network

MDPI

Article

Advanced Security Framework for 6G Networks: Integrating Deep Learning and Physical Layer Security

Haitham Mahmoud [1], Tawfik Ismail [2], Tobi Baiyekusi [1] and Moad Idrissi [3,*]

[1] Faculty of Computing, Engineering and Built Environment, Birmingham City University, Birmingham B4 7RQ, UK; tobi.baiyekusi@bcu.ac.uk (T.B.)
[2] College of Engineering, Taibah University, Madinah 42353, Saudi Arabia; tismail@cu.edu.eg
[3] School of Computing and Data Science, Oryx Universal College, Liverpool John Moores University, Doha P.O. Box 12253, Qatar
* Correspondence: moad.i@oryx.edu.qa

Abstract: This paper presents an advanced framework for securing 6G communication by integrating deep learning and physical layer security (PLS). The proposed model incorporates multi-stage detection mechanisms to enhance security against various attacks on the 6G air interface. Deep neural networks and a hybrid model are employed for sequential learning to improve classification accuracy and handle complex data patterns. Additionally, spoofing, jamming, and eavesdropping attacks are simulated to refine detection mechanisms. An anomaly detection system is developed to identify unusual signal patterns indicating potential attacks. The results demonstrate that machine learning (ML) and hybrid models outperform conventional approaches, showing improvements of up to 85% in bit error rate (BER) and 24% in accuracy, especially under attack conditions. This research contributes to the advancement of secure 6G communication systems, offering details on effective defence mechanisms against physical layer attacks.

Keywords: physical layer security; 6G privacy; multi-stage detection; anomaly detection; machine learning

Citation: Mahmoud, H.; Ismail, T.; Baiyekusi, T.; Idrissi, M. Advanced Security Framework for 6G Networks: Integrating Deep Learning and Physical Layer Security. *Network* **2024**, *4*, 453–467. https://doi.org/10.3390/network4040023

Academic Editor: Youn-Hee Han

Received: 9 August 2024
Revised: 1 October 2024
Accepted: 8 October 2024
Published: 23 October 2024

1. Introduction

The adoption of 5G cellular technology and its rapid evolution of advanced services has opened the door to numerous applications, including network-assisted computing, extended reality (XR), and mixed reality. These technologies promise to revolutionise sectors such as tele-medicine, augmented reality (AR), the Internet of Things (IoT), connected vehicles, sensors, and robotics by minimising delays in data transmission [1–3]. As the groundwork for the next-generation sixth-generation (6G) wireless communications is being laid, initiatives such as those by the International Telecommunication Union (ITU) and the 3GPP standards community are driving towards significant enhancements. These include achieving enormous data transfer at terabit rates, implementing AI/ML-driven processes for network function automation, expanding cloud-native operations, and supporting ultra-low-latency tactile applications in a real-time manner within the edge [4,5].

The vision for 6G encompasses a range of advanced capabilities. These include automated network planning through an AI-native optimiser, smart network slicing, self-healing networks, and management without manual intervention [6]. Robotics, including unmanned aerial vehicles (UAVs), are also anticipated to be pivotal in advancing automation and connectivity [7]. UAVs are increasingly recognised as essential tools in the advancement of 6G future wireless networks. This is because their flexibility and mobility allow them to operate in diverse environments, which makes them ideal for supporting wireless infrastructure, particularly in scenarios where ground-based networks may be limited or unavailable. As mentioned in [8], UAVs can serve as aerial base stations or relays to enhance communication coverage and improve data rates, particularly in rural and disaster-affected

areas. It is worth mentioning that integrating UAVs into wireless networks requires the development of efficient algorithms that can support autonomous flight missions. The trajectory of UAVs must be optimised to maintain continuous connectivity with ground users whilst avoiding obstacles and ensuring safety. The authors in [9] propose a deep reinforcement learning (DRL) framework that optimises the flight paths of UAVs to ensure stable connections with cellular networks while accounting for environmental constraints and dynamic network conditions. The use of quantum-inspired experience replay enhances the learning process, which enables the UAV to make more informed decisions in real time. In support of this, the authors of [10] highlight the application of UAV-assisted communications in delivering high-quality services in densely populated urban environments. Their research study demonstrated how UAVs can provide on-demand connectivity during network congestion or service outages to meet the dynamic demands of users. This flexibility is particularly important for 6G, where diverse services that consist of IoT and autonomous systems will require highly dynamic network infrastructures. Although the 3GPP standards for 6G are under development, there are high expectations for maximum data rates reaching 1 Tbps, 100-microsecond latency, and a five-fold increase in spectral efficiency compared to 5G [11]. In order to achieve these objectives, 6G systems must efficiently utilise the available spectrum, which ranges up to 300 GHz, through the gathering of frequency division duplexing (FDM) and Time division duplexing (TDM) [12]. This broad spectrum is divided into several bands: low, mid, upper-mid, mmWave, and other sub-THz bands. The emergence of 6G technologies will lead to the dense deployment of massive network infrastructures, exponentially increasing the size of the network and improving the possibilities for the Internet of Vehicles (IoV) [13,14]. A crucial focus in the evolution of 6G-IoT is security because of the increase in malicious attacks which can severely disrupt operations [15,16]. Potential security solutions have been proposed using AI/ML, quantum communications, blockchain and smart contracts, and zero-trust architectures [17–19]. Applying security in Layer 1 of the OSI stack, known as PLS, is another security direction and the focus of this paper. Unlike transport and network layer security protocols, such as TLS and IPSEC, which operate at Layers 3 and 4, PLS provides a lower latency method for exchanging secret information. This method utilises the distinctive features of the transmitter-receiver channel as a secret key for higher-level encryption algorithms [16,20]. PLS techniques, such as channel quantisation and precoder matrix indexing (PMI), depend on the inherent differences in the communication channel rather than the signal-to-noise ratio (SNR), making them resilient to eavesdropping, even when the eavesdropper is physically closer to the transmitter [21,22]. However, despite its advantages, PLS is not immune to various security attacks that target the transmission channel [23,24]. Common attacks include spoofing, jamming, and eavesdropping. Spoofing attacks involve an adversary impersonating a legitimate user by altering the transmitted signals, potentially gaining unauthorised access to sensitive information or network resources. Jamming attacks, on the other hand, involve deliberate interference with the communication channel by emitting disruptive signals, thereby degrading the quality of service or even causing complete denial of service. Eavesdropping remains a significant threat, where an attacker intercepts the communication between legitimate users to gain access to confidential information without altering the transmission. These attacks exploit the vulnerabilities at the physical layer, necessitating robust countermeasures within PLS frameworks to ensure secure and reliable communication. Advanced PLS techniques, such as utilising unique channel state information and adaptive modulation schemes, are essential to mitigate these threats and enhance the overall security of next-generation wireless networks [25].

Although PLS leverages the inherent properties of wireless channels, such as noise, fading, and interference to protect transmitted information from unauthorised access without relying solely on traditional cryptographic methods, a growing area of research, known as covert communications, extends beyond PLS by focusing on ensuring the very existence of the transmission remains undetected. This makes covert communications a highly relevant technique for environments where merely being noticed could compromise operations.

Covert communications, also known as low probability of detection communications, are designed to conceal the transmission, not just the content of the information being sent. It is this that can make all the difference in applications where a lack of detection may be at least as important as data confidentiality in surveillance and other sensitive operations. While PLS offers security via the undecidability of information by unauthorised parties, in covert communication, even the detection of a transmission by adversaries should not be allowed. This additional layer of security becomes crucial in wireless systems where adversaries can easily monitor the communication environment. The integration of covert communication with PLS offers a robust solution for next-generation networks, including 6G. The authors in [26] explore this methodology by examining how covert communications can be integrated with energy-harvesting techniques. In their work, the authors propose a system where nodes harvest energy from the environment and opportunistically relay covert signals, ensuring that the transmission remains undetected while still maintaining efficient communication. Their findings show that this combined approach not only improves energy efficiency but also strengthens the covertness of transmissions, making it particularly useful for low-power devices such as IoT sensors and UAVs. The research group in [27] investigate how covert communications can be applied to mobile systems such as UAVs. The study presents a twin delayed deep deterministic policy gradient (TD3) and prioritised experience replay (PER) solution to optimise UAV flight paths, ensuring that their transmissions are both efficient and undetectable. The dynamic nature of the trajectory design allows the UAV to adapt its movement based on environmental factors and potential adversarial detection. Several other studies support the importance of covert communications in enhancing transmission security. For example, the authors of [28] highlight the role of covert techniques in mitigating the detection risk posed by adversarial eavesdroppers, and the authors of [29] discuss the importance of using stochastic methods to achieve covertness in wireless communications, which demonstrates how randomisation in signal transmission can further obscure detection efforts. As wireless networks evolve, the integration of covert communications into existing security frameworks will become increasingly vital. The unique combination of PLS and covert communication techniques offers a dual-layer defence: PLS ensures that even if a message is detected, it cannot be decoded without authorisation, while covert communications reduce the likelihood that the transmission will be detected in the first place.

Hence, this paper presents considerable research on the privacy of 6G at the physical layer, employing PMI and advanced machine learning (ML) algorithms, specifically deep neural networks, to predict or classify received signals based on historical data using recognition and classification of the pattern. This work extends to Kelly and Ara's study [16] and the development of an intelligent PLS scheme that combines random forests (RFs) for feature extraction and long short-term memory (LSTM) for sequential learning to enhance classification accuracy and handle complex data patterns while simulating three common physical layer attacks (spoofing, jamming, and eavesdropping). Additionally, we developed an anomaly detection system using isolation forests to identify unusual patterns in received signals, ensuring robust security against potential threats. This paper develops an intelligent PLS scheme utilising deep neural networks (DNNs) for detection. This lays the foundations for the 6G service-based architecture, which preserves the privacy of the shared data. This system, operating within the 6G Core Radio Access Network (RAN), enhances the security and management of received information, ensuring significant security and quality of service (QoS) via secret shared key generation and integrated key management strategies. This system works in addition to the traditional cryptographic security at the network and transport layers to facilitate lower latency of machine-to-machine (M2M) communication. Our complete contributions are as follows:

- By utilising deep neural networks (i.e., LSTM) and a hybrid model of RF and recurrent neural networks (RNNs) (in particular, LSTM) where the hybrid model utilises RF for feature extraction and LSTM for sequential learning, we enhance classification accuracy and handle complex data patterns;

- We simulated three common attacks on the physical layer: spoofing, jamming, and eavesdropping. These simulations aid in understanding the attack vectors and refining our detection mechanisms. By creating realistic scenarios, we ensure that our PLS model is well-prepared to counter these threats in real-world applications;
- We have developed an anomaly-detection system using isolation forests. This technique is capable of identifying unusual patterns in received signals that may indicate an attack or interference. By isolating anomalies, the system can quickly respond to potential threats, maintaining the integrity and security of the communication channel.

This paper is structured as follows: Section 2 proposes the proposed system model. Section 3 presents and discusses the results of the system model, including the bit error rate (BER) using multi-bit codebooks for multi-antenna systems. Finally, Section 4 concludes the work and addresses the future work of this study.

2. System Model

The physical layer of wireless communication systems is inherently vulnerable to various impairments, such as noise, interference, and fading. The dynamic and complex nature of 6G networks, characterised by large-scale deployment and heterogeneity, further complicates the optimisation process [11]. The traditional optimisation techniques fall short of addressing these challenges. However, advancements in network intelligence (i.e., ML and DL) provide promising solutions. These technologies can dynamically learn the features of radio signals and carry out tasks such as network optimisation, signal detection, and classification in real time. This system model focuses on implementing secure communication between mobile devices named Alice and Bob as an example for transmission evaluation, where the framework for securely transmitting information between a mobile device named Alice and an access node named Bob. The communication channels between Alice and Bob are assumed to operate in time division duplex (TDD) mode, ensuring channel reciprocity ($H_{AB}H_{BA}^{T}$). This reciprocity allows shared channel information to be used for secure communication. Bob transmits his secret information to Alice, utilising the shared channel information to conceal it. Alice receives this information over a noisy channel and, in turn, sends her secret information back to Bob using the same method. This bidirectional exchange enables both parties to recover each other's secret information securely.

A key feature of this system is the development of the service-based architecture (SBA), which supports a modular approach to software design. As shown in Figure 1, the 6G-SA SBA includes a privacy plane feature enabled by the mobility management function. Network function (`NF`) services expose network capabilities via standard interfaces, usually HTTP RESTful interfaces. In most cases, 6G applications will adopt a "client-server" software model to utilise the most effective network services. The core network aims to deliver data messages with designated QoS assignments. A specialised 6G service employing a privacy plane is adopted to ensure secure and confidential communications. This allows for ultra-low latency for applications such as UAVs, connected vehicle control, and vehicle-to-vehicle (`V2V`) communication.

2.1. Use Case

The use case is a simulated representation of signal transmission and reception between two entities, Alice and Bob, within the context of a 6G air interface. This simulation, conducted using MATLAB, focuses on a 2×2 multiple input multiple output (MIMO) system, enhancing communication performance through the use of multiple antennas for both transmitting and receiving signals. In this simulation, Alice and Bob each generate a set of random information bits to transmit. For Alice, 1000 random bits are generated and modulated using binary phase shift keying (BPSK). The modulated bits are then transmitted through a Rayleigh fading channel, represented by a complex matrix H_{AB}. In order to simulate realistic channel conditions, Gaussian noise is added to the transmitted signal. Bob receives the signal, applies a decoding process to estimate the transmitted bits, and then

generates his own set of random information bits to transmit back to Alice through a similar channel H_{BA}. The key parameters of the simulation include the number of information bits (1000), SNR set at 15 dB, and the use of a 2 × 2 MIMO system. The channel model used is Rayleigh fading, and the modulation scheme is BPSK. The dataset columns capture critical aspects of the communication process, including the information bits transmitted by Alice and Bob, the real and imaginary parts of the transmitted signals from both Alice and Bob and the real and imaginary parts of the signals received by both parties. This information is essential for analysing the performance and reliability of the 6G air interface communication system, providing insights into the behaviour of MIMO channels under various noise conditions and signal strengths.

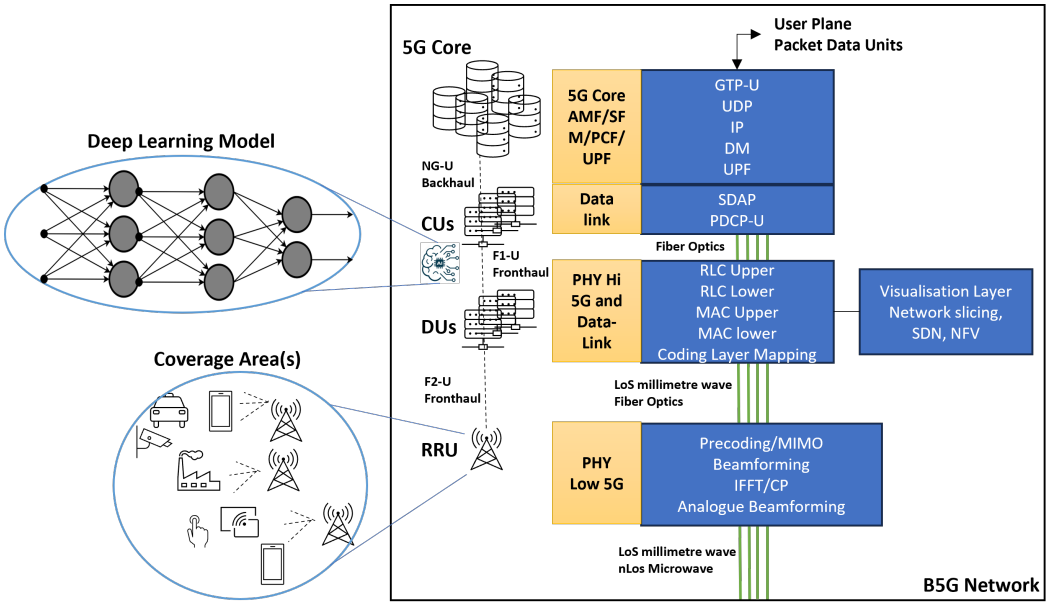


Figure 1. Intelligent network for B5G service-based architecture.

2.2. Signalling Through Precoder Matrix Indices

The system model depicted in Figure 1 employs transmitted reference signals applied to precoders, G_i, with dimensions corresponding to the number of transmitting and receiving antennas (i.e., $N \times N$). These reference signals are pre-known to the receiver, enabling the recovery of information related to the precoders. During initialisation, the precoder G is selected from a collection of random unitary operators with complex coefficients ($g_{i,j} \in \mathbb{C}$).

Consider the precoder matrix G defined as

$$G = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,N} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ g_{N,1} & g_{N,2} & \cdots & g_{N,N} \end{bmatrix} \tag{1}$$

where $g_{i,j} \in \mathbb{C}$ are complex coefficients. The selection of G is based on a set of random unitary operators. The relationship between the transmitted signal x, the precoder G, and the received signal y can be expressed as

$$y = Gx + n \tag{2}$$

where n represents the noise vector. Precoders G_1 and G_2 are derived from a combination of the received signals by both parties (Alice and Bob), the CSI between them, and an information-bearing codebook that maps an n-bit binary tuple to a codebook matrix. The codebook of a finite set of precoder matrices is shared among both parties. Each matrix is identified by an index called the precoder matrix index (PMI). The private data or

secret information serves as an index for these precoding matrices within the universally known codebook. The actual secret information bits are not shared with any entities in the system; instead, the receiver decodes the mapped codebook elements to retrieve the codebook indices. The codebook that maps an n-bit binary tuple b to a precoder matrix $C(b)$ is defined as

$$C(b) = G_{PMI(b)} \tag{3}$$

where $PMI(b)$ is the precoder matrix index associated with the binary tuple b. Due to the Rayleigh fading channel differences between Bob and Alice, the precoding matrix of a multiple input multiple output (MIMO) system is known only to them, not to any potential interceptor or eavesdropper. Therefore, the PMI is also utilised to map secret information tuples. The detection probability P_d for a given PMI scheme can be evaluated using

$$P_d = \Pr(\hat{PMI} = PMI | y, G) \tag{4}$$

where $\hat{PMI}$ is the estimated precoder matrix index at the receiver. Furthermore, the bit error rate (BER) is given by

$$\text{BER} = \frac{1}{n} \sum_{i=1}^{n} \Pr(b_i \neq \hat{b}_i) \tag{5}$$

where b_i and $\hat{b}_i$ represent the i-th bit of the transmitted and received binary tuples, respectively.

2.3. Non-ML Detection

This utilises a rule-based mechanism for bit detection in received signals, specifically designed for telecommunications applications. This function evaluates the real part of the received signal; if the real part is greater than zero, the bit is classified as '1'; otherwise, it is classified as '0'. This threshold-based approach enables efficient bit detection without the need for complex signal processing techniques.

One of the primary advantages of this method is its capability for real-time detection. Non-ML methods provide rapid, real-time detection of anomalies or bit errors, which is crucial in telecommunications where low latency and high-speed processing are essential [30,31]. Additionally, these methods are easy to implement, as they do not require the extensive data collection and labelling necessary for training machine learning models. This simplicity can be beneficial in scenarios where rapid deployment and operational efficiency are prioritised. However, the non-ML detection method has certain limitations. Threshold-based detection methods exhibit limited adaptability to varying signal conditions and sophisticated interference attacks. In dynamic and hostile environments, their performance may degrade since they are not designed to adjust to changes in signal characteristics. Moreover, the accuracy of these methods can be lower compared to ML-based approaches, particularly in complex environments with high noise levels and multiple interference sources. The fixed threshold may not account for nuanced variations in the signal, leading to potential misclassifications.

2.4. Codebook Detection Using Deep Learning

A key aim of this scheme is to minimise the manual tasks involved in detecting and estimating decoded private information from noisy received signals. This is achieved by automating the process using AI/ML algorithms. Specifically, we utilise LSTM networks and a hybrid model combining LSTM with RF algorithms for the detection and recovery of secret information. The LSTM model is designed to handle the temporal dependencies of the received signals, as shown in Algorithm 1.

Algorithm 1 LSTM model for PLS codebook detection

1: **Step 0: Initialisation**—Alice sends a reference signal r that has been rotated by a random unitary matrix. G.
2: **Step 1: Bob-to-Alice Communication**
3: Bob receives the signal and sends back a rotated reference signal $G1r$ to Alice, where $G1 = U_B^* F_B^T$.
4: Alice receives the noisy signal, estimates $H_{BA}G1$, and inputs this into the LSTM model, referred to as the Alice AI/ML detector.
5: The input data are split into real and imaginary parts. The LSTM model updates its bias weights through backpropagation during training. The output layer identifies the predicted class, eventually mapping the PMI. Alice decodes this to obtain S_B, Bob's secret information.
6: **Step 2: Alice-to-Bob Communication**
7: Alice generates her own random secret information S_A and transmits a rotated reference signal $G2r$ to Bob, where $G2 = V_A F_A^T$.
8: Bob estimates $H_{AB}G2$, inputs the received noisy signal into his AI/ML model, and decodes Alice's transmitted information S_A.

Moreover, the hybrid LSTM and RF Model combines the feature extraction capabilities of RF with the temporal dependency management of LSTM. By using RF, features are extracted from the received signals before they are fed into the LSTM. The LSTM model is trained with the extracted features from RF to improve detection accuracy.

The selection of LSTM and RF models for our 6G security framework is based on the specific requirements of 6G communication systems, which demand both high accuracy in signal classification and the ability to handle complex temporal dependencies in dynamic network environments. LSTM networks, a variant of RNNs, are specifically designed to capture long-range dependencies in time-series data, making them particularly well-suited for analysing sequential data, such as the rapidly changing patterns of communication signals in a 6G environment. This capability allows LSTM to efficiently model the temporal aspects of the physical layer, where patterns of interference or attack may emerge gradually over time. On the other hand, RF provides a robust mechanism for feature extraction due to its ensemble learning nature, which aggregates decision trees to improve classification performance. By leveraging multiple decision paths, RF reduces the risk of overfitting and ensures more reliable classification even when the data are noisy or incomplete—conditions that are common in wireless communication. Finally, RF is computationally efficient, which is crucial for real-time applications in 6G networks where latency and speed are paramount.

2.5. Simulation of Physical Layer Attacks

In order to rigorously evaluate the robustness of the proposed PLS mechanisms, it is essential to simulate various attack scenarios. These scenarios are designed to reflect the types of threats that a 6G network might encounter. We focus on three primary types of attacks: jamming, eavesdropping, and spoofing. Each attack type is characterised by its unique method of disrupting communication, which helps in assessing the system's resilience. Table 1 summarises the simulated physical layer attacks with the implemented approach and their expected impact on the communication system.

Jamming attacks: Jamming involves the introduction of interference into the communication channel to disrupt the signal transmission [32,33]. This can be simulated by adding Gaussian noise to the received signal, thereby degrading the SNR.

$$y_{\text{jammed}} = y + n_j \tag{6}$$

where n_j is the jamming noise.

Table 1. Summary of simulated physical layer attacks with the implemented approach and their expected impact.

Attack Type	Generation Method	Expected Impact
Jamming	Adding Gaussian noise	Degraded SNR, increased BER
Eavesdropping	Introducing random bit flips	Compromised data confidentiality, increased BER
Spoofing	Adding sinusoidal signal	False data reception, misleading information
Replay Attack	Re-transmitting captured signals	Confusion in the communication flow, false timestamps
Signal Fading	Reducing signal strength artificially	Loss of data, degraded communication quality
Denial of Service (DoS)	Flooding the communication channel	Complete disruption of communication, inability to transmit data
Man-in-the-Middle (MitM)	Intercepting and modifying signals	Unauthorised data manipulation, compromised integrity

Eavesdropping attacks: Eavesdropping attempts to intercept and decode the communication between legitimate users without authorisation [34,35]. This attack can be modelled by introducing random bit flips in the transmitted signal, simulating the effect of an interceptor manipulating the signal.

$$x_{\text{eavesdropped}} = x \oplus e \tag{7}$$

where e represents the error vector due to eavesdropping.

Spoofing attacks: Spoofing involves injecting false signals into the communication channel to deceive the receiver [36,37]. This can be simulated by adding structured noise, such as a sinusoidal signal, to the original signal.

$$y_{\text{spoofed}} = y + A\sin(2\pi f t) \tag{8}$$

where A is the amplitude and f is the frequency of the sinusoidal spoofing signal.

Replay attacks: Replay attacks can be defined as the adversary's interception of legitimate data and replaying it with the intention of misleading the receiver to accept it as an authentic message. This generally affects the system's whole operation depending on message sequencing or the timings, which would create disarray or unauthorised access. By reintroducing the previously transmitted data in the communication channel, the attacker makes the receiver process outdated or previously validated information, hence undermining the integrity of the whole communication process.

$$y_{\text{replayed}} = y(t - \Delta t)$$

where Δt is the time delay applied to the original signal before being replayed.

Signal fading: Signal fading is essentially the process where the strength of a signal weakens due to multiple environmental factors, such as distance, obstacles, and interference. In this type of attack, an adversary can intentionally minimise the power of a signal such that it becomes very challenging for the receiver to decode the message with much accuracy. Therefore, the effect of the faded signal may be in the form of losses, delays, and communication errors. The latter can be emulated by multiplying the original signal with a fading coefficient h_f, in which its amplitude is weakened.

$$y_{\text{faded}} = h_f y$$

where h_f represents the fading factor (typically $0 < h_f < 1$).

Denial of service: Denial of service is a type of attack where the communication channel is overwhelmed with unwanted traffic to the point where the legitimate user cannot access the network. The result may vary from degraded network performance to complete interruption of communication. It could also be modelled by simulating a high volume of noise or irrelevant packets injected into the communication channel that actually congests the bandwidth.

$$y_{\text{DoS}} = \sum_{i=1}^{N} n_i$$

where N is the number of noise signals or irrelevant packets overwhelming the channel.

Man-in-the-middle (MitM): Man-in-the-middle (MitM) is an attack that involves an adversary who intercepts the communication between two legitimate parties. The interceptor may or may not alter the transmitted data before forwarding it. This type of attack poses a threat to data integrity and confidentiality because the communication can be altered or eavesdropped upon without any noticeable issues by the sender or receiver. In the case of a MitM attack, the received signal y is intercepted and changed by the attacker, then retransmitted to the intended receiver.

$$y_{\text{MitM}} = f(y) + n_{\text{MitM}}$$

where $f(y)$ represents the modification of the original signal by the attacker, and n_{MitM} is any additional noise introduced during the attack.

2.6. Anomaly Detection Mechanism

Anomaly detection is a critical component of the proposed security framework, enabling the system to identify and mitigate the effects of malicious activities on communication signals [38,39]. For this purpose, we employ isolation forest, a machine learning technique well-suited for detecting anomalies in high-dimensional data. Isolation forest operates by randomly selecting features and splitting values to create isolation trees. The assumption is that anomalies are few and different, leading to their isolation in fewer steps compared to normal instances. This method is particularly effective for our use case, as it can handle the complex and high-dimensional nature of the received signals in 6G networks. The isolation forest algorithm constructs t isolation trees, and the anomaly score s for a given point x is calculated as

$$s(x,t) = 2^{-\frac{E(h(x))}{c(n)}} \tag{9}$$

where $E(h(x))$ is the average path length from the root to the terminating node of x in the isolation trees, and $c(n)$ is the average path length of unsuccessful searches in binary search trees, defined as

$$c(n) = 2H(n-1) - \left(\frac{2(n-1)}{n}\right) \tag{10}$$

and $H(i)$ is the i-th harmonic number. The anomaly score ranges from 0 to 1, with values close to 1 indicating anomalies.

The isolation forest algorithm, as applied in our framework, effectively detects anomalies in the physical layer of 6G networks by identifying unusual signal patterns indicative of attacks such as spoofing, jamming, and eavesdropping. The method isolates data points by building multiple decision trees based on random feature subsets of the received signals. Anomalous signals, caused by attacks, are typically isolated with fewer splits, leading to shorter path lengths, while normal signals require more splits, resulting in longer paths.

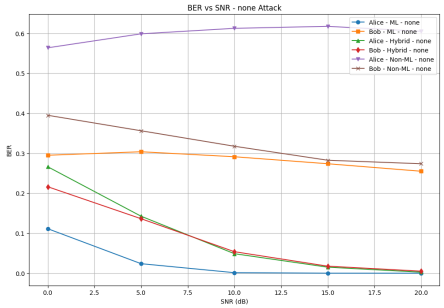
This method demonstrated a high level of accuracy in detecting anomalies during our simulations, particularly under noisy and complex channel conditions, providing real-time insights into potential threats. The key advantages of using isolation forest include its ability to manage high-dimensional data efficiently and its relatively low computational cost compared to more resource-intensive machine learning models. This makes it suitable for real-time applications, as shown by the reduced BER and improved detection accuracy in attack scenarios, particularly under jamming conditions. However, the method has its limitations. Although it performed well in detecting anomalies, its effectiveness can diminish when facing more sophisticated, blended attacks that may not fit the typical anomaly patterns. Additionally, the reliance on predefined parameters, such as the number of trees and sample size, may require fine-tuning to adapt to different network environments, potentially affecting scalability and robustness across the wider 6G use cases.

3. Results and Discussion

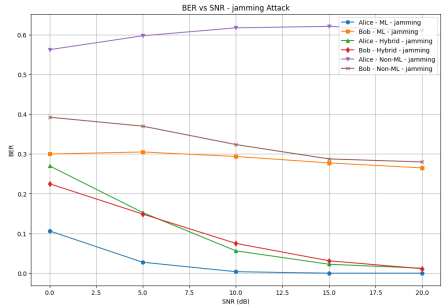
The performance of different models (ML, hybrid, and non-ML) under various conditions of no attack, spoofing attack, eavesdropping attack, and jamming attack is evaluated in terms of BER and accuracy. In the absence of attacks, the BER decreases as the SNR increases for all models, as shown in Figure 2e. The ML-based models for both Alice and Bob show the lowest BER, demonstrating their effectiveness in decoding signals under normal conditions. The hybrid models also perform well, closely following the ML models. Non-ML models have the highest BER, indicating their relative ineffectiveness in error correction compared to ML and hybrid models. For instance, at an SNR of 20 dB, the ML models achieve a BER of less than 0.05, whereas the non-ML models have a BER of around 0.3, reflecting a performance difference of approximately 85%. Under spoofing attacks, the BER trends are similar to the no-attack scenario, as shown in Figure 2d. However, the overall BER values are higher, reflecting the impact of the spoofing attack. The ML and hybrid models still outperform the non-ML models, but the effectiveness of the ML model is slightly reduced due to the attack interference. Specifically, at 20 dB SNR, the ML models' BER is about 0.1, while the non-ML models' BER is around 0.35, indicating that the ML models' BER is about 71% lower than that of the non-ML models. Eavesdropping attacks increase the BER across all models, but ML and hybrid models maintain better performance, as shown in Figure 2c. The non-ML models show a significant rise in BER, highlighting their vulnerability to such attacks. At an SNR of 20 dB, the BER for ML models is approximately 0.15, while for non-ML models, it is around 0.4, suggesting that the ML models have a 63% lower BER compared to non-ML models under eavesdropping attacks. Jamming attacks result in the highest BER among all attack scenarios, as shown in Figure 2b. The ML and hybrid models show resilience to some extent, but their performance is still affected. The non-ML models exhibit the worst performance under jamming conditions. For example, at 20 dB SNR, the ML models' BER is around 0.2, whereas the non-ML models' BER is close to 0.5, indicating that the ML models' BER is 60% lower than that of the non-ML models.

Without attacks, the accuracy increases with SNR. The ML models for both Alice and Bob achieve near-perfect accuracy at higher SNR levels, as shown in Figure 2e. Hybrid models also perform well, while non-ML models lag, demonstrating their limitations in achieving high accuracy. At an SNR of 20 dB, ML models achieve an accuracy of over 99%, whereas non-ML models achieve around 80%. Under spoofing attacks, the accuracy decreases compared to the no-attack scenario, attributed to the injected false signals, which disrupt the legitimate signal patterns and make it harder for the models to correctly identify the legitimate data. ML and hybrid models still outperform non-ML models, though the accuracy improvement is less pronounced due to the attack interference, as shown in Figure 2h. At 20 dB SNR, the ML models achieve an accuracy of approximately 95%, while non-ML models achieve around 75%. Eavesdropping attacks lead to a significant drop in accuracy across all models because of the introduction of the random bit flips into the signal, complicating the models' ability to accurately decode the original message, as

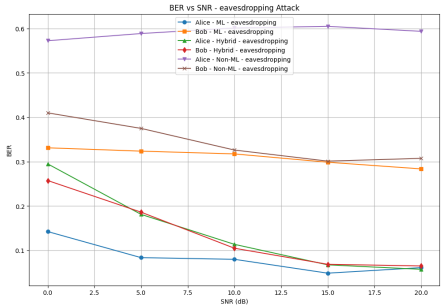
shown in Figure 2g. The ML and hybrid models manage to retain relatively higher accuracy, but the performance gap with non-ML models widens, emphasising the robustness of ML and hybrid models. At 20 dB SNR, the accuracy for ML models is about 90%, while for non-ML models, it is around 70%. Jamming attacks cause the most significant decrease in accuracy because of the substantial interference in the communication channel, as shown in Figure 2f. Despite this, the ML and hybrid models show better resilience compared to non-ML models, though all models are impacted by the high interference. At 20 dB SNR, the accuracy of ML models is approximately 88%, while non-ML models achieve around 68%.



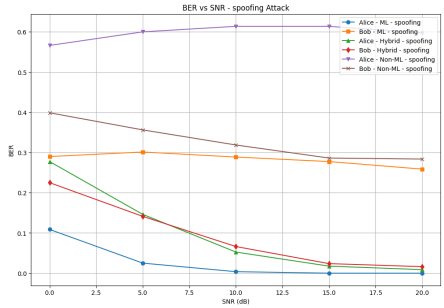
(**a**) No attack.



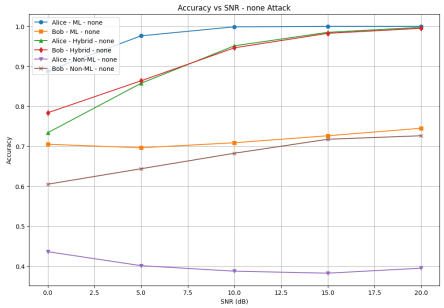
(**b**) Jamming attack.



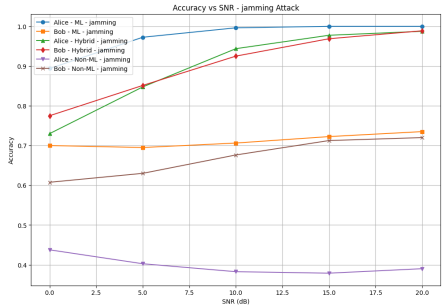
(**c**) Eavesdropping.



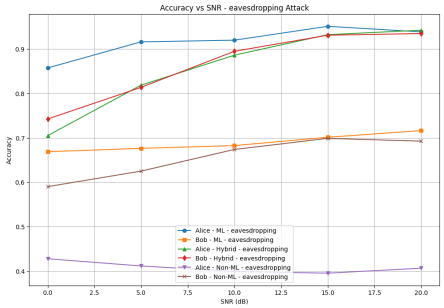
(**d**) Spoofing.



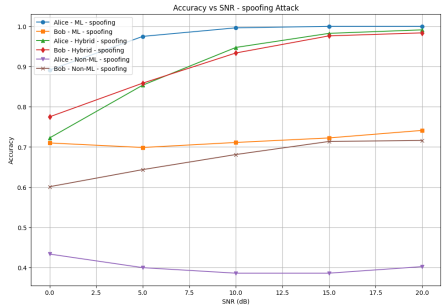
(**e**) No attack.



(**f**) Jamming attack.



(**g**) Eavesdropping.



(**h**) Spoofing.

Figure 2. Evaluation of the BER (**a**–**d**) and accuracy (**e**–**h**) of different approaches of non-ML, ML (LSTM), and hybrid.

The training and validation loss graphs for Alice and Bob indicate that both the ML and hybrid models converge well, with the hybrid model showing faster convergence, as shown in Figure 3. This demonstrates the effectiveness of combining feature extraction with sequential learning in the hybrid model. For instance, the loss for the hybrid model drops to nearly zero within the first 10 epochs, whereas the ML model takes slightly longer, and the non-ML model shows slower convergence and higher final loss values.

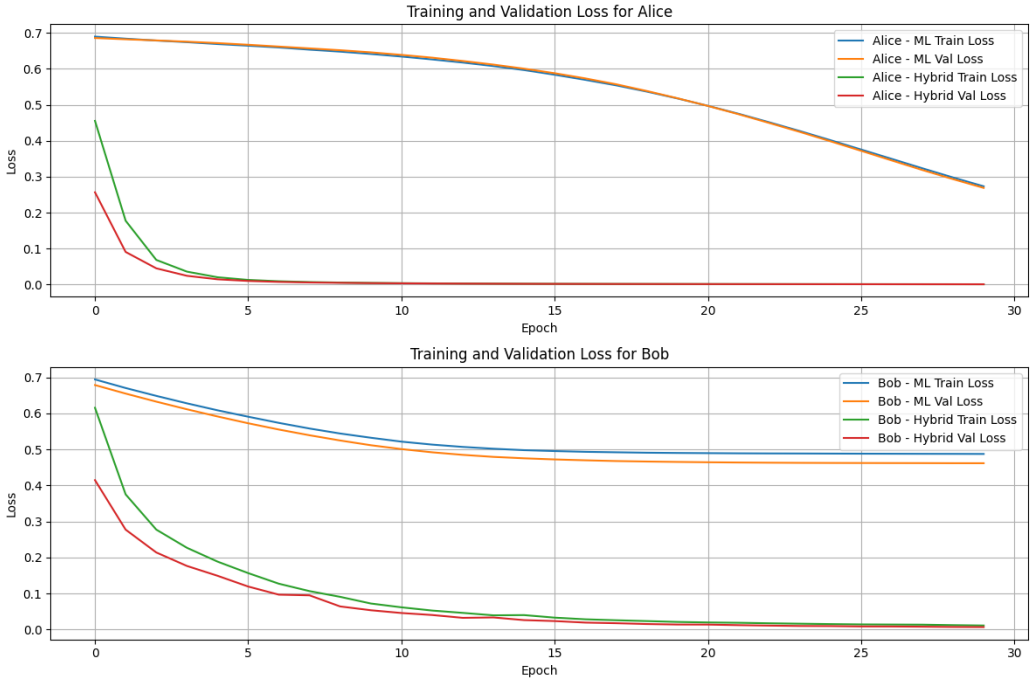


Figure 3. Training and validation convergence for both the ML and hybrid models for Alice and Bob. The loss corresponds to the model's error during training, representing the difference between the predicted and actual outcomes.

The integration of deep learning and PLS in 6G networks offers several advantages, such as enhanced accuracy in detecting physical layer attacks and improved resilience against common threats such as spoofing, jamming, and eavesdropping. The use of machine learning models such as LSTM and RF allows for better pattern recognition and anomaly detection, contributing to more secure communications. However, the high computational power required for these models can strain the energy efficiency of devices, particularly in large-scale 6G deployments. Moreover, the potential latency introduced by these techniques may be problematic in real-time applications, such as autonomous systems and vehicle-to-vehicle communication, where ultra-low latency is critical. Furthermore, the scalability of these techniques to handle the massive data throughput expected in 6G networks, alongside the need for efficient resource management to maintain quality of service, poses a significant challenge.

4. Conclusions and Future Work

This study presents a cutting-edge framework for improving the security of 6G communication networks by combining deep learning techniques with PLS. We demonstrate significant improvements in classification precision and reliability over intricate data patterns by integrating multi-stage detection techniques and using deep neural networks together with a hybrid model for sequential learning. Through the simulation of spoofing, jamming, and eavesdropping attacks, we optimised the detection algorithms and developed an anomaly-detection system to identify potential threats. Our results demonstrate the advantages of ML and hybrid models over traditional approaches, with significant improvements in BER and accuracy, particularly under adversarial conditions. Future work

will focus on expanding the applicability of our framework to diverse 6G communication scenarios and exploring the integration of emerging technologies such as blockchain, quantum communications, and AI/ML for enhanced security. Furthermore, additional research is required to investigate the scalability and real-world implementation of the proposed security framework.

Future work can extend and further strengthen the results by addressing a broader range of attacks beyond spoofing, jamming, and eavesdropping, particularly in the context of blockchain-assisted authentication for IoT [40]. Attacks such as replay, denial of service (DoS), and man-in-the-middle (MitM) are particularly relevant to IoT environments, where security vulnerabilities at the physical and network layers can expose critical infrastructure to threats. For instance, while the system showed strong resilience against simulated attacks, its ability to handle replay attacks—where attackers can retransmit intercepted communication—was not explored. Similarly, DoS attacks, which can overwhelm blockchain-assisted authentication systems by exhausting computational resources, could be particularly disruptive in real-time 6G applications that require ultra-low latency and reliable connectivity. Lastly, MitM attacks, which intercept and alter communication between nodes, pose a significant risk in environments relying on continuous secure exchanges, such as IoT healthcare systems or autonomous vehicles.

Moreover, another future piece of work aims to conduct a comprehensive comparison of our security framework with other existing methods for 6G, such as quantum communication, blockchain-based approaches, and zero-trust architectures. This will allow us to assess the relative strengths and weaknesses of our approach in terms of computational efficiency, real-time performance, and resilience against a broader range of threats. By benchmarking our framework against these alternative solutions, we aim to provide a clearer understanding of its practical applicability and effectiveness in meeting the stringent security requirements of 6G networks.

Furthermore, we plan to expand our research by incorporating covert communications as a complementary security mechanism to PLS. Covert communications offer an additional layer of transmission security by making the presence of communication undetectable, which is highly relevant in the evolving landscape of 6G. This includes the exploration of relevant frameworks such as harvest and opportunistically relay- and covertness-aware trajectory design for UAVs to integrate covert communication principles into our study. This will provide a more comprehensive approach to 6G security, enhancing both the privacy and undetectability of transmissions.

Author Contributions: Conceptualization, H.M., T.I., T.B. and M.I.; Investigation, H.M. and T.B.; Methodology, H.M., T.I. and M.I.; Validation, H.M., T.I., T.B. and M.I.; Writing—Original draft, H.M., T.I., T.B. and M.I.; Writing—Review and editing, H.M. and M.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

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

Abbreviations

ML	Machine learning
PLS	Physical layer security
BER	Bit error rate
XR	Extended reality
IoT	Internet of Things
ITU	International telecommunication union
UAVs	Unmanned aerial vehicles
IoV	Internet of Vehicles
DT	Digital twin

FDM	Frequency division multiplexing
TDM	Time division multiplexing
PMI	Precoder matrix indexing
SNR	Signal–noise ratio
RF	Random forest
LSTM	Long short-term memory
DNN	Deep neural network
M2M	Machine-to-machine
NF	Network function
V2V	Vehicle-to-vehicle

References

1. Khattak, S.B.A.; Nasralla, M.M.; Rehman, I.U. The role of 6g networks in enabling future smart health services and applications. In Proceedings of the 2022 IEEE International Smart Cities Conference (ISC2), Paphos, Cyprus, 26–29 September 2022; pp. 1–7.
2. Oruma, S.O.; Petrovic, S. Security threats to 5G networks for social robots in public spaces: A survey. *IEEE Access* **2023**, *11*, 63205–63237. [CrossRef]
3. Hakak, S.; Gadekallu, T.R.; Maddikunta, P.K.R.; Ramu, S.P.; Parimala, M.; De Alwis, C.; Liyanage, M. Autonomous Vehicles in 5G and beyond: A Survey. *Veh. Commun.* **2023**, *39*, 100551. [CrossRef]
4. Mahmoud, H.H.H.; Ismail, T. A review of machine learning use-cases in telecommunication industry in the 5G Era. In Proceedings of the 2020 16th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 29–30 December 2020; pp. 159–163.
5. Mahmoud, H.; Aneiba, A.; He, Z.; Tong, F.; Guo, L.; Asyhari, T.; Wang, Z.; Gao, Z. Intelligent Network Optimisation for Beyond 5G Networks Considering Packet Drop Rate. In Proceedings of the 2024 IEEE International Conference on Industrial Technology (ICIT), Bristol, UK, 25–27 March 2024; pp. 1–6.
6. Mahmoud, H.H.H.; Amer, A.A.; Ismail, T. 6G: A comprehensive survey on technologies, applications, challenges, and research problems. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4233. [CrossRef]
7. Idrissi, M.; Annaz, F. Dynamic modelling and analysis of a quadrotor based on selected physical parameters. *Int. J. Mech. Eng. Robot. Res. (IJMERR)* **2020**, *9*, 784–790. [CrossRef]
8. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.H.; Debbah, M. A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2334–2360. [CrossRef]
9. Li, Y.; Aghvami, A.H.; Dong, D. Path planning for cellular-connected UAV: A DRL solution with quantum-inspired experience replay. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 7897–7912. [CrossRef]
10. Zhou, M.; Guan, Y.; Hayajneh, M.; Niu, K.; Abdallah, C. Game theory and machine learning in uavs-assisted wireless communication networks: A survey. *arXiv* **2021**, arXiv:2108.03495.
11. Wang, C.X.; You, X.; Gao, X.; Zhu, X.; Li, Z.; Zhang, C.; Wang, H.; Huang, Y.; Chen, Y.; Haas, H.; et al. On the road to 6G: Visions, requirements, key technologies and testbeds. *IEEE Commun. Surv. Tutorials* **2023**, *25*, 905–974. [CrossRef]
12. Dang, S.; Amin, O.; Shihada, B.; Alouini, M.S. What should 6G be? *Nat. Electron.* **2020**, *3*, 20–29. [CrossRef]
13. Prateek, K.; Ojha, N.K.; Altaf, F.; Maity, S. Quantum secured 6G technology-based applications in Internet of Everything. *Telecommun. Syst.* **2023**, *82*, 315–344. [CrossRef]
14. Taslimasa, H.; Dadkhah, S.; Neto, E.C.P.; Xiong, P.; Ray, S.; Ghorbani, A.A. Security issues in Internet of Vehicles (IoV): A comprehensive survey. *Internet Things* **2023**, *22*, 100809. [CrossRef]
15. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Niyato, D.; Dobre, O.; Poor, H.V. 6G Internet of Things: A comprehensive survey. *IEEE Internet Things J.* **2021**, *9*, 359–383. [CrossRef]
16. Kelley, B.; Ara, I. An intelligent and private 6g air interface using physical layer security. In Proceedings of the MILCOM 2022–2022 IEEE Military Communications Conference (MILCOM), Rockville, MD, USA, 28 November–2 December 2022; pp. 968–973.
17. Porambage, P.; Gür, G.; Osorio, D.P.M.; Livanage, M.; Ylianttila, M. 6G security challenges and potential solutions. In Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 8–11 June 2021; pp. 622–627.
18. Zuo, Y.; Guo, J.; Gao, N.; Zhu, Y.; Jin, S.; Li, X. A survey of blockchain and artificial intelligence for 6G wireless communications. *IEEE Commun. Surv. Tutorials* **2023**, *25*, 2494–2528. [CrossRef]
19. Yasar, A.; Yazicigil, R.T. Physical-Layer Security for Energy-Constrained Integrated Systems: Challenges and Design Perspectives. *IEEE Open J. Solid-State Circuits Soc.* **2023**, *3*, 262–273. [CrossRef]
20. Yerrapragada, A.K.; Ormond, P.; Kelley, B. On the application of key-based physical layer security in 5g heterogeneous networks. In Proceedings of the MILCOM 2019–2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 12–14 November 2019; pp. 1–6.
21. Furqan, H.M.; Hamamreh, J.M.; Arslan, H. Secret key generation using channel quantization with SVD for reciprocal MIMO channels. In Proceedings of the 2016 international symposium on wireless communication systems (ISWCS), Poznan, Poland, 20–23 September 2016; pp. 597–602.

22. Boodai, J.; Alqahtani, A.; Frikha, M. Review of Physical Layer Security in 5G Wireless Networks. *Appl. Sci.* **2023**, *13*, 7277. [CrossRef]
23. Hamamreh, J.M.; Furqan, H.M.; Arslan, H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Commun. Surv. Tutorials* **2018**, *21*, 1773–1828. [CrossRef]
24. Solaija, M.S.J.; Salman, H.; Arslan, H. Towards a unified framework for physical layer security in 5G and beyond networks. *IEEE Open J. Veh. Technol.* **2022**, *3*, 321–343. [CrossRef]
25. Prado-Roman, C.; Diez-Martin, F.; Blanco-Gonzalez, A. The effect of communication on the legitimacy and performance of organizations. *Rev. Bras. Gest Ao Negócios* **2020**, *22*, 565–581. [CrossRef]
26. Li, Y.; Zhao, R.; Deng, Y.; Shu, F.; Nie, Z.; Aghvami, A.H. Harvest-and-opportunistically-relay: Analyses on transmission outage and covertness. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 7779–7795. [CrossRef]
27. Li, Y.; Aghvami, A.H. Covertness-aware trajectory design for UAV: A multi-step TD3-PER solution. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 7–12.
28. Hu, Z.; Hu, J.; Yang, G. A survey on distributed filtering, estimation and fusion for nonlinear systems with communication constraints: New advances and prospects. *Syst. Sci. Control Eng.* **2020**, *8*, 189–205. [CrossRef]
29. Lee, W.; Lee, K. Deep learning-based transmit power control for wireless-powered secure communications with heterogeneous channel uncertainty. *IEEE Trans. Veh. Technol.* **2022**, *71*, 11150–11159. [CrossRef]
30. Bacanlı, E.; İlhan, H. Advantages of Using Edge Machine Learning for Communication Networks and Grasp Analysis in Robotic Hand Network Based on Federated AVG & Machine Learning. In Proceedings of the 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 9–11 June 2022; pp. 1–5.
31. Bennis, M.; Debbah, M.; Poor, H.V. Ultrareliable and low-latency wireless communication: Tail, risk, and scale. *Proc. IEEE* **2018**, *106*, 1834–1853. [CrossRef]
32. Pirayesh, H.; Zeng, H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 767–809. [CrossRef]
33. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communications. *Veh. Commun.* **2020**, *23*, 100214. [CrossRef]
34. Zhong, X.; Fan, C.; Zhou, S. Eavesdropping area for evaluating the security of wireless communications. *China Commun.* **2022**, *19*, 145–157. [CrossRef]
35. Cai, Q.Y. The ping-pong protocol can be attacked without eavesdropping. *arXiv* **2004**, arXiv:quant-ph/0402052. [CrossRef]
36. Altaweel, A.; Mukkath, H.; Kamel, I. GPS Spoofing attacks in FANETs: A systematic literature review. *IEEE Access* **2023**, *11*, 55233–55280. [CrossRef]
37. Yılmaz, M.H.; Arslan, H. A survey: Spoofing attacks in physical layer security. In Proceedings of the 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), Clearwater Beach, FL, USA, 26–29 October 2015; pp. 812–817.
38. Nassif, A.B.; Talib, M.A.; Nasir, Q.; Dakalbab, F.M. Machine learning for anomaly detection: A systematic review. *IEEE Access* **2021**, *9*, 78658–78700. [CrossRef]
39. Hassan, M.U.; Rehmani, M.H.; Chen, J. Anomaly detection in blockchain networks: A comprehensive survey. *IEEE Commun. Surv. Tutorials* **2022**, *25*, 289–318. [CrossRef]
40. Shahidinejad, A.; Abawajy, J. An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for IoT. *ACM Comput. Surv.* **2024**, *56*, 1–38. [CrossRef]