applied sciences

MDPI

Article

Review of Physical Layer Security in 5G Wireless Networks

Jawhara Boodai [1,*], Aminah Alqahtani [1] and Mounir Frikha [2]

[1] College of Computer Science and Information Technology, King Faisal University (KFU), Al-Ahsa 31982, Saudi Arabia; 223002599@student.kfu.edu.sa
[2] Department of Computer Networks and Communications, King Faisal University (KFU), Al-Ahsa 31982, Saudi Arabia; mmfrikha@kfu.edu.sa
* Correspondence: 222453718@student.kfu.edu.sa

Abstract: Fifth generation (5G) wireless networks promise to revolutionize the way we communicate and connect to the internet. However, as with any new technology, 5G networks also bring new security challenges that need to be addressed. One of the key areas of concern is physical layer security, which refers to the protection of the physical layer of the network against attacks that could compromise its integrity and availability. In this systematic review, we examined the current state of research on physical layer security in 5G wireless networks. Our search identified 36 relevant studies that focused on various aspects of physical layer security, including threat models, vulnerabilities, and mitigation techniques. The findings of the review suggest that whereas some progress has been made in developing physical layer security solutions for 5G networks, such as advancements in multi-antenna systems, interference exploitation, secrecy metrics, and understanding the impact of fading channels, there is still much work to be performed. Further research is needed to develop more effective security solutions and risk assessment frameworks, as well as to evaluate the effectiveness of existing solutions under different conditions and scenarios. Collaboration between industry, academia, and government agencies will also be essential to address the physical layer security challenges in 5G wireless networks. The idea of the proposal is physical layer security in 5G wireless networks. We conduct proper research on this paper and analyze 45 papers to understand this topic in depth. Our research's integrity is built on a commitment to our core principles, which include objectivity, honesty, transparency, fairness, accountability, and stewardship. These managing ideologies aid in confirming that knowledge is innovative through the research zone.

Keywords: physical layer security; 5G wireless networks; threat models; vulnerabilities; mitigation techniques; risk assessment; security solutions; collaboration

Citation: Boodai, J.; Alqahtani, A.; Frikha, M. Review of Physical Layer Security in 5G Wireless Networks. *Appl. Sci.* **2023**, *13*, 7277. https://doi.org/10.3390/app13127277

Academic Editor: Christos Bouras

Received: 11 May 2023
Revised: 8 June 2023
Accepted: 12 June 2023
Published: 19 June 2023

1. Introduction

Physical layer security (PLS), which acts at the physical layer of the communication system, is a new method for securing wireless communication. PLS is essential to the security, integrity, and availability of user data in 5G wireless networks. PLS offers security without relying on cryptographic methods, which can be computationally demanding and subject to assaults, which is one of its key benefits. To establish a secure communication link between the sender and receiver, PLS instead takes advantage of the special characteristics of wireless communication channels, such as fading, interference, and noise. Beamforming is the name of one of the PLS techniques. Instead of sending the wireless signal everywhere, beamforming entails directing it to a single receiver [1]. This may aid in preventing eavesdropping by users who are not authorized and outside the beamforming range. Artificial noise (AN) injection is another PLS method. To make it more challenging for eavesdroppers to obtain useful information from the wireless signal, AN injection involves injecting random noise into the transmission. This method can help to increase communication link security without the need for any additional encryption or decoding. In order to give a multi-layered approach to security, 5G wireless networks also incorporate additional

security features, including encryption and authentication [2]. These steps combine with PLS to offer a complete security solution that can defend against a variety of attacks. PLS is a crucial component of 5G wireless network security and is necessary to guarantee the security and privacy of user data. PLS is projected to become a more crucial instrument for safeguarding wireless communication networks as the adoption of wireless communication rises. PLS for 5G wireless networks uses a number of other techniques in addition to beamforming and synthetic noise injection [3]. To help ensure that the receiver can correctly decode the message even if some of the bits are corrupted during transmission, channel coding involves adding error-correcting codes to the wireless signal [4]. This can help to ensure data integrity and avoid eavesdropping. The wireless signal is sent using several frequencies during frequency hopping, which involves quick and unpredictable frequency changes. As a result, it would be more challenging for an eavesdropper to concurrently collect the communication on numerous frequencies [5]. Spatial diversity is the process of an eavesdropper that would need to intercept all of the antenna pathways, which can help to increase the communication link's security and reliability. Before transmission, a mathematical change is applied to the wireless signal to help reduce interference and increase the dependability of the communication link. Between the sender and recipient, a safe and dependable communication relationship is established using all of these methods. In order to provide a multi-layered approach to security, 5G wireless networks also use additional security mechanisms such as network slicing, secure boot, and secure element [6]. Big data, connected vehicles, smart cities, and IoT are some of the significant social applications brought on by the launch of 5G and beyond, emphasizing the importance of strong security. Researchers are essential in creating secure solutions that safeguard privacy, secure data, and protect devices from illegal access. The importance of security for broadband and mobile networks drives researchers to improve physical layer security in 5G networks.

2. Methodology

The research methodology for this study on physical layer security in 5G wireless networks followed a systematic review approach using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology. During the identification stage, the Google Scholar database was searched using the inclusion and exclusion criteria in Table 1. The papers that were included were those that focus on physical layer security in 5G networks and were published between 2014 and 2023 in academic journals or conference proceedings, which were listed as the source type.

Table 1. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Studies that focus on physical layer security in 5G wireless networks.	Studies that do not focus on the physical layer security in 5G wireless networks.
Studies that investigate security issues, vulnerabilities, and threats in the physical layer of 5G wireless networks.	Studies that focus on other layers of the 5G network or on other wireless networks.
Studies that propose or evaluate physical layer security solutions or mechanisms for 5G wireless networks.	Studies that are not related to security, vulnerabilities, or threats in the physical layer of 5G wireless networks.
Studies that are published in peer-reviewed journals or conference proceedings.	Studies that do not propose or evaluate physical layer security solutions or mechanisms for 5G wireless networks.

This review article aims to analyze the current state of research on physical layer security in 5G wireless networks. Papers that were excluded were those of studies that do not focus on the physical layer; studies that focus on other layers of the 5G network or on other wireless networks; studies that are not related to security, vulnerabilities, or threats in

the physical layer of 5G wireless networks; studies that do not propose or evaluate physical layer security solutions or mechanisms for 5G wireless networks; studies that were not written in English. Furthermore, some documents were not available online. The Figure 1 explains the PRISMA methodology. The PRISMA flowchart was used to guide the selection of articles [2]. The PRISMA flow diagram passes through four stages. The identification stage is when items are identified for review, and during this stage, the papers were identified from Google Scholar. The screening stage is when the papers are screened and selected for review. The eligibility stage is when the papers are eligible to be included [7]. The inclusion stage yields a list of studies to be included in the systematic review. Figure 1 shows that 3500 articles were selected during the identification stage after using the search string ("psychical layer security" OR "5G security"). At first, 2626 articles were rejected because of exclusion criteria. At the screening stage, 874 articles were reviewed for title and abstract, and all but 252 were rejected. Next, out of the 252 articles, only 89 were accepted due to the exclusion criteria at the eligibility stage because they did not closely fulfill the requirements, leaving only 45 articles to be included in the review.

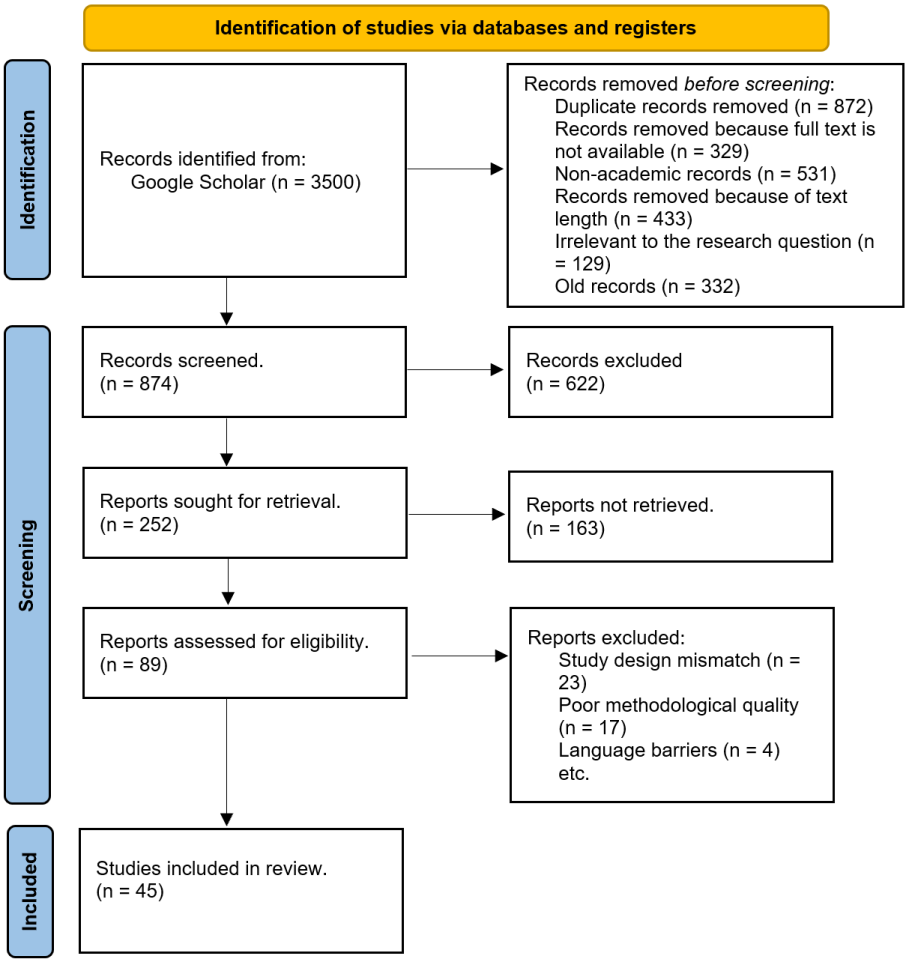

Figure 1. PRISMA flowchart.

3. Literature Review

Y. Gao and S. Hu et al. [8] proposed that encryption is one practical method for preserving security and privacy in social networks. To prevent wireless leakage and boost information security, physical layer security is increased. Several academics are researching physical layer refuge in wireless complexes relevant to 5G. The performance of network security will be impacted by both physical and logical connections, and this study primarily focuses on the security challenges of the physical level in extensive social linkages. Part III summarizes the prospects for physical layer safekeeping in communal linkages,

whereas Part IV discusses the challenges. Part II discusses the characteristics of physical layer security in large-scale social networks. The majority of security measures used in the design and actions of the current safety network are constructed on the encryption algorithm and key. This coordination of encryption operates beyond the physical level (in the MAC layer, linkage layer, application layer, etc.). The equation is used to express the safety amount in the MIMO scenario

$$Cs = maxQ : Q \geq 0, Tr(Q) \leq P[log|I + HQHH| - -log|I + GQGH|] \quad (1)$$

In Equation (1) Cs is the channel capacity, Q is the input covariance matrix, and we assume that H and G are perfectly known as Alice and Bob. System layer, linkage layer, and cross-layer optimization could increase the level of physical layer refuge. However, the use of physical layer safety is still constrained by ideal assumptions. In this study, which serves as a review article, we suggest some new possibilities for physical security in 5G-based massive communal networks that we must highlight in subsequent research.

N. Yang, L et al. [9] found that upcoming wireless applications will require an ultra-high data amount, an ultra-wide radio analysis, an ultra-large quantity of expedients, and an ultra-low invisibility, and the fifth generation (5G) network will be a critical facilitator in addressing these expectations. The popularity of numerous intelligent devices has fueled an extraordinary increase in data circulation in mobile wireless communication in recent years. For the 5G era, for instance, academic institutions are investigating reliable and effective wireless transmission technologies, such as the heterogeneous network (HetNet). In the 5G era, the HetNet is a promising design for network densification. The HetNet aims to deliver a system that is both spectrum and energy efficient and meets the dramatically rising data requirements of future wireless applications. We assume that the pico- and macrocells operate in the same frequency range. Macrocell HPN and picocell LPN positions adhere to independent homogeneity. Based on the knowledge from the domains of graph theory and stochastic geometry, the impact of the positions of HPNs and LPNs on physical layer security can be investigated. Massive MIMO systems are a developing research area that has piqued the interest of both academics and businesspeople. Consuming very huge antenna arrays (usually tens or even hundreds) at the transmitter and/or headset allows for the massive MIMO technique's advantages to be realized. The paper's main objective is to explain how the path to 5G is practically unavoidable and how this will have a significant impact on how physical layer security is designed. In this work, they described the technical difficulties brought on by HetNet, massive MIMO, and mm-wave communication while also identifying the scientific prospects. The innovative solutions created have the potential to significantly increase data secrecy and usher in a brand new security paradigm that is deserving of the 5G moniker.

F. J. Lopez-Martinez et al. [10] stated that for decades, the moment-generating function (MGF) has been a crucial component of announcement theory as a tool for assessing the effectiveness of communication systems in a variety of situations. For the majority of common fading distributions, the MGF of the signal-to-noise ratio (SNR), which is well-defined as the Laplace change in the likelihood solidity function (PDF), is well-known. The remaining part of this paper is organized as mentioned: The primary mathematical assistances of this study are addressed in Section 2, the most pertinent of which is a common technique for determining the IMGF of some given fading circulation. Furthermore, all of the special instances covered have closed-form formulas for the IMGF. These mathematical findings are then used in Section 3 to propose an IMGF-based strategy for the physical-layer refuge examination in wireless systems and to show in what way other interesting wireless communications scenarios may also be studied by consuming the IMGF. Results in numbers are provided in Section 4. Moreover, this finding implies that the IMGF of any circulation for which neither the CDF nor the MGF is known in the secure form will probably lack a closed-form expression. The opposite Laplace renovation operation conducted by the MGF can be used to obtain the IMGF of any non-negative RV in a fairly broad manner.

According to "On the control of the imperfect mgf with applications to wireless transportations" paper [10], there is a basic relationship between the incomplete MGF of a progressive unplanned variable and its whole MGF. As illustrated in the Figure 2, the major conclusion is that whereas the IMGF is anticipated to have a practical shape comparable to that of the CDF, evaluating it should not be very complicated. For the first time in the literature, closed-form equations for the IMGF of the shadowed circulation (and all the special instances contained therein) have been developed. With the eavesdropper's link undergoing shadowing fading and the targeted link being exaggerated by any random fading distribution, this has allowed us to provide a novel structure for the examination of physical layer refuge.

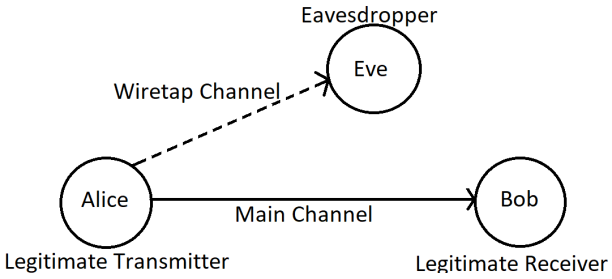

Figure 2. The fundamental physical layer security channel model, which consists of three nodes: Alice (legitimate transmitter), Bob (legitimate receiver), and Eve (eavesdropper).

W. Stallings et al. [11] stated that communication must be kept secret to prevent information from reaching prospective enemies. Providing secure communications is difficult due to the transmission nature of wireless communications. The physical layer refuge is discussed, which exploits the wireless channel's physical layer properties (such as diversity or independence) to accomplish secrecy. It depicts the fundamental model that is typically considered for PLS. According to this paradigm, the legitimate transmitter and receiver communicate with each other over the main channel while an outsider uses the so-called wiretap channel to passively listen in on their conversations. Claude Shannon introduced the PLS concept in their landmark article. Shannon proposed that evidence of theoretical secrecy for such a system is given by H(M | X), where H stands for the entropy of M assumed X.

The receiver is made up of Nr antennas, whereas the transmitter has Nt antenna components. Nt × Nr matrix Hab represents the appropriate channel from Alice to Bob. The eavesdropper *Ye* and Bob *Yb* receives signals that are provided by

$$Yb = HabX + nb \tag{2}$$

$$Ye = HaeX + ne \tag{3}$$

Channel estimation is a key component of many PLS systems, as we have demonstrated above, whether it's because an exact estimation of the legal station is needed at the receiver or because the eavesdropper must not be aware of the valid channel state information. Thus, this paper offers a tutorial on the PLS and newly developed real-world methods for maintaining confidentiality. The multiple problems that PLS currently faces can be resolved using MIMO-based approaches. Moreover, relay networks can help to secure communication between authorized couples. Multiple antennae and relay-based secrecy approaches are vulnerable because they rely too heavily on reliable channel predictions. Solutions for reliable, secure communications are promised by the use of secure channel estimation algorithms. The DCE-based (Differential Channel Estimation) methods might be able to offer useful PLS. To match the presentation of DCE with other privacy strategies, quantitative studies are needed. To offer reliable and secure communication, future work should concentrate on combining DCE with MIMO-based secrecy approaches.

B. He and X. Zhou et al. [12] declared that due to the widespread use of wireless devices in modern life, an extraordinary quantity of private and complex info is exchanged across wireless stations. As a consequence of the wireless medium's inherent openness, security challenges related to wireless communications have grown urgent. From a practical standpoint, the privacy outage likelihood has two boundaries: (1) it cannot characterize the quantity of data that is disclosed to an observer when an outage happens, and (2) it cannot provide any info regarding the listener's capacity to decipher personal messages. In this study, they offer three novel secrecy metrics for secure broadcasts over quasistatic disappearing channels, which are encouraged by the constraints of the privacy outage likelihood. The first measure provides a connection between the idea of a privacy outage and the ability of an eavesdropper to decode messages. For the practical implementation of secure wireless networks, the second metric offers an error probability-based secrecy meter. The third statistic describes how much or how quickly private information is disclosed to the listener. They demonstrate how the proposed secrecy metrics, when taken as a whole, provide a more thorough knowledge of physical layer safety over disappearing channels and allow one to properly design protected message systems with various secrecy measurement philosophies.

F. Ud Din et al. [13] described research that proposes a physical-layer refuge pattern for an inspired relay-based cognitive radio network (CRN), where the medium access technology is an orthogonal frequency-division multiplexing (OFDM). The issue of spectrum scarcity, which is brought on by the widespread usage of wireless range for multiple determinations, is addressed by cognitive radio. In cognitive radio linkages, a secondary consumer, or cognitive radio (CR) consumer, can unscrupulously access the spectrum used by the primary user (PU), as long as the PU is sedentary as long as the level of interference from the CR user communications with PU communications is below a predetermined threshold. The suggested technique can greatly increase the confidentiality rate while sustaining the interference limits put in place to protect the PU's transport network from damaging interference, as demonstrated by simulation results. We also demonstrated that, despite being computationally simpler, the suggested strategy closely approximates the exhaustive search technique, which serves as its upper bound.

H. A. Shah et al. [14] proposed a two-stage safe hybrid beamforming technique with artificial noise (AN) assistance, suggested for MIMO mm-wave relay systems from the standpoint of physical layer security. Wireless service providers are under increased pressure to solve the world's bandwidth constraint as a result of the explosive rise of mobile data traffic and mobile terminals. One of the most important technologies for upcoming mobile communications is millimeter wave (mm-wave), which can offer spectrum resources up to GHz bandwidth. Traditional microwave systems incorporate the beamforming methods in the baseband using digital signal processing, which gives the beamforming matrices better control. RF chains are normally used significantly less frequently than antennas in mm-wave communications. They amplify and forward (AF) relaying systems, which is the subject of the proposed method. In this system, K data streams are transmitted by the source during phase I, and during phase II, the relay amplifies the signals it receives and transmits them to all K destinations. We presume that various listeners wiretap the kth destination during both phases. The non-collusion and passive eavesdropping instances are taken into consideration, which is a typical premise in many different genres of writing. They recommend a two-stage locked hybrid beamforming technique in this study for a MIMO mm-wave relay eavesdropping system where the source and relay serve various destination nodes and the analog and digital beamforming designs are separated. In the second stage, the source employs the ZF technique to create an information signal digital beamforming matrix depending on the effective channel to remove interference between various destinations.

S. Wang et al. [15] improve physical layer security. This study suggests a brand-new channel training (CT) approach for a full-duplex receiver. The receiver, which has N B full-duplex antennas, simultaneously receives and sends a signal carrying information (AN).

The receiver must estimate the self-interference channel before the data communication phase to limit the non-cancellable self-interference caused by the broadcast AN. In the proposed CT method, just a small number of internal pilot symbols are transmitted by the receiver. This covert CT technique efficiently reduces the eavesdropping capabilities by preventing an observer from estimating the jamming route from the observer to the receiver. Analytically, we investigate the secrecy outage chance due to eavesdropping for the proposed secret CT technique as well as the connection probability of the legitimate channel. Our analysis demonstrates that when the number of antennas at the eavesdropper is greater than one, the newly suggested secret CT method greatly outperforms the non-secret CT strategy that uses pilots who are known to the public.

S. Yan, X. Zhou et al. [16] proposed that the fifth generation (5G) of mobile networks seeks to achieve previously unheard of levels of capacity and performance, including ultra-high data rates, ultra-wide radio coverage, vast numbers of concurrently connected devices, and ultra-low latencies. Millimeter-wave (mm-wave), device-to-device, machine-type, and vehicular communications are only a few of the novel wireless system possibilities covered by 5G. The worldwide wireless communications industry refers to fifth-generation wireless technology as "5G", and it aims to achieve multiple-fold improvements in crucial wireless communication areas. Major research institutions and businesses are looking into millimeter-wave (mm-wave) and THz frequencies and technologies in addition to traditional microwave frequencies. This paper proposes a special issue covering many of the technological issues that need to be resolved to usher in the 5G era, and they provide in-depth insights and encouraging outcomes.

D. Liu et al. [17] conducted the research that because of smartphones, the desire for high-definition multimedia content, and an increase in base stations, mobile wireless communication networks have seen a notable increase in data traffic in recent years (BS). Although many experts have worked to address this security issue in the 5G network, it is still unclear how sensitive data are protected in wireless connections. Opposed to cryptography, physical layer security offers two key advantages that make it a preferable option for the 5G network. The first benefit is that, in the event of illegal access to data in the 5G network, the physical layer security mechanisms employed would not be influenced by computing complexity. This suggests that no compromises or trade-offs would be necessary for the attained level of security. The physical layer security technique's tremendous scalability is its second benefit. Devices can be connected to a variety of nodes in 5G networks, each of which has a varied level of processing capability and power needs. Furthermore, because of the decentralized network architecture, devices tend to connect to or disengage from the network at different times. Cryptographic encryption for security would be challenging as a result. Physical layer security can directly secure the transmission of sensitive data or even support cryptographic encryptions in the 5G network.

A. Mathur et al. [18] examine the privacy presentation of the traditional Wyner's wiretap ideal, which models the central and eavesdropper networks consuming a flexible and all-purpose fading model. A proposed model to improve conservation privacy in contradiction to snooping in wireless message networks is physical layer security (PLS). The typical privacy aptitude and confidentiality outage possibility have new and precise expressions. Furthermore, the resulting results can also be used to analyze the privacy view of specific topic dimensions (such as those in millimeter tendency transportations), which could not be completed using the earlier findings. In the active eavesdropping scenario of the ASC Analysis, node B has access to occupied channel state info mutually for the central and eavesdropper stations. To learn more about the ASC, asymptotic analysis is employed. This study is conducted on behalf of the ASC's presentation in the great transfer SNR command, supposing that B = E. As a result, we can see from Figure 3 that there is no enhancement in ASC through increasing transmit SNR. Similar to this, the ASC improves when it is decreased from 1 to 0.7 for =2, =0, and =p. In Figure 4, they match the SOP for various values of E and Rs = 1 as a function of B. The graphic illustrates how the SOP declines as the eavesdropper SNR, E, rises as in figure Figure 5.

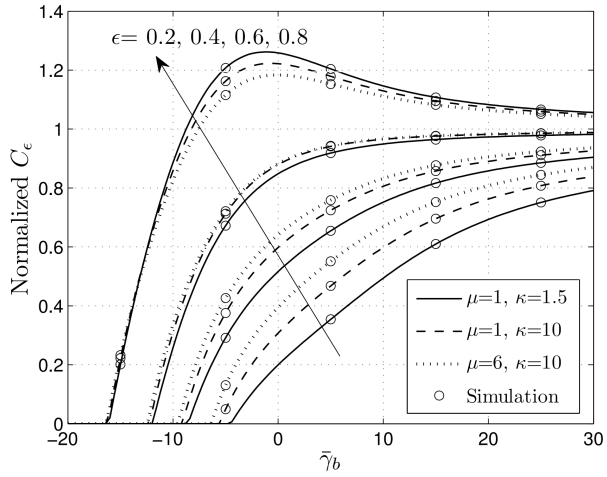

Figure 3. Normalized—ϵ outage privacy volume C under $\kappa-\mu$ observed fading as a job of γ'b. Parameter standards: m = 2, γ'e = −10 dB.

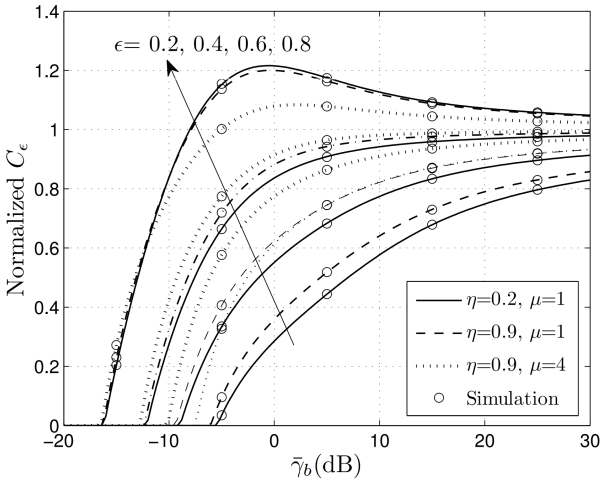

Figure 4. Normalized—ϵ outage privacy volume C under $\eta-\mu$ disappearing as a task of γ'b. Parameter worth: m = 2, γ'e = −10 dB.

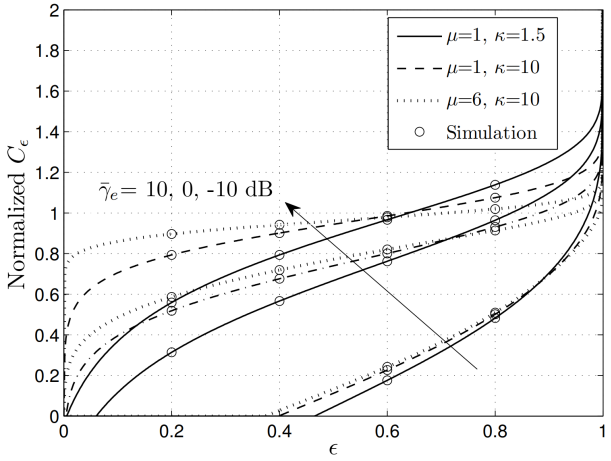

Figure 5. Normalized—ϵ outage privacy volume C under $\kappa-\mu$ as as a task of ϵ. Parameter worth: γb = 10 dB.

W. Zeng et al. [19] explored that due to the substantial amount of accessible bandwidth at mm-wave frequencies, millimeter layer (mm-wave) transportations have drawn interest

as a feasible method for sustaining exponentially rising data rates in 5G. One of the most important elements in the success of 5G is communication. The PHY security in mm-wave conservations through FTR vanishing channels is examined in-depth in this study. The PHY refuge examination for mm-wave transportations has extensively used Wyner's wiretap model. The FTR channel model includes ground reflections in mm-wave channels and features two inconsistent specular constituents with variable stages in addition to a verbose element. In terms of straightforward functions, they originate systematic equations on behalf of the SPSC, ASC, and SOP that can rapidly and progressively congregate with as rare as N expressions as necessary to achieve the requisite precision. The research confirms that by raising the ordinary SNR of the core channel or lowering the middling SNR of the observer station, the performance of the system under consideration can be enhanced. Additionally, the observer network's light surveillance will raise the SPSC. Regarding up-to-date and upcoming instructions, it would be interesting to look into how well mm-wave communications perform in terms of PHY security by considering more useful network and structure functions such as impasses, structure, and multi-antenna.

H. Bocheand et al. [20] analyze different characteristics intended for the enhancement of the Medium Access Control (MAC) and the expansion of a robust locked communication solution. There are conference chores in which the Dueck proof of identity strategy is significantly further effective rather than Shannon's communication pattern, such as in the resulting generation linking systems that trust on reliable and lesser invisibility material sharing. The illogically changing bug frequency (AVWC), which simulates cramming assaults and offers a programming technique for safe proof of identity and figuring out the AVWC's mystery volume, is the main focus of this article. We also examine this capacity function's crucial characteristics, such as steadiness and super complexity. These characteristics are crucial for the optimization of the Medium Access Control (MAC) and the expansion of a robust refuge communication solution.

Y. Zou et al. [21] provided an overview of the problems with wireless security and the defence mechanisms designed to defend the availability, authenticity, secrecy, and integrity of wireless transmissions from malicious attacks. In order to fulfill the exponentially growing demand, wireless transportation substructures and facilities have been expanding over the past few decades. The announcement nodules in wired linkages are materially associated with cables. Wireless linkages, in comparison, are very susceptible as the wireless equipment is the transmission. In this article, we examine the variety of wireless outbreaks and refuge risks that might come across several etiquette coatings, ranging from the application level to the physical layer. The threats are characterized by application layer and transport layer attacks, network layer, MAC layer, and physical layer attacks. Then, in the circumstance of numerous extensively used remote linkages, such as Bluetooth, LTE, and Wi-fi, present refuge standards and procedures designed on behalf of defending in contradiction of attacks on the various protocol coatings have been swotted. More specifically, a number of physical layer security methods have been given and contrasted, containing information-theoretic refuge, simulated noise-aided refuge, diversity-assisted refuge, and physical-layer undisclosed key cohort processes. We have also provided an overview of the major wireless jamming assault types, as well as methods for detecting and avoiding them.

A. Mukherjee et al. [22] explained a thorough analysis of physical layer refuge in multiuser remote linkages. In order to guarantee trustworthy or sheltered transportation in the existence of oppositional consumers, the two essential properties of the remote medium—broadcast and superposition—present several obstacles. They began by providing a general overview of the information-theoretic security foundations going back to Shannon, Wyner, and Maurer's ground-breaking work. They then discussed how locked communication policies evolved from point-to-point networks to several antenna structures before generalizing to greater multiuser linkages. Only a few of the potential directions for future research in this area are discussed here. For instance, there has not been much research into how physical layer security approaches might be applied to commercially

available wireless systems. The majority of the methods included in this review are independent of the fundamental air edge, such as generated sound for observer jamming and CSI-based precoding to maximize privacy rates. After distributing the data with a pseudo-noise sequence, a CDMA transmitter might carry out the same action. Another rich but untapped area for research is a greater comprehension of the interactions between traditional cryptography security and physical layer security. Secure transmission techniques that keep the secret message concealed so that possible listeners are unsure whether transmissions are in progress are also of interest at the moment.

Akram and R. N.'s [23] study examines how quantum computing can affect actual security, concentrating on how it might affect 5G networks. The authors analyze the risks posed by quantum computers and examine vulnerabilities in the current cryptographic systems used in 5G networks. They offer insights into the challenges and opportunities involved with incorporating quantum-safe protocols into current infrastructure and propose a novel quantum-safe security mechanism created for 5G systems. The main conclusions highlight the serious threat that quantum computers pose to the security of cryptographic systems in 5G networks, the vulnerability of the current security mechanisms to quantum computer attacks, and the requirement for quantum-safe cryptographic algorithms and protocols to guarantee the long-term security of 5G networks. The paper also underlines the importance of giving different technical and practical difficulties due thought when incorporating quantum-safe protocols into the current 5G infrastructure. Finally, the authors propose post-quantum cryptography (PQC) and quantum key distribution (QKD) as feasible approaches to attain quantum-resistant security in 5G networks.

In Raza and S.'s study [24], the one-time pad (OTP) is used to improve the Network Time Synchronization Algorithm's (NTSA) secure communication in the context of the Internet of things (IoT). To reduce the vulnerabilities associated with typical cryptographic mechanisms, the authors suggest modifying the NTSA protocol. They explore its benefits and drawbacks while demonstrating how well the OTP-based strategy works for creating secure communication in IoT scenarios. The main conclusions show that due to computational constraints, typical cryptographic mechanisms used in IoT systems may not be able to provide sufficient security. In contrast, using an OTP can considerably increase the NTSA's security in IoT contexts. If the key distribution method is secure, OTP-based communication guarantees complete security. The suggested OTP-based method provides defense against a number of attacks, such as replay attacks and unauthorized access. However, integrating OTP into IoT systems, it is important to carefully consider implementation issues such as key distribution and storage requirements.

With an emphasis on its applications, attacks, and defenses, ref. [25] S. Ullah and S.'s survey article provides a thorough review of the current NIST Lightweight Cryptography Standard. The authors analyze the most recent lightweight cryptographic protocols and algorithms suggested by NIST, evaluating their advantages and disadvantages. The importance of lightweight cryptography in contexts with limited resources is emphasized through the discussion of various attack scenarios and associated mitigation measures. The most important findings highlight the critical function of lightweight cryptography in protecting constrained devices and systems. A selection of lightweight cryptographic algorithms appropriate for these limited situations is suggested by the NIST Lightweight Cryptography Standard. The performance, security, and applicability of the studied algorithms are assessed in relation to several application scenarios. The study explores numerous attacks on lightweight cryptography, such as side-channel attacks and fault attacks, and also offers defenses against these threats. Furthermore, for the actual application of lightweight cryptographic algorithms, implementation aspects including code size, memory needs, and energy usage are essential.

Maqbool, A.'s [26] study on FaultMeter introduced a tool for assessing block cipher software's vulnerability to fault attacks. The authors suggest using a quantitative method to assess how well fault attacks against cryptographic algorithms work. They carry out analyses to assess the fault resistance of various block ciphers, consider the effects of alter-

native fault injection techniques, and provide suggestions for developing fault-resistant encryption protocols. The main conclusions emphasize that fault attacks make use of cryptographic methods' vulnerability to unexpected faults created during execution. FaultMeter offers a quantifiable way to evaluate how susceptible such attacks are to block cipher software. A number of parameters, including fault models, fault injection methods, and the targeted cryptographic algorithm, affect how effective fault attacks are. The study gives experimental findings on the fault vulnerability of popular block ciphers, including AES and Serpent. These findings can guide the design of fault-resistant cryptographic algorithms and help in the development of countermeasures versus fault attacks.

Maqbool, A.'s [27] article provides a thorough review of the security issues and difficulties associated with the 5G network design. The authors look at the core elements of 5G networks and evaluate how they affect security. They examine multiple threats and attacks and offer matching countermeasures to guarantee the confidentiality, integrity, and availability of 5G networks. The main conclusions show that, in comparison to other wireless network generations, the design of 5G networks presents new security challenges. The paper gives a summary of important elements such as base stations, the core network, and user devices, as well as the security issues that are related to them. In the context of 5G networks, several security concerns and attacks, such as identity spoofing, denial-of-service assaults, and eavesdropping, are examined in order to successfully address the security challenges posed by 5G networks. The study highlights the significance of collaboration between network operators, equipment vendors, and regulatory bodies. It also emphasizes the importance of applying countermeasures and security mechanisms including secure key management, authentication protocols, and network slicing.

In order to secure Internet of things (IoT) devices, Shah, H. A.'s [28], review study provides an overview of lattice-based algorithms as post-quantum cryptosystems. The authors discuss typical cryptographic algorithms that are vulnerable to quantum attacks and present lattice-based encryption as a viable alternative. They provide a thorough analysis of different lattice-based algorithms, including NTRU, LWE, and RLWE, emphasizing their security attributes and computing needs. The main conclusions highlight the necessity to investigate post-quantum cryptosystems because typical cryptographic algorithms are vulnerable to attacks from quantum computers. Lattice-based cryptography has the ability to protect against quantum attacks and is appropriate for IoT devices with limited resource availability. The study covers the difficulties of implementing lattice-based algorithms in IoT contexts, taking into account factors such as key size, memory needs, and energy usage. It also highlights how crucial it is to carry out more research in order to improve lattice-based algorithms for effective deployment on IoT devices while retaining the appropriate level of security.

Study [29] illustrates that in order to achieve high performance, the suggested microarchitecture design for the Curve448 and Ed448 elliptic curves on the ARM Cortex-M4 CPU combines parallelization and pipelining. The elliptic curve operations are carried out in parallel by employing several datapaths. By segmenting the elliptic curve operations into stages and carrying out the stages sequentially, the pipelining is accomplished. An innovative approach to lowering the area overhead of the finite field multiplier is also suggested by the design under consideration. The new approach is based on employing a finite field multiplier with fewer bits. The proposed concept was put into operation with a Xilinx Artix-7 FPGA and proved to be up to 2.5 times faster than the prior state-of-the-art implementation. This study makes use of a 32-bit microcontroller called the ARM Cortex-M4 CPU. The article suggests a brand-new microarchitecture for this processor's Curve448 and Ed448 elliptic curves.

Paper [30] shows that compression and acceleration techniques are combined to achieve great performance in the proposed Supersingular Isogeny Key Encapsulation (SIKE) Round 3 implementation on the ARM Cortex-M4 CPU. The compression is accomplished by representing the points on the elliptic curves using fewer bits. A variety of methods, such as pipelining, parallelization, and the usage of unique hardware accelerators, are used to accelerate the process. It was demonstrated that the proposed implementation, which

was put into use on a Xilinx Artix-7 FPGA, could speed up processes by up to 1.5 times compared to the prior state-of-the-art implementation. Another CPU used in this study is an ARM Cortex-M4. For the SIKE Round 3 scheme on this CPU, a new compression method has been proposed in the paper.

In paper [31], the Supersingular Isogeny Key Encapsulation (SIKE) Round 3 method is implemented more quickly using a number of strategies suggested in this research for ARM Cortex-M4 processors. Compression, pre-computation, and hardware acceleration are among the suggested methods. The research analyzes the performance of the suggested strategies on several ARM Cortex-M4 processors and demonstrates that the suggested techniques can result in considerable speedups, up to 10× in some circumstances. The presented methods can be utilized to implement the SIKE Round 3 scheme on ARM Cortex-M4 processors with great performance, according to the paper's conclusion.

Paper [32] shows that using a combination of software and hardware acceleration approaches, the compact implementations of the Kyber post-quantum key exchange protocol on 64-bit ARM Cortex-A processors are based. The usage of pre-computed tables and the use of optimized code are two examples of software acceleration strategies. Utilizing unique hardware accelerators is one of the hardware acceleration strategies. On a Xilinx Zynq UltraScale+ MPSoC, the suggested implementations were put into operation and demonstrated to deliver speedups of up to 10 times over the prior state-of-the-art implementation. On 64-bit ARM Cortex-A processors, compact Kyber implementations were made; a 64-bit general-purpose ARM Cortex-A processor, which is used in this paper, was used. On this CPU, the study suggests an innovative implementation of the Kyber post-quantum key exchange protocol.

Paper [33] highlights that a 32-nm CMOS technology is used to implement the Ed25519 curve-based cryptographic accelerator for digital signatures, which has a throughput of up to 100 million signatures per second. The accelerator is made to be used in many different applications, such as cloud computing, embedded systems, and mobile devices. The accelerator uses a variety of strategies, such as pipelining, parallelization, and the usage of unique hardware accelerators, to attain its high performance. Application-specific integrated circuits are used in this paper. A specialized circuit created for a particular application is known as an ASIC. The research suggests a brand-new Ed25519-based cryptographic accelerator for digital signatures.

Chen et al. [34] present a new approach for identifying faults in finite field multipliers in the study "Reliable CRC-Based Error Detection Constructions for Finite Field Multipliers With Applications in Cryptography" (2022). The technique, which is based on CRC codes, can be used to find single-bit errors in a data stream. The proposed method has been tested on a number of finite field multipliers and has proven to be highly effective at spotting faults. The finite field multiplier is not significantly burdened by the approach, which is also effective. The lightweight stream cipher Pomaranch, which is made for devices with limited resources, can have its fault resistance improved using the suggested technique. The Pomaranch encryption is vulnerable to fault attacks, but the suggested technique can be used to find mistakes in the Pomaranch cipher's finite field multipliers. The cipher has the option to stop and restart if an error is found. The fault resilience of the Pomaranch cipher can be increased by employing the suggested way. An FPGA (field-programmable gate array) is used in this paper. An FPGA is a programmable semiconductor that may be set up to carry out various tasks. The research suggests a novel CRC-based error detection scheme for finite field multipliers.

The authors of article [35] review state-of-the-art lightweight hash functions and assess how well they perform on various IoT devices. The Grostl hash function, a compact hash function created for devices with limited resources, is the main topic of this study. On a variety of IoT devices, the Grostl hash function has been assessed and confirmed to be effective and secure. The firmware implementation, which can be used on a range of IoT devices and is immune to side-channel attacks, is the most dependable architecture for the Grostl hash function. The hardware and software platforms used in this work include

FPGAs, ARM Cortex-A processors, and ARM Cortex-M4 CPUs. Several lightweight hash algorithms are tested for performance on different platforms in the article.

The authors of study [36] introduce a novel technique for fault diagnostics of the low-energy Midori cipher, as proposed in the work by Jikang Lin et al. (2023) titled "From Unbalanced to Perfect: Implementation of Low Energy Stream Ciphers." By analyzing the statistical output of the encryption, the technique identifies errors resulting from flaws in the Midori cipher. The suggested approach is evaluated using multiple Midori implementations, demonstrating a high level of accuracy in fault detection without significantly increasing overhead. The paper concludes that this promising method should be employed to enhance Midori's security. Additionally, the research presents a new implementation of a low-energy stream cipher specifically designed for the ARM Cortex-M4 CPU.

The RECTANGLE cipher's fault diagnostics is paper [37]'s main topic. A compact block cipher developed for devices with limited resources is the RECTANGLE cipher. The bitslice architecture and substitution–permutation network (SPN) are the foundations of the cipher. The study suggests a brand-new hardware RECTANGLE implementation. The bitslice architecture is the foundation of the suggested implementation. A form of architecture known as bitslice divides the encryption into manageable pieces and implements each block concurrently. A range of hardware platforms have been used to assess the suggested implementation. The evaluation's findings demonstrate that the suggested implementation is effective and suitable for use on a range of devices with limited resources. The paper also suggests an innovative approach to RECTANGLE fault diagnosis. The approach is based on the finding that RECTANGLE flaws can lead to incorrect output from the cipher. The technique analyzes the output of the encryption statistically to find errors. The suggested approach has been examined on numerous RECTANGLE implementations. The evaluation's findings demonstrate that the method has a high degree of accuracy in fault detection. The technique is effective and does not significantly increase the cipher's overhead. The proposed method is a potential new approach for RECTANGLE fault diagnosis, the paper finds. The strategy should be utilized to increase RECTANGLE's security, according to the report.On this platform, the article suggests a brand-new hardware implementation of the RECTANGLE algorithm.

Table 2 provides a summary of related research papers, highlighting suggested techniques, advantages, and limitations.

Table 2. Summary of related works.

Author	Publication Year	Type	Suggested Technique	Advantages	Limitations
Y. Gao, S. Hu, et al. [8]	2018	Physical Layer Security Testing	To determine the coverage area and find any signal leakage or interference from unauthorized devices, a wireless signal strength analysis can be conducted. Any unauthorized equipment using the same frequency band can be found via spectrum analysis. Testing for jamming can be conducted to see how well the system resists different kinds of jamming attacks. Testing for interception involves attempting to intercept wireless signals in order to assess the confidentiality of the sent data.	It can be utilized to verify the system's security requirements and guarantee adherence to security standards.	It is unable to solve more complex security problems such as authentication and authorization, which call for separate testing approaches.

Table 2. *Cont.*

Author	Publication Year	Type	Suggested Technique	Advantages	Limitations
N. Yang, L et al. [9]	2015	Physical Layer Security Testing	Channel estimate can be used to assess the wireless channel's quality and find any irregularities that can point to a security risk.	Physical layer security testing offers a thorough assessment of the system's wireless security.	Additional testing could be necessary to guarantee full security coverage because it might not find all kinds of security flaws.
F. J. LopezMartinez et al. [10]	2017	Security Testing	Valuable insights into the mathematical foundations of wireless communications, which can inform the design and development of wireless communication systems.	Fading channels, which are frequently found in wireless networks, are accurately modeled by the incomplete MGF.	It can be challenging to apply the incomplete MGF in practice due to its complexity and the requirement for specialized mathematical tools to calculate it.
W. Stallings. et al. [11]	2008	Network	It provides foundational knowledge that can inform the design and testing of secure network systems.	The book provides practical examples and case studies to help readers understand the material.	The book does not provide specific recommendations for Pen Test Types or testing techniques.
B. He, et al. [12]	2016	Network security	Valuable resource for researchers and practitioners working in the field of physical layer security over quasistatic fading channels	It provides insights into the effects of quasistatic fading channels on physical layer security.	The article focuses specifically on quasistatic fading channels and may not be directly applicable to other types of channels.
F. Ud Din et al. [13]	2018	Physical layer testing	It provides insights into the principles and techniques of physical layer security that can inform the design and testing of secure wireless communication systems.	The article provides practical examples and case studies to help readers understand the material.	The article does not provide specific recommendations for Pen Test Types or testing techniques
H. A. Shah et al. [14]	2018	Physical	Provides insights into the principles and techniques of physical layer security in cognitive radio networks that can inform the design and testing of secure wireless communication systems.	The proposed scheme is based on OFDM technology, which is widely used in modern wireless communication systems.	The article may be too technical for readers without a strong background in wireless communications or signal processing.
S. Wang et al. [15]	2019	Wireless Security Penetration Testing	A wireless security penetration testing approach, involving spectrum analysis and radio signal analysis, can be used to evaluate the effectiveness of the proposed approach and identify potential vulnerabilities in the system.	The proposed approach utilizes artificial noise-aided hybrid analog–digital beamforming for secure transmission.	The effectiveness of the proposed approach may be impacted by environmental factors, such as interference and multi-path propagation.

Table 2. *Cont.*

Author	Publication Year	Type	Suggested Technique	Advantages	Limitations
S. Yan, et al. [16]	2018	Wireless Security Penetration Testing	Man-in-the-Middle Attack Simulation	The article proposes a novel approach to enhancing physical layer security with a full-duplex receiver by using secret channel training.	The proposed model is extremely effective in detecting vulnerabilities and identifying web application threats/risks.
D. Liu, et al. [17]	2017	Vulnerability Assessment	Wireless signal analysis and simulation tools to assess the antenna and propagation characteristics of 5G networks	Helps identify potential interference and signal attenuation issues that can affect network performance.	Requires detailed knowledge and understanding of antenna and propagation characteristics and wireless signal analysis tools.
A. Mathur, et al. [18]	2018	Wireless communica-tion system	An analytical approach to evaluate the physical layer security of wireless communication systems operating in $\alpha - \eta - \kappa - \mu$ fading channels.	The approach is based on mathematical modeling and analysis, which can provide insights into the fundamental aspects of the system design.	The proposed approach is based on certain assumptions and simplifications, which may not represent the real-world wireless communication scenarios.
W. Zeng, et al. [19]	2018	Physical security	Fluctuating Two-Ray Fading Channel Model	The fluctuating two-ray fading channel model can provide a more accurate representation of the physical layer security of wireless communication systems.	The accuracy of the results obtained from the fluctuating two-ray fading channel model is dependent on the accuracy of the model parameters and assumptions made.
H. Boche, C. Deppe [20]	2019	Security	The scheme uses a hybrid approach that combines the advantages of both approaches to improve security against passive eavesdroppers and active jamming attacks.	The proposed scheme provides a high level of security against both passive and active attacks, making it suitable for applications that require strong authentication and protection against eavesdropping and jamming.	The proposed scheme may have high computational and processing requirements due to the use of multiple authentication mechanisms.

Table 2. *Cont.*

Author	Publication Year	Type	Suggested Technique	Advantages	Limitations
Y. Zou, et al. [21]	2016	Wireless security	Conduct a literature review of recent research in wireless security to identify technical challenges, recent advances, and future trends.	This can be useful for understanding the landscape of wireless security, identifying potential vulnerabilities and threats, and informing the development of new security solutions.	A survey paper may not provide detailed technical information on specific security solutions, and it may not cover all recent research in the field.
N. A. Mukherjee et al. [22]	2014	Physical Layer Security Testing	The analysis and conclusions of the paper are limited by the quality of the studies that were reviewed.	Provides a comprehensive overview of the principles of physical layer security in multiuser wireless networks.	The paper may not include the latest research developments and techniques, as it was published in 2014.
Akram, R. N., Khan. [23]	2021	IoT Security	The usage of lattice-based algorithms, a type of cryptographic algorithm built on the conceptual framework of lattices, was used. It examines several lattice-based cryptographic primitives and how to use them to protect IoT connections and devices.	IoT scenarios can use lattice-based cryptography in a variety of ways. Numerous cryptographic attacks, such as those based on number factorization and discrete logarithm problems, have proven resilient against lattice-based techniques.	Due to the requirement for standardization, interoperability, and integration with existing systems, lattice-based algorithms may encounter difficulties in real-world IoT deployments.
Raza, S., Ullah, S. [24]	2020	Network Security	Quantum computing on cryptographic algorithms used in 5G network security.	Emphasizing the possible effects of quantum computing on practical security. Highlights the application of quantum computing to a particular system in the real world.	As the field develops, it could need to be re-evaluated.
Ullah, S., Riaz, M. [25]	2023	Security	Enhances the security of communication in the Internet of things by combining the NTSA secure communication protocol with a one-time pad (OTP).	The suggested method adds an extra layer of security to IoT connection. Focuses on solving the unique difficulties and vulnerabilities that IoT networks deliver in order to improve privacy and security.	One-time pads (OTPs) can add to computational cost, especially in IoT devices with limited resources. The study does not go into great detail on the possible effects on system performance or energy usage.

Table 2. *Cont.*

Author	Publication Year	Type	Suggested Technique	Advantages	Limitations
Maqbool, A., Abbas, H. [26]	2023	Security	Focuses on the NIST Lightweight Cryptography Standard.	Covering a range of topics, including implementations, attacks, and defenses.	The study might not have conducted a thorough analysis of how well lightweight cryptography works in particular real-world situations. It's possible that the conversation will be less practical and more theoretical.
Maqbool, A., Abbas, H. [27]	2023	Security Assessment	The FaultMeter technique, which is designed for quantitative assessment of fault attacks on block cipher software.	By inserting particular flaws into the block cipher algorithm's execution, the technique permits precise analysis. This enables researchers to measure fault propagation and evaluate how susceptible the software is to various fault assaults.	The particular way the block cipher software is implemented may have an impact on how well FaultMeter works. When exposed to fault attacks, various implementations could behave differently, which could have an impact on the technique's reliability and generalizability.
Shah, H. A. [28]	2021	5G Security	Security architecture of 5G networks.	Explains the various standards, protocols, and security techniques employed in the 5G architecture. It offers information on key management, access control, authentication, encryption, and other security-related topics.	The theoretical elements of the 5G security architecture are the main emphasis of the article. There are no in-depth case studies or instances from the real world of security issues or breaches in 5G networks.
Seo, H., R. [29]	2021	Security	New microarchitecture design for Curve448 and Ed448 elliptic curves on ARM Cortex-M4 processor.	Compared to the prior state-of-the-art implementation, achieves a substantial speedup. Compared to the prior state-of-the-art implementation, has a reduced overhead area.	More complicated than the most recent innovative implementation. Not always appropriate for all uses.
Anastasova, M., M. [30]	2021	Security	New compression technique for the SIKE Round 3 scheme on the ARM Cortex-M4 processor.	Reduces by up to 50 percent the size of the points on the elliptic curves. Can result in a significant speedup of the SIKE Round 3 computation.	Not as precise as the initial illustration of the elliptic curve points. May result in a minor loss of security.

Table 2. *Cont.*

Author	Publication Year	Type	Suggested Technique	Advantages	Limitations
Anastasova, M., M. [31]	2021	Security	Number of techniques for accelerating the implementation of the Supersingular Isogeny Key Encapsulation (SIKE) Round 3 scheme on ARM Cortex-M4 processors.	Can result in considerable speedups, perhaps up to 10 times. A number of applications where great performance is needed can leverage this.	Not always appropriate for all uses, maybe calling for more hardware or software resources.
Sanal, P., Karagoz, E. [32]	2021	Security	Combination of software and hardware acceleration techniques for the Kyber post-quantum key exchange protocol on 64-bit ARM Cortex-A processors.	Can significantly speed up compared to the most recent state-of-the-art implementation. A number of applications where great performance is needed can leverage this.	Not always appropriate for all uses, maybe calling for more hardware or software resources.
Bisheh-Niasar, M. [33]	2021	Security	Cryptographic accelerator for digital signatures based on the Ed25519 curve.	Can significantly outperform the most recent state-of-the-art implementation in terms of speed. Is suitable for a wide range of applications where excellent performance is needed.	Not always appropriate for all uses, maybe calling for more hardware or software resources.
Canto, A. C. [34]	2020	Security	Uses cyclic redundancy check (CRC) codes to detect single-bit errors in a stream of data.	Effective at most likely spotting problems. Efficient, and the finite field multiplier is not much burdened.	Might not be able to catch every error. Not as effective as some other methods of error detection.
Abed, S. E., Jaffal, R. [35]	2021	Security	Lightweight hash functions. Focuses on the Grostl hash function.	Secure and effective. Can be applied to a range of IoT gadgets.	Possibly less secure than certain other hashing operations. On some platforms, it might not be as effective as some other hash methods.
Lin, J., He, J., Fan, Y. [36]	2023	Security	Method uses a statistical analysis of the cipher's output to detect faults.	Efficient and does not significantly increase the cipher's burden. Can be used to increase Midori's security.	Possibly unable to find all flaws. Possibly less precise than some other methods of defect diagnosis.

Table 2. *Cont.*

Author	Publication Year	Type	Suggested Technique	Advantages	Limitations
Li, M., Zhao, D., Tang, X. [37]	2020	Security	Proposes a new hardware implementation of the RECTANGLE cipher. The proposed implementation is based on a bitslice architecture.	Efficient and adaptable to a range of devices with limited resources. Additionally suggests a novel technique for RECTANGLE fault diagnosis. The approach is based on the finding that RECTANGLE flaws can lead to incorrect output from the cipher. The technique analyzes the output of the encryption statistically to find errors.	A RECTANGLE implementation that is not as secure as others might be. On some platforms, this RECTANGLE implementation might not be as effective as some other ones.

4. Conclusions

The literature review study on physical layer security in 5G wireless networks concludes by emphasizing the importance of this field of study in addressing the rising demand for secure and dependable communications. The research articles under consideration have highlighted a number of opportunities and difficulties related to physical layer security in 5G networks and have suggested solutions and methods to solve them. The studies, which cover topics including multi-antenna systems, interference exploitation, secrecy metrics, and the effect of fading channels, have made a substantial contribution to our understanding of physical layer security [38]. These inquiries have demonstrated how physical layer security methods can improve the secrecy and integrity of wireless communications in 5G networks. A number of directions require additional investigation, notwithstanding the advancements made. First, improving physical layer security in 5G networks requires researching novel transmission methods [39]. Investigating interference exploitation techniques can also help to improve security precautions. It is crucial to create quantum-safe security mechanisms given the potential threat posed by quantum computing. Furthermore, it is essential to create secure network architectures that successfully incorporate physical layer security. To guarantee the easy acceptance and deployment of secure physical layer solutions in 5G networks, practical implementations, and standardization initiatives need to be given priority [40]. The difficulties in physical layer security can be resolved by addressing these research directions and improving security for 5G wireless networks. This helps with the development and implementation of safe and reliable 5G networks overall while also offering users strong protection against eavesdropping and other security threats [41]. In conclusion, the study recognizes the advancements made in the area and emphasizes the significance of physical layer security in 5G wireless networks. To overcome obstacles and enhance the physical layer security of 5G networks, it also highlights the necessity for more research and development. The objective of realizing safe and dependable wireless communications in the 5G future can be accomplished by concentrating on the indicated research directions.

5. Future Research

5.1. Security and Fading Channel Models in 5G Networks

A noteworthy significance for accurate fading channel models is played in a 5G transmission design that is most secure. Determining more precise channel models that offer

a better fit to field observations in several different mm-wave propagation scenarios has thus been the focus of various studies [42]. According to the authors, Fluctuating Multiple-Ray and N-Wave with Diffuse Power fading models both represent viable alternatives to existing models in this context for describing the propagation environment on mm-wave communications. Consequently, it is crucial to continue researching how PLS approaches perform over these generalized channels [43]. Usually, to provide PLS, other system QoS needs must be sacrificed. For instance, throughput is frequently sacrificed in favor of strong security levels, whereas AN systems compromise power efficiency. Access Control (MAC) and the expansion of a robust locked communication solution also be used to enhance the security of 5G networks.

5.2. Security Solutions for 5G Networks

Opportunities and Collaborative: Efforts Further research is needed to develop more effective physical layer security solutions for 5G wireless networks. This could involve exploring new techniques and technologies, such as machine learning and artificial intelligence, to enhance the security of the physical layer. More research is needed to understand the vulnerabilities of the physical layer in 5G wireless networks and how they can be exploited by attackers. This could involve conducting more in-depth studies of the physical layer and its components to identify potential weaknesses. Future research should focus on developing more comprehensive risk assessment frameworks for physical layer security in 5G wireless networks. These frameworks should consider not only technical vulnerabilities but also organizational, social, and economic factors that may affect the security of the physical layer. There is a need for more collaboration between industry, academia, and government agencies to address the physical layer security challenges in 5G wireless networks [44]. This could involve establishing partnerships to share knowledge and resources, develop new solutions, and address common challenges.

5.3. Evaluating the Effectiveness of Physical Layer Security Solutions in 5G Networks

More research is needed to evaluate the effectiveness of physical layer security solutions in 5G wireless networks. This could involve conducting large-scale experiments and simulations to test the performance of different security solutions under various conditions and scenarios.

5.4. New Transmission Methods

Research and develop innovative transmission methods that can enhance security in 5G networks. Investigating innovative modulation and coding techniques, multiple antenna systems, and beamforming techniques designed especially for physical layer security can all be part of this [45]. To improve the secrecy performance, it is also possible to investigate the integration of innovative technologies such as massive MIMO, millimeter-wave communication, and full-duplex communication.

5.5. Exploiting Interference

Research the use of interference for physical layer security. By intentionally interfering with eavesdroppers' ability to listen in on wireless communications, artificial noise techniques, for instance, can be further refined to increase their secrecy. To reach a compromise between security and system performance, investigate the best configuration and distribution of generated noise in various network settings.

5.6. Quantum-Safe Security

The vulnerability of typical cryptography algorithms is a concern with the development of quantum computers. The development of encryption and key distribution techniques that are specifically designed for 5G networks should be the main emphasis of future research. For example, lattice-based cryptography has demonstrated remarkable potential in fending off attacks from quantum computers and can be investigated for 5G

communication security, designing and assessing secure networks for use in 5G systems. Examine how physical layer security techniques can be incorporated into the entire network design while taking into account elements such as network slicing, virtualization, and software-defined networking. Create scalable, effective security frameworks that can accommodate the dynamic, heterogeneous character of 5G networks while offering strong defense against hacking and other security risks.

5.7. Standardization and Practical Implementations

Focus should be directed to the use of physical layer security techniques in 5G networks in order to determine the viability and efficacy of suggested security solutions, and conduct experimental evaluations and performance measurements. To ensure interoperability and broad adoption, work with standardization organizations to establish protocols and recommendations for including physical layer security methods into the 5G standard should be conducted.

Author Contributions: Conceptualization, J.B. and A.A.; methodology, J.B. and A.A.; formal analysis, J.B. and A.A.; investigation, J.B. and A.A.; resources, J.B. and A.A.; writing original draft preparation, J.B. and A.A.; writing—review and editing, J.B., A.A. and M.F.; supervision, M.F.; funding acquisition, M.F. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by King Faisal University, Saudi Arabia [Project No. GRANT3,606].

Acknowledgments: This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT3,606].

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

References

1. Li, J.; Yang, H.; Chen, W.; Sun, Y.; Wang, S. A survey on physical layer security for 5G wireless networks. *Wirel. Pers. Commun.* **2019**, *105*, 113–138. [CrossRef]
2. Zhou, L.; Wu, D.; Zheng, B.; Guizani, M. Joint physical-application layer security for wireless multimedia delivery. *IEEE Commun. Mag.* **2014**, *52*, 66–72. [CrossRef]
3. Wang, H.-M.; Zheng, T.-X.; Yuan, J.; Towsley, D.; Lee, M.H. Physical layer security in heterogeneous cellular networks. *IEEE Trans. Commun.* **2016**, *64*, 1204–1219. [CrossRef]
4. Wang, Y.; Zhang, L.; Ye, Q.; Li, Y.; Liu, G. Physical layer security for 5G wireless networks: Recent advances and future challenges. *J. Netw. Comput. Appl.* **2018**, *116*, 53–67. [CrossRef]
5. Zheng, T.-X.; Wang, H.-M.; Yuan, J.; Han, Z.; Lee, M.H. Physical layer security in wireless Ad Hoc networks under a hybrid full-/half-duplex receiver deployment strategy. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3827–3839. [CrossRef]
6. Islam, S.M.R.; Zhang, J.; Lu, R.; Hussain, S.A. 5G security: Analysis of threats and solutions. *IEEE Wirel. Commun.* **2019**, *26*, 120–128. [CrossRef]
7. Cepheli, O.; Tedik, S.; Kurt, G.K. A high data rate wireless communication system with improved secrecy: Full duplex beamforming. *IEEE Commun. Lett.* **2014**, *18*, 1075–1078. [CrossRef]
8. Gao, Y.; Hu, S.; Tang, W.; Li, Y.; Sun, Y.; Huang, D.; Cheng, S.; Li, X. Physical layer security in 5G based large-scale social networks: Opportunities and challenges. *IEEE Access* **2018**, *6*, 26350–26357. [CrossRef]
9. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Renzo, M.D. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27. [CrossRef]
10. Lopez-Martinez, F.J.; Romero-Jerez, J.M.; Paris, J.F. On the calculation of the incomplete mgf with applications to wireless communications. *IEEE Trans. Commun.* **2017**, *65*, 458–469. [CrossRef]
11. Stallings, W. *Cryptography and Network Security: Principles and Practice*; Prentice Hall: New York, NY, USA, 2008.
12. He, B.; Zhou, X.; Swindlehurst, A.L. On secrecy metrics for physical layer security over quasi-static fading channels. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 6913–6924. [CrossRef]
13. Ud Din, F.; Labeau, F. Multiple antenna physical layer security against passive eavesdroppers: A tutorial. In Proceedings of the 2018 IEEE Canadian Conference on Electrical Computer Engineering (CCECE), Quebec, QC, Canada, 13–16 May 2018; pp. 1–6. [CrossRef]
14. Shah, H.A.; Koo, I. A novel physical layer security scheme in OFDM-based cognitive radio networks. *IEEE Access* **2018**, *6*, 29486–29498. [CrossRef]
15. Wang, X.; Xu, K.; Huang, X.; Ji, X.; Chen, Y.; Jin, L. Artificial noise aided hybrid analog-digital beamforming for secure transmission in MIMO millimeter-wave relay systems. *IEEE Access* **2019**, *7*, 28597–28606. [CrossRef]

16. Yan, S.; Zhou, X.; Yang, N.; Abhayapala, T.D.; Swindlehurst, A.L. Secret channel training to enhance physical layer security with a full-duplex receiver. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2788–2800. [CrossRef]
17. Liu, D.; Hong, W.; Rappaport, T.S.; Luxey, C.; Hong, W. What will 5G antennas and propagation be? *IEEE Trans. Antennas Propag.* **2017**, *65*, 6205–6212. [CrossRef]
18. Mathur, A.; Ai, Y.; Bhatnagar, M.R.; Cheffena, M.; Ohtsuki, T. On physical layer security of $\alpha - \eta - \kappa - \mu$ fading channels. *IEEE Commun. Lett.* **2018**, *22*, 2168–2171. [CrossRef]
19. Zeng, W.; Zhang, J.; Chen, S.; Peppas, K.P.; Ai, B. Physical layer security over fluctuating two-ray fading channels. *IEEE Trans. Veh. Technol.* **2018**, *67*, 8949–8953. [CrossRef]
20. Boche, H.; Deppe, C. Secure identification under passive eavesdroppers and active jamming attacks. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 472–485. [CrossRef]
21. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
22. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1550–1573. [CrossRef]
23. Akram, R.N.; Khan, M.A.; Raza, S.; Awais, M. Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. *Internet Things* **2021**, *2*, 5. [CrossRef]
24. Raza, S.; Ullah, S.; Khan, M.A. The impact of quantum computing on real-world security: A 5G case study. *Comput. Netw.* **2020**, *171*, 107167. [CrossRef]
25. Al-Shareeda, M.A.; Manickam, S.; Saare, M.A. Enhancement of NTSA secure communication with one-time pad (OTP) in IoT. *Informatica* **2023**, *43*, 569–580. [CrossRef]
26. Maqbool, A.; Abbas, H.; Mustafa, M.; Zahoor, A. A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard. *J. Cryptogr. Eng.* **2023**, *11*, 103–128. [CrossRef]
27. Maqbool, A.; Abbas, H. FaultMeter: Quantitative Fault Attack Assessment of Block Cipher Software. *J. Cryptogr. Eng.* **2023**, *10*, 363–380. [CrossRef]
28. Shah, H.A.; Koo, I. Overview of 5G architecture security. *IEEE Access* **2021**, *6*, 39152–39168. [CrossRef]
29. Seo, H.; Azarderakhsh, R. Curve448 on 32-Bit ARM Cortex-M4. In Proceedings of the 15th International Conference on Embedded Security in Silicon, Seoul, Republic of Korea, 2–4 December 2020; Springer Nature: Cham, Switzerland, 2021; pp. 107–125. [CrossRef]
30. Anastasova, M.; Bisheh-Niasar, M.; Azarderakhsh, R.; Kermani, M.M. Compressed SIKE Round 3 on ARM Cortex-M4. In *Security and Privacy in Communication Networks, Proceedings of the 17th EAI International Conference, SecureComm 2021, Virtual Event, 6–9 September 2021*; Springer International Publishing: Cham, Switzerland, 2021; Part II, pp. 441–457.
31. Anastasova, M.; Azarderakhsh, R.; Kermani, M.M. Fast strategies for the implementation of SIKE round 3 on ARM Cortex-M4. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2021**, *68*, 4129–4141. [CrossRef]
32. Sanal, P.; Karagoz, E.; Seo, H.; Azarderakhsh, R.; Mozaffari-Kermani, M. Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM Cortex-A processors. In *Security and Privacy in Communication Networks, Proceedings of the 17th EAI International Conference, SecureComm 2021, Virtual Event, 6–9 September 2021*; Springer International Publishing: Cham, Switzerland, 2021; Part II, pp. 424–440.
33. Bisheh-Niasar, M.; Azarderakhsh, R.; Mozaffari-Kermani, M. Cryptographic accelerators for digital signature based on Ed25519. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2021**, *29*, 1297–1305. [CrossRef]
34. Canto, A.C.; Mozaffari-Kermani, M.; Azarderakhsh, R. Reliable CRC-based error detection constructions for finite field multipliers with applications in cryptography. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2020**, *29*, 232–236. [CrossRef]
35. Abed, S.E.; Jaffal, R.; Mohd, B.J.; Al-Shayeji, M. An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. *Clust. Comput.* **2021**, *24*, 3065–3084. [CrossRef]
36. Lin, J.; He, J.; Fan, Y.; Wang, M. From Unbalanced to Perfect: Implementation of Low Energy Stream Ciphers. *Cryptol. ePrint Arch.* **2023**, *136*, 101–118.
37. Li, M.; Zhao, D.; Tang, X.; Cheng, S.; Hu, X.; Bao, L. Hardware Implementation and optimization Design of Lightweight RECTANGLE Algorithm. In Proceedings of the 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 11–13 December 2020; IEEE: Piscataway, NJ, USA, 2020; Volume 9, pp. 1447–1450.
38. Zheng, F.; Li, Y.; Li, X.; Wang, Q.; Mao, G. 5G wireless networks: From architecture to physical layer security. *IEEE Wirel. Commun.* **2018**, *25*, 102–108. [CrossRef]
39. Lyu, Q.; Han, G.; Fu, X. Physical layer security in multi-hop AF relay network based on compressed sensing. *IEEE Commun. Lett.* **2018**, *22*, 1882–1885. [CrossRef]
40. Vuppala, S.; Tolossa, Y.J.; Kaddoum, G.; Abreu, G. On the physical layer security analysis of hybrid millimeter-wave networks. *IEEE Trans. Commun.* **2018**, *66*, 1139–1152. [CrossRef]
41. Schaefer, R.F.; Amarasuriya, G.; Poor, H.V. Physical layer security in massive MIMO systems. In Proceedings of the 2017 51st Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 29 October–1 November 2017; pp. 3–8. [CrossRef]
42. Wang, C.; Wang, H.-M. Physical layer security in millimeter wave cellular networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 5569–5585. [CrossRef]

43. Eltayeb, M.E.; Choi, J.; Al-Naffouri, T.Y.; Heath, R.W., Jr. On the security of millimeter wave vehicular communication systems using random antenna subsets. *arXiv* **2016**, arXiv:1609.04499.
44. Chen, G.; Gong, Y.; Xiao, P.; Chambers, J.A. Physical layer network security in the full-duplex relay system. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 574–583. [CrossRef]
45. Zhu, F.; Gao, F.; Zhang, T.; Sun, K.; Yao, M. Physical-layer security for full duplex communications with self-interference mitigation. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 329–340. [CrossRef]