This comprehensive understanding is critical for creating effective countermeasures and defensive methods, as it allows for a proactive approach to possible jammer threats in the dynamic context of 5G network security.

Table 7: The details the implementation techniques and effectiveness evaluations for each 5G jamming countermeasure.

Implementation	Effectiveness
Spectrum analysis tools, anomaly detection algorithms	Rapid detection and classification of jamming attacks
Intelligent algorithms, network-wide synchronization	Increased resilience against frequency-based jamming attacks
Encryption, authentication mechanisms	Enhanced confidentiality and integrity of transmitted data
Machine learning algorithms	Timely and effective countermeasures against evolving threats
User-centric tools and training	Enhanced user awareness and participation in jamming mitigation
Decay networks, false communication patterns	Increased difficulty for jammers to accurately target the network
Redundancy, rapid adaptive strategies	Minimizing the impact of jamming attacks and ensuring service availability
Shared threat intelligence, cooperative efforts	Strengthening the collective defense posture and fostering a proactive response
Enforcing legal consequences, international agreements	Creating a deterrent effect and promoting responsible network use
Forensic analysis tools, blockchain, advanced tracking	Facilitating accountability, legal actions, and discouraging malicious activities
Behavioral analytics tools, machine learning algorithms	Early detection of abnormal activities and timely responses
Public awareness campaigns, training programs, educational materials	Engaging the community in safeguarding against jamming attacks
Robust security measures, access controls, encryption	Secure critical computing resources at the network edge
Collaborative research, joint training, information-sharing platforms	A multidisciplinary approach to address 50 jamming challenges
User interfaces for real-time security information	Context-aware decisions in response to nuanced jamming scenarios
Open-source security frameworks, threat intelligence platforms	The broader community of developers and security experts to improve 50 security
Rigorous supply chain risk management	Mitigate the risk of compromised components entering the 5G infrastructure
Threat hunting teams, forensic techniques	Enhance the ability to detect, respond, and learn from jamming incidents
Sensors and monitoring systems	Protect the environment and maintain the integrity of environmental monitoring systems
International agreements and protocols	Strengthen international relations and responses to 5G jamming threats
Economic impact assessments and modelling scenarios	Provide insights into the economic implications and inform strategies for recovery and future investments
Regularly review and update regulatory frameworks	Create an environment that supports ongoing security enhancements and compliance with emerging standards
User-friendly privacy settings interfaces and transparent data usage policies	Enhance user trust and allow individuals to manage their privacy preferences in the 50 ecosystem

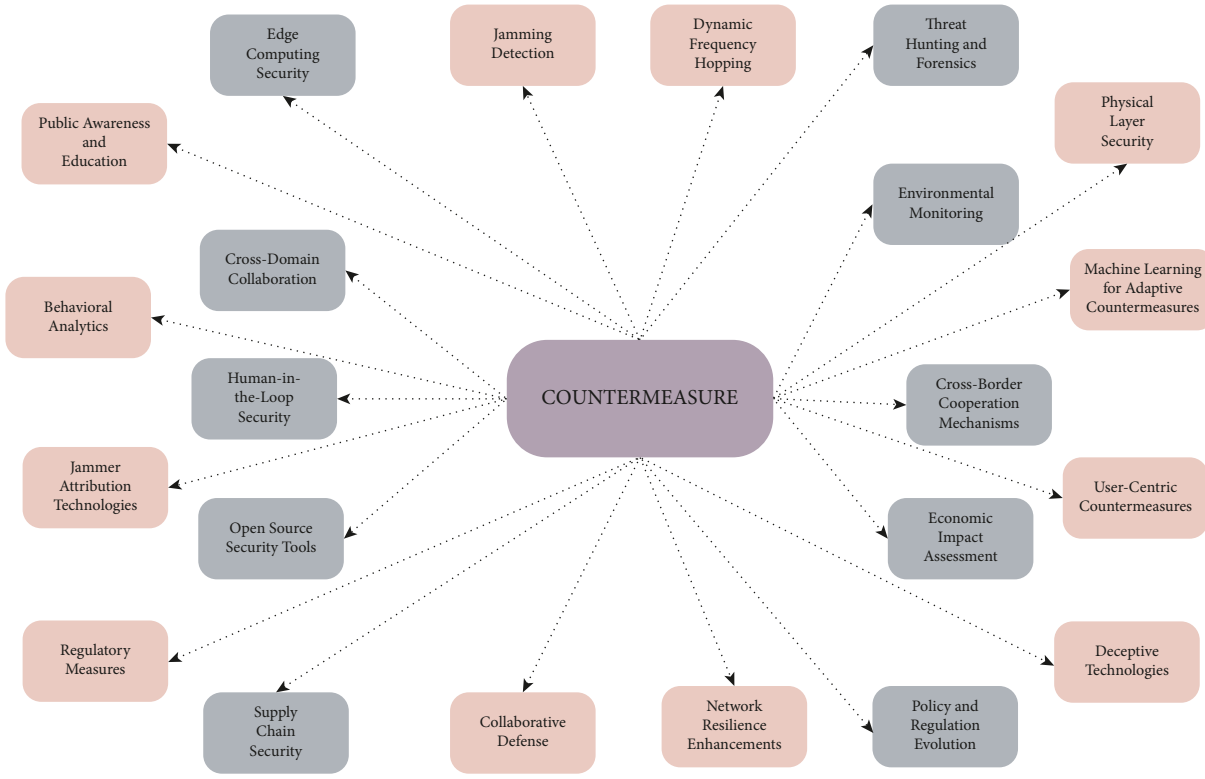

Figure 7: An outline of the techniques employed to mitigate the effects of jamming attacks.

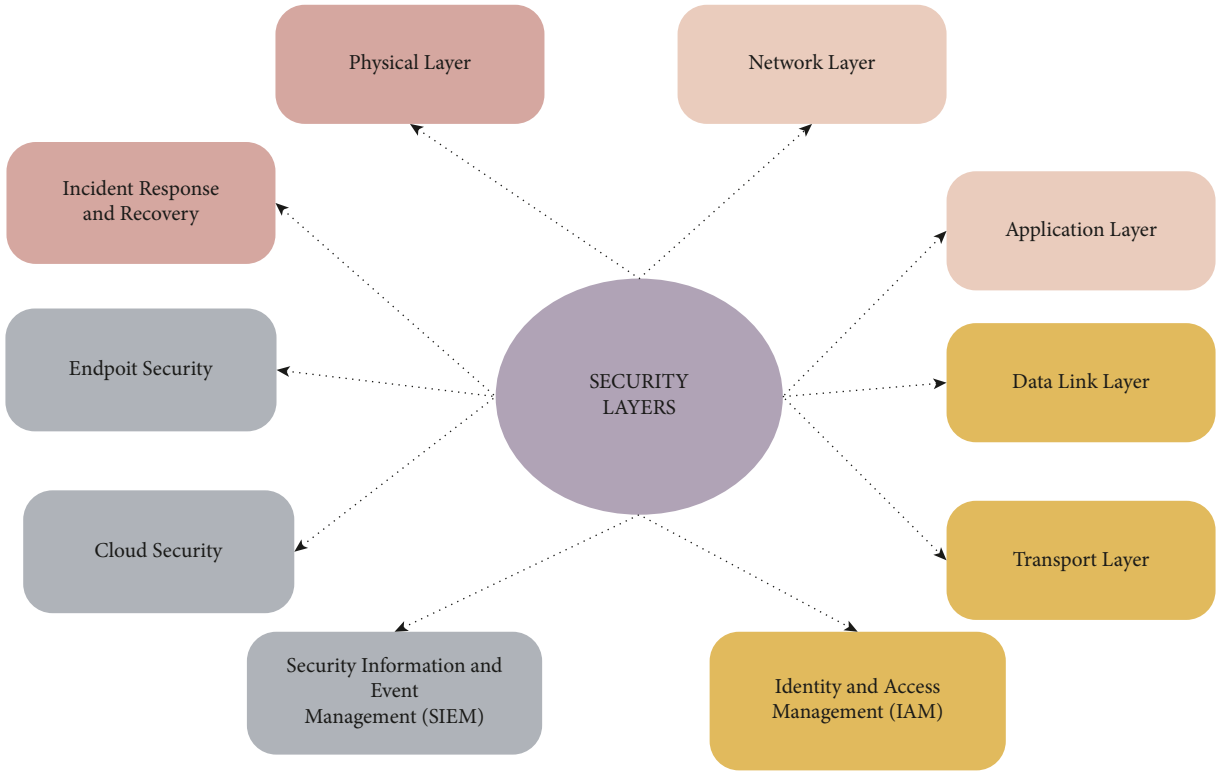

Figure 8: A schema showcasing the protective measures and techniques used to defend against jamming intrusions.

Table 8: A taxonomy delineating the diverse security layers within 5G networks, offering a structured overview of protective measures and implementation.

Security layer	Description	Implementation
Physical layer	Protects hardware, infrastructure, and transmission mediums	Access controls, surveillance, tamper-evident seals
Network layer	Safeguards communication between devices and systems	Firewalls, intrusion detection/prevention systems, VPNs
Application layer	Defends against application-level vulnerabilities	Encryption of application data, secure coding practices
Data link layer	Enforces secure data transfer at the data link level	MAC address filtering, VLANs
Transport layer	Ensures secure end-to-end communication	TLS/SSL protocols, port filtering, session management
Identity and access management (IAM)	Manages user identities and access	Multifactor authentication, access controls, identity verification
Security information and event management (SIEM)	Collects, analyses, and manages security data	Log monitoring, threat intelligence integration, incident response automation
Cloud security	Protects cloud computing environments	Data encryption, identity management, API security
Endpoint security	Protects individual devices	Antivirus software, endpoint detection and response (EDR), device encryption
Incident response and recovery	Addresses and recovers from security incidents	Incident response plans, backup, and recovery processes

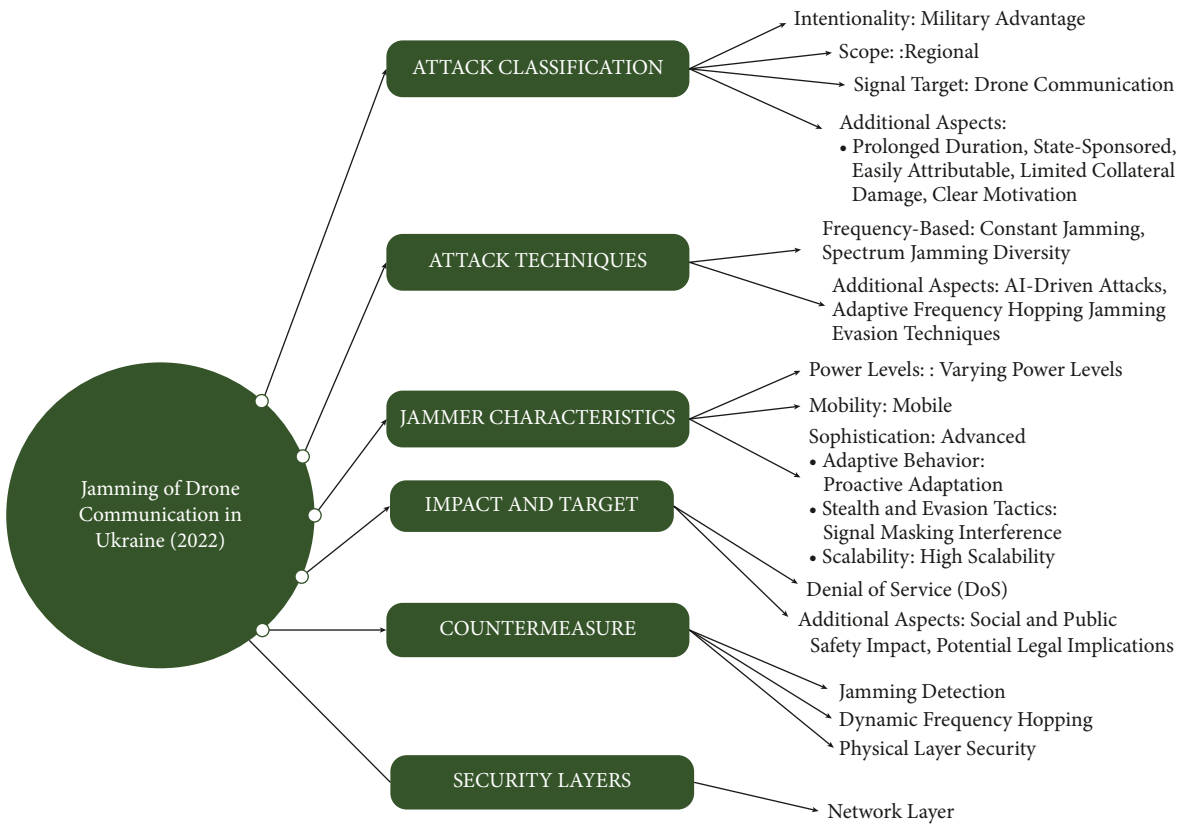

Figure 9: Classification of jamming techniques disrupting drone operations in the 2022 Ukrainian conflict.

4.4. Impact and Target. The "impact and target" component inside the taxonomy looks into the ramifications of 5G jamming attacks and carefully defines their unique targets. As shown in Figure 6 and described in Table 5, this dimension gives a visual representation of the wide range of effects these attacks can have in many areas, ranging from changing data and denial of service to health issues and international trade. The taxonomy helps create a thorough understanding of the potential effects of 5G systems on public safety, data integrity, network functionality, and other areas by categorizing these effects. Through the development of effective countermeasure techniques, stakeholders can proactively address and mitigate the various effects of 5G jamming assaults, thanks in large part to the thorough investigation.

4.5. Countermeasure. Tables 6 and 7 go into more detail about the "countermeasures" dimension in Figure 7. It delineates a wide range of methods utilized to counteract the impact of jamming assaults on 5G networks. These countermeasures cover a broad range of tactics, such as machine learning for adaptive countermeasures, user-centric countermeasures, dynamic frequency hopping, physical layer security, and jamming detection. The taxonomy provides a full overview of each countermeasure's description, implementation, and effectiveness. Through this comprehensive investigation, interested parties can create preemptive strategies that not only identify and counter-jamming attempts but also strengthen the 5G network's overall resiliency. The taxonomy provides network managers, security experts, and policymakers with useful insights to protect against potential security vulnerabilities by providing an organized summary of countermeasure options.

4.6. Security Layers. The "security layers" dimension provides a paradigm that highlights defenses against jamming incursions in 5G networks, as shown in Figure 8 and explained in Table 8. Taxonomy offers an organized summary that distinguishes between various network security tiers. Measures at the physical, network, application, data connection, transport, identity, and access management, cloud security, endpoint security, security information and event management (SIEM), and incident response and recovery levels are included in these layers. This methodical approach fosters a robust 5G security landscape by providing stakeholders with a thorough grasp of the layers required to fight against jamming attacks.

5. Implementation and Evaluation

This section demonstrates the robustness and versatility of the proposed taxonomy by systematically applying it to three real-world case studies: jamming of Ukrainian drone communication (2022), jamming of GPS signals in the South China Sea (2019), and jamming of cellular networks in Cuba (2021).

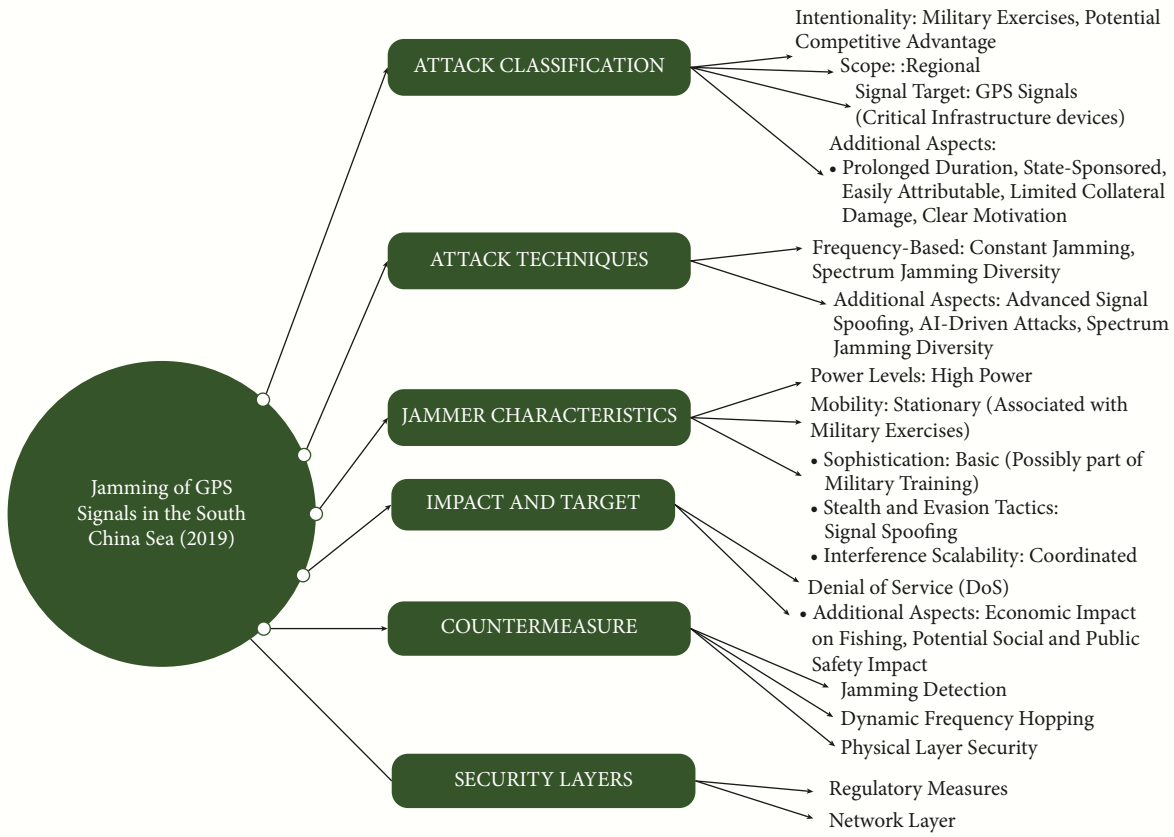

Figure 10: A comprehensive classification of jamming techniques hindering drone communication in the 2019 South China Sea conflict.

5.1. Methodology. The proposed taxonomy was employed to evaluate its effectiveness in categorizing various aspects of the jamming attacks in each case study. This involved applying the taxonomy's dimensions, such as attack types (e.g., continuous jamming), techniques, targets, impacts, countermeasure strategies and security layers to analyze the case studies, and a coding scheme was developed based on the taxonomy dimensions. The specific details of each jamming incident based on the relevant categories within the taxonomy were coded. By applying the taxonomy in this way, the aim is to demonstrate its ability to comprehensively categorize the jamming techniques, targets, and impacts across all three cases. This would help validate the robustness and versatility of the proposed taxonomy for analyzing diverse jamming scenarios.

5.1.1. Applying Taxonomy to the Jamming of Drone Communication in Ukraine (2022). Figure 9 shows that during the ongoing conflict in Ukraine, Russian forces have been accused of using jamming devices to disrupt the communication of Ukrainian drones. This has made it difficult for Ukrainian forces to operate their drones for reconnaissance and surveillance purposes [43].

5.1.2. Applying Taxonomy to Jamming of GPS Signals in the South China Sea (2019). Figure 10 shows that fishermen in the South China Sea reported widespread disruptions to their GPS signals. The jamming was attributed to Chinese military exercises, and it caused significant disruption to fishing and navigation activities in the region [44].

5.1.3. Applying Taxonomy to Jamming of Cellular Networks in Cuba (2021). Figure 11 shows that during antigovernment protests in Cuba, the Cuban government reportedly jammed cellular networks in several parts of the country. This was seen as an attempt to prevent protesters from communicating with each other and organizing demonstrations [45].

6. Discussion and Results

The presented taxonomy, illustrated through case studies like the 2022 drone communication interference in Ukraine and the 2019 GPS signal interruption in the South China Sea, offers valuable insights into cyber threats. It excels at classifying diverse cyberattack features, encompassing sociopolitical motivations, technological nuances, and impacts. Notably, its inclusion of modern attack strategies, jammer features, and security layers distinguishes it from outdated frameworks, enhancing adaptability to evolving threats.

While the taxonomy proves valuable for understanding and mitigating cyber threats, acknowledging its inherent limitations is crucial, particularly in predicting future

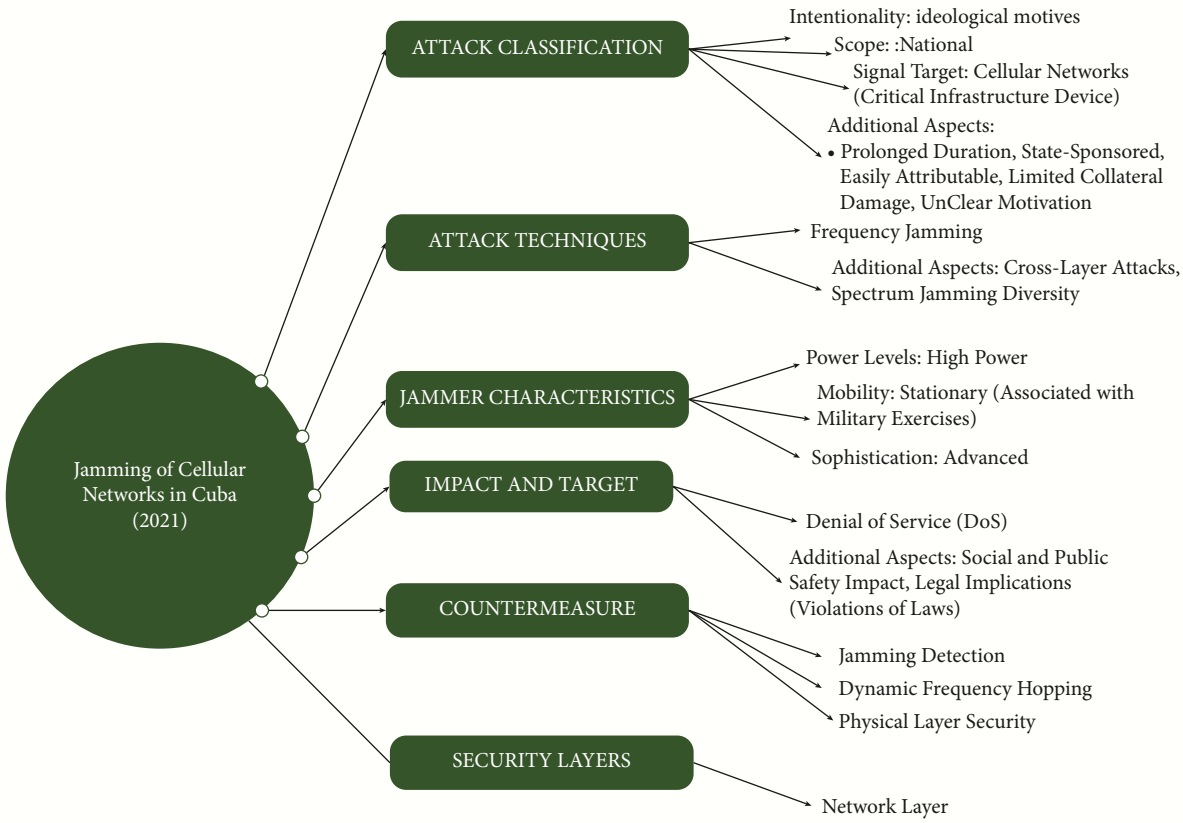

Figure 11: A structured categorization of jamming methods used to impede drone communication in the 2020 Cuban conflict.

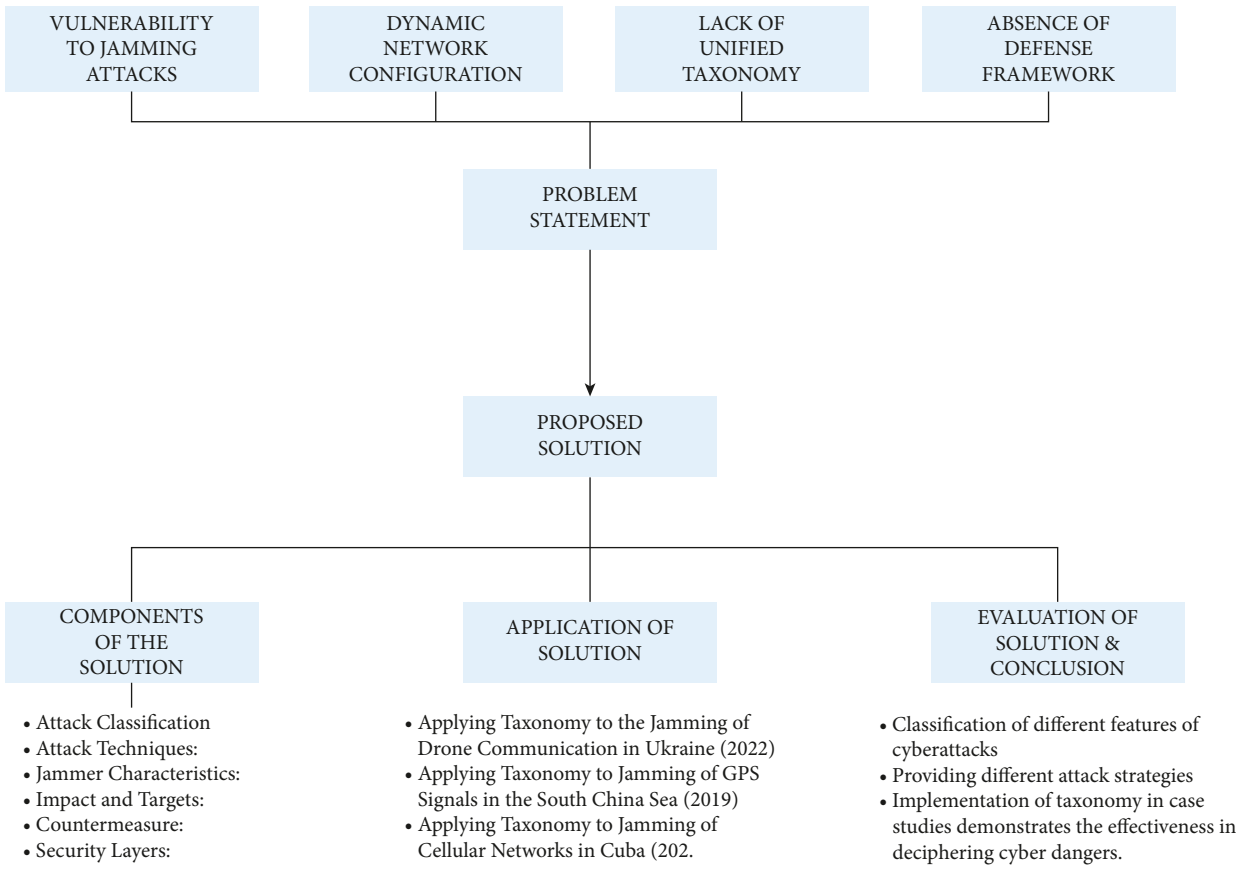

Figure 12: A visual representation of the jamming issue and its proposed countermeasure, highlighting the changes and mitigation strategy.

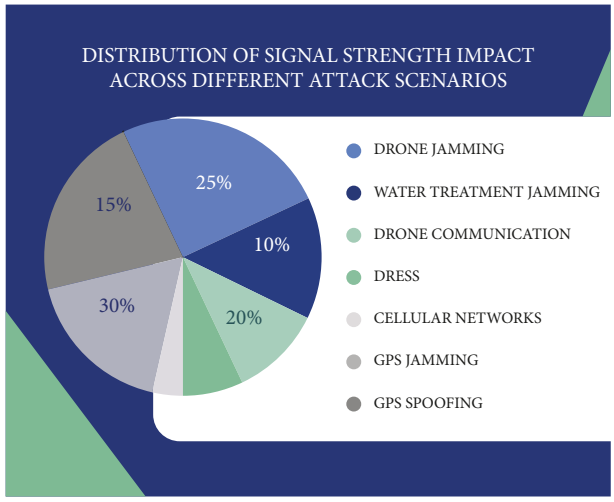

Figure 13: The distribution of signal strength impact.

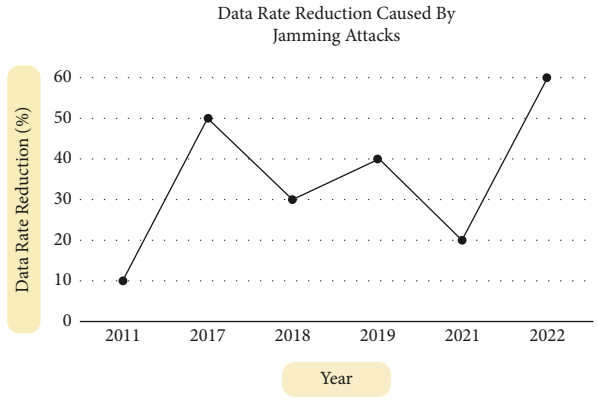

Figure 14: The data reduction caused by jamming attacks.

trajectories. Continuous refinement is essential to align with the dynamic cybersecurity landscape. Applied to real-world situations, the taxonomy aids comprehension and mitigation, serving as a practical resource for researchers, policymakers, and cybersecurity practitioners. Its comprehensive classification allows tailored solutions, enhancing the overall resilience of critical systems.

This research builds upon various previous research on the taxonomy of jamming attacks by delving deeper into the intricacies of 5G's vulnerabilities and attack vectors, offering a more targeted and detailed analysis. While the previous work provides a valuable overview of jamming attacks in wireless networks, this study extends that by specifically addressing the unique challenges posed by 5G infrastructure. By incorporating recent case studies and leveraging incident databases, this taxonomy not only categorizes jamming attacks but also provides empirical validation, enhancing the applicability and reliability of the classification scheme. This focused approach (Figure 12) allows for a more nuanced understanding of 5G jamming attacks, enabling better-informed cybersecurity strategies tailored to the complexities of next-generation networks.

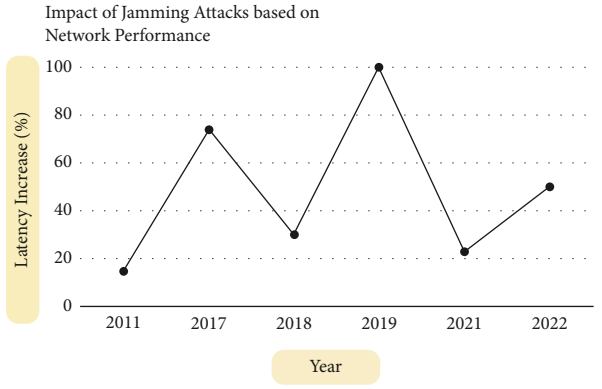

Figure 15: The impact of jamming attacks based on network performance.

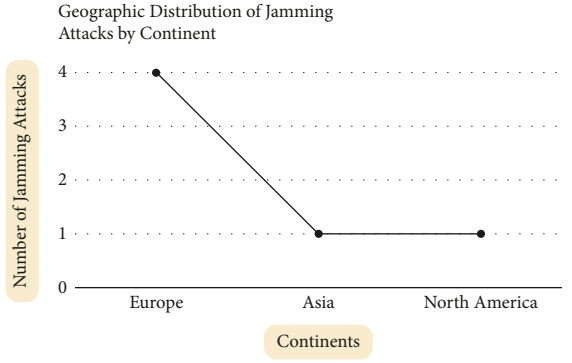

Figure 16: The geographic distribution attacks by content.

6.1. Numerical Analysis of the Case Studies. The pictures clearly show (Figures 13–16) a lot of important information, like how signal strength affects different areas, how data are lost because of jamming attacks, how network performance is affected by jamming attacks, and where attacks happen based on what they are trying to do. These visualizations serve as valuable insights into the quantitative aspects of the examined scenarios, providing a comprehensive understanding of the observed phenomena in each case study.

7. Conclusion

In conclusion, the proposed taxonomy effectively categorizes cyber-attacks, providing a robust framework for in-depth study. Demonstrated through case studies, it proves valuable in deciphering complex cyber threats and showcases adaptability in addressing contemporary cybersecurity issues. Beyond classification, the taxonomy offers a comprehensive understanding by considering technical, socio-political, and economic factors, enhancing defense measures against cyber dangers. This holistic approach, incorporating diverse attack methodologies, jammer characteristics, and security layers, contributes to a more nuanced comprehension of cyber-attacks. To remain relevant, future research should focus on enhancing and expanding the taxonomy to address evolving cyber risks and technology. Additionally, exploring the efficacy of countermeasures and evolving

assault strategies will advance the field's knowledge. Collaboration among policymakers, researchers, and academics is essential for continuous modification of the taxonomy to keep pace with the ever-changing nature of cyber threats. There is scope to delve deeper into advanced attack scenarios beyond the scope of the current taxonomy, such as coordinated jamming attacks orchestrated by multiple malicious actors or attacks targeting specific functionalities of 5G networks, including beamforming techniques or vulnerabilities in network slicing implementations. Enhancing the proposed taxonomy could involve developing dynamic countermeasure strategies capable of adapting to evolving jamming tactics. By incorporating artificial intelligence (AI) or machine learning (ML) algorithms into network defense mechanisms for real-time threat detection and response, 5G networks could become more resilient overall. Expanding the research scope to include security considerations for Internet of Things (IoT) devices and edge computing within 5G networks would be beneficial. This expansion would involve addressing vulnerabilities specific to IoT devices and securing data transmissions in distributed environments, thereby enhancing overall network security posture. Future work could focus on developing collaborative defense mechanisms among network operators, device manufacturers, and security agencies. This collaborative approach would create a unified front against not only jamming attacks but also other cyber threats, fostering a more resilient and secure 5G ecosystem.

Data Availability

No data were used to support the findings of this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Radhakrishnan Delhibabu supervised and conceptualized the study and was also responsible for methodology and writing of the original draft. Sakshi Kuldeep Dhariwal curated data, investigated, and visualized the study. Radhakrishnan Delhibabu reviewed and edited the manuscript. Shruthi Krishnamoorthy provided software and validated the study.

Acknowledgments

The Open Access APC and VIT SEET grants supported this work.

References

[1] Park, "A comprehensive survey on core technologies and services for 5G security: taxonomies, issues, and solutions," *Human-centric Computing and Information Sciences*, vol. 11, no. 3, 2021.

[2] N. Al-Falahy and O. Y. Alani, "Technologies for 5G networks: challenges and opportunities," *It Professional*, vol. 19, no. 1, pp. 12–20, 2017.

[3] N. T. Le et al., "Survey of promising technologies for 5G networks," *Mobile Information Systems 2016*, 2016.

[4] M. Humayun, B. Hamid, N. Jhanjhi, G. Suseendran, and M. N. Talib, "5G network security issues, challenges, opportunities and future directions: a survey," *Journal of Physics: Conference Series*, vol. 1979, no. 1, p. 012037, Article ID 012037, 2021.

[5] P. Marsch, I. Da Silva, O. Bulakci et al., "5G radio access network architecture: design guidelines and key considerations," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 24–32, 2016.

[6] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: a survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, Article ID 106984, 2020.

[7] K. Benzekki, A. El Fergougui, and A. Elbelrhiti Elalaoui, "Software-defined networking (SDN): a survey," *Security and Communication Networks*, vol. 9, no. 18, pp. 5803–5833, 2016.

[8] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: a survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, Article ID 106984, 2020.

[9] Ngmn White Paper, *NGMN Alliance*, 2015, https://www.ngmn.org/work-programme/5g-white-paper.html.

[10] Understanding Perspectives on future technological advancements in mobile, GSMA Intelligence, December, 2014, https://www.gsma.com/solutions-and-impact/technologies/networks/5g-network-technologies-and-solutions.

[11] J. Qiao, X. Shen, J. Mark, Q. Shen, Y. He, and L. Lei, "Enabling device-to-device communications in millimeter-wave 5G cellular networks," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 209–215, 2015.

[12] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, "Energy efficiency and spectrum efficiency of multihop device-to-device communications underlaying cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 367–380, 2016.

[13] M. Dabbagh, B. Hamdaoui, M. Guizani, and A. Rayes, "Software-defined networking security: pros and cons," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 73–79, 2015.

[14] J. Zhang et al., "An architecture for 5G mobile network based on SDN and NFV," *6th International Conference on Wireless, Mobile and Multi-Media (ICWMMN2015)*, vol. 2015, pp. 87–92.

[15] O. Goldreich, "Cryptography and cryptographic protocols," *Distributed Computing*, vol. 16, no. 2-3, pp. 177–199, 2003.

[16] V. O. Nyangaresi, Z. Amin Abduljabbar, and Z. Ameen Abduljabbar, "Authentication and key agreement protocol for secure traffic signaling in 5G networks," *2021 IEEE 2nd International Conference on Signal, Control and Communication (SCC)*, IEEE, 2021.

[17] S. Al and A. Mustafa et al., "Stochastic security ephemeral generation protocol for 5G enabled internet of things," *International Conference on Internet of Things as a Service*, Springer International Publishing, Cham, 2021.

[18] V. O. Nyangaresi et al., "Towards security and privacy preservation in 5G networks," *2021 29th Telecommunications Forum (TELFOR)*, IEEE, 2021.

[19] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: a taxonomic survey," *International Journal of Production Economics*, vol. 172, pp. 76–94, 2016.

[20] V. O. Nyangaresi et al., "Intelligent target cell selection algorithm for low latency 5G networks," *CICom 2021*, Springer International Publishing, Cham, 2022.

[21] V. O. Nyangaresi et al., "Optimized hysteresis region authenticated handover for 5G HetNets," in *Artificial Intelligence and Sustainable Computing: Proceedings of ICSISCET 2021*, 2022.

[22] J. Berg, *Broadcasting on the Short Waves, 1945 to Today*, McFarland, Incorporated Publishers, 2008.

[23] Lichtman et al., "5G NR jamming, spoofing, and sniffing: threat assessment and mitigation," in *Proceeding of the IEEE International Conference on Communications Workshops (ICC Workshops)*, Kansas City, MO, USA, December 2018.

[24] X. Tang, P. Ren, Y. Wang, Q. Du, and L. Sun, "Securing wireless transmission against reactive jamming: a Stackelberg game framework," in *2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2015.

[25] S. Görmüş, H. Aydın, and G. Ulutaş, "Security for the internet of things: a survey of existing mechanisms, protocols and open research issues," *Journal of the Faculty of Engineering and Architecture of Gazi University*, vol. 33, no. 4, pp. 1247–1272, 2018.

[26] L. Sun, P. Ren, Q. Du, and Y. Wang, "Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 291–300, 2016.

[27] B. Upadhyaya, S. Sun, and B. Sikdar, "Machine learning-based jamming detection in wireless IoT networks," in *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, pp. 1–5, 2019.

[28] P. Kryszkiewicz and M. Hoffmann, "Open RAN for detection of a jamming attack in a 5G network," *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, pp. 1-2, 2023.

[29] J. Li et al., "Jamming attacks on wireless networks: classification, countermeasures, and challenges," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 1107–1124, 2013.

[30] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5G new radio: a review," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1010–1015, IEEE, 2020.

[31] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE communications surveys tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[32] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: a comprehensive survey," *IEEE communications surveys & tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[33] A. Proano and L. Lazos, "Selective jamming attacks in wireless networks," in *Proceeding of the IEEE International Conference on Communications*, Cape Town, South Africa, May 2010.

[34] R. H. Mitch et al., "Signal characteristics of civil GPS jammers," in *Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Myrtle Beach, SC, USA, May 2011.

[35] S. Shahabi, H. Fazlalizadeh, J. Stedman, L. Chuang, A. Shariftabrizi, and R. Ram, "The impact of international economic sanctions on Iranian cancer healthcare," *Health Policy*, vol. 119, no. 10, pp. 1309–1318, 2015.

[36] T. S. Rappaport et al., "5G wireless systems: advancements in radio access technology," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 1, pp. 132–147, 2018.

[37] J. G. Andrews, S. Buzzi, W. Choi et al., "What will 5G be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[38] A. Samaddar and A. Easwaran, "Online schedule randomization to mitigate timing attacks in 5G periodic URLLC communications," *ACM Transactions on Sensor Networks*, vol. 19, no. 4, pp. 1–26, 2023.

[39] J. G. Andrews, S. Buzzi, W. Choi et al., "What will 5G Be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, June, 2014.

[40] J. Singh, I. Woungang, S. K. Dhurandher, and K. Khalid, "A jamming attack detection technique for opportunistic networks," *Internet of Things*, vol. 17, no. 2022, Article ID 100464, 2022.

[41] X. Li, H. N. Dai, M. K. Shukla, D. Li, H. Xu, and M. Imran, "Friendly-jamming schemes to secure ultra-reliable and low-latency communications in 5G and beyond communications," *Computer Standards & Interfaces*, vol. 78, no. 2021, Article ID 103540, 2021.

[42] W. Xu et al., "The evolution of jamming attacks in wireless networks," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1, pp. 294–331, 2016.

[43] S. Adepu, J. Prakash, and A. Mathur, "WaterJam: an experimental case study of jamming attacks on a water treatment system," *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2017.

[44] A. Grant, P. Williams, N. Ward, and S. Basker, "GPS jamming and the impact on maritime navigation," *Journal of Navigation*, vol. 62, no. 2, pp. 173–187, 2009.

[45] R. Muraleedharan and L. A. Osadciw, "Jamming attack detection and countermeasures in wireless sensor network using ant system," *Wireless Sensing and Processing*, vol. 6248, 2006.