ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2025.0551

COMPREHENSIVE REVIEW OF CHALLENGES AND SOLUTIONS FOR PHYSICAL LAYER SECURITY IN IOT NETWORKS

Muhammad Hamza Rauf and Muhammad Usman
Department of Electrical and Electronics Engineering, Glasgow Caledonian University, Scotland

Abstract

The IoT (Internet of Things) networks face various types of security issues and threats at the physical layer because of massive connectivity, a large number of interconnections, and resource-constrained devices. In this research article, we have discussed the security issues, challenges, and threats at the physical layer in IoT networks, including eavesdropping, jamming, spoofing, unauthorized access, and pilot contamination. In this research, we have also highlighted various techniques and approaches to overcome the threats and issues at the physical layer of IoT networks and ensure secure connectivity, authenticity, authorization, and confidentiality. The noise aggregation and anti-eavesdropping techniques provide initial defense against unauthorized access and eavesdroppers. Radio Frequency Fingerprinting (RFF), Multiple Input Multiple Output (MIMO) systems, Non-Orthogonal Multiple Access (NOMA) technique, Secret Key Generation (SKG), and Reconfigurable Intelligent Surfaces (RIS) improve channel randomness, ensure secure connectivity, and optimize resource allocation. Cooperative techniques (jamming and beam-forming) enhance physical layer security through spatial diversity against various attacks and threats. Deep Learning-based Intrusion Detection Systems (DL-based IDS) detect and mitigate security threats, while Quantum Computing and Federated Learning solve cryptographic and privacy issues in distributed IoT networks. This research presents a comprehensive review, comparison, and analysis of physical layer security techniques for IoT networks.

Keywords:

IoT Networks, Physical Layer Security, Eavesdropping, Jamming, Wireless Channel

1. INTRODUCTION

The physical layer security in IoT networks focuses on various security techniques and approaches to ensure security at the hardware level. The objectives of physical layer security in IoT networks are to secure connectivity and communication amongst devices, networks, and nodes while mitigating threats such as unauthorized access, jamming, eavesdropping, and spoofing. The implementation of physical layer security (PLS) techniques protects the IoT networks and devices from active and passive attacks, such as eavesdropping, message modification, information leakage, pilot contamination, and jamming attacks [1]. The secrecy capacity method is used to secure connectivity while restricting the eavesdropper from accessing information [2]. The channel signature or fingerprint method relies on the Radio Frequency (RF) of the legitimate communication link and the channel impulse response, introducing noise in the direction of the eavesdropper to secure communication between legitimate users [2]. Both RFF and key generation techniques are suitable for power-constrained IoT networks due to low energy consumption. The three main steps of the RFF technique are signal segmenting, feature extraction, and identification and classification [3].

In 5G networks, physical layer security uses physical layer coding, massive MIMO, millimeter-wave communication, and non-orthogonal multiple access (NOMA) [4]. Reconfigurable Intelligent Surfaces (RIS) at the physical layer control the wireless channel to secure communication and reduce interception threats, and RIS provides better security by increasing the reflecting elements [5]. The keyless PLS techniques include code-based and artificial noise methods, and Intelligent Reflecting Surfaces (IRS) and AI-based keyless approaches play a key role in securing IoT networks [6]. The PLS in 6G networks uses RIS to secure connectivity and communication [16]. Secrecy outage probability (SOP) and average secrecy capacity (ASC) are used to analyze security in RIS-aided NOMA systems [17].

Multi-factor authentication methods using Physical Unclonable Functions (PUFs), proximity detection, and Secret Key Generation (SKG) are very effective against man-in-the-middle and jamming attacks [7]. A lightweight authentication method called MAG-PUFs uses electromagnetic emissions from IoT devices for identification [18]. The coding-based PLS scheme for downlink NOMA systems is also a secure method to restrict eavesdroppers from decoding information [19]. IoT PLS attacks are categorized into passive and active, including eavesdropping, contamination attacks, jamming, and spoofing [8], as shown in Fig.1. PLS techniques using quantum computing and federated learning also improve IoT security [9]. Blockchain secures transaction records while Machine Learning (ML) based techniques are used for detection and mitigation of Denial of Service (DoS) and Distributed DoS attacks [10]. Intrusion Detection Systems (IDS) and Deep Learning (DL) methods can detect unusual network patterns, enhance IoT security and reduce cyber-attack risks [11]. PLS techniques replace lightweight cryptographic methods to provide efficient and robust protection [12]. The IoT network security requirements include privacy, confidentiality, integrity, authentication and authorization [13]. Wireless Sensor Networks (WSN) face threats such as sinkholes, black hole, Sybil, DoS, and node injection attacks, while RFID networks are exposed to spoofing, cloning, and sniffing [14]. Spectrum-sharing technologies also address the security concerns in IoT [20], and the Cooperative Jamming (CJ) technique for multi-hop IoT networks improves security without consuming extra power [21, while traditional centralized security systems are unsuitable for IoT due to decentralized and resource-limited devices [22].

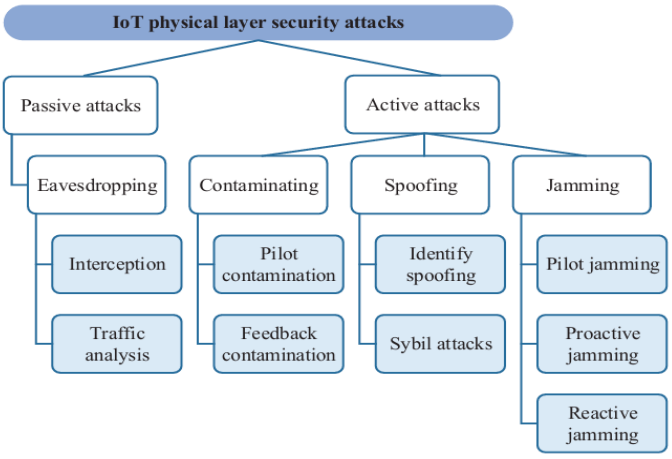

Fig.1. IoT PLS Attacks [8]

PLS needs a flexible framework to divide security methods into two main types: signal-to-interference-plus-noise ratio (SINR)-based and complexity-based approaches [23]. A Virtual Antenna Array (VAA) is used to optimize performance even with channel state information (CSI) errors and achieves higher secrecy rates than if the eavesdropper is close to the intended receiver [24]. Smart devices in IoT networks improve physical layer security, such as device protection, supply chain security, employee training, and regular vulnerability checks [25]. The Equalized Fuzzy C-Means (EFCM) vector quantization method eliminates risks to achieve high key entropy, low bit error rates, and enhances security for secure key generation in IoT networks [26]. Gaussian-Tag Embedded Authentication (GTEA) scheme using the Weighted Fractional Fourier Transform (WFRFT) performs better against spoofing and replay attacks [27]. A key generation method with random probing signals offers greater security compared to constant probing signals in the presence of active attacks [28]. A secure approach with cryptographic features using an adaptable RC6 encryption/decryption offers a suitable solution for achieving secure data transmission at the physical layer [29].

The physical layer of IoT is susceptible to adversarial attacks due to limited computations, processing, and low power [30]. In eavesdropping attacks, user information is collected from unattended devices and compromised sensors, while in sniffing attacks, malicious sensors are placed near legitimate users to intercept sensitive user data [31]. The common issues of the physical layer are physical damage, power loss, environmental threats, channel variations, hardware damage, and physical tampering [32]. The impact of mobility on physical layer security (PLS) is investigated through two random mobility models: Random Way Point (RWP) and Random Direction (RD) [33].

2. TECHNIQUES AND APPROACHES

2.1 NOISE AGGREGATION METHOD

The noise aggregation method addresses the issue of injecting artificial noise and extra power consumption in IoT networks. In the noise aggregation method, packets are assigned indices and transmitted in alternating slots such that odd-numbered packets are sent directly, while even-numbered packets are XORed with successfully decoded odd-numbered packets. The noise aggregation method uses natural channel noise instead of artificial noise without using extra power [1]. The noise aggregation method is energy-efficient and ideal for IoT applications and has already been applied in various applications to offer a practical and efficient solution for secure IoT communications.

2.2 ANTI-EAVESDROPING THROUGH CONSTELLATION ROTATION

The constellation rotation-based anti-eavesdropping technique has been introduced for securing two-way communication in untrusted relay systems. In this system, two users exchange information through an untrusted relay without data risk. The signal constellations are rotated in such a manner that each rotated signal has a one-to-one mapping with its real or imaginary component. One component is used for user data, while the other introduces artificial noise (AN) [1]. In the first phase, users A and B encode their information symbols with rotated constellations and inject AN, where the untrusted relay decodes the signals by separating the real and imaginary parts. In the second phase, the relay amplifies and broadcasts the received composite signal [1]. This constellation rotation method enhances transmission secrecy using relay assistance.

2.3 RFF AND KEY GENERATION

The manufacturing imperfections are used for variations in radio frequency (RF) components, which result in unique features and these features are detected through the electromagnetic waves emitted by each device. This process is known as radio frequency fingerprinting (RFF), which uses circuitry characteristics of transceivers to authenticate device identities through RFF identification [3]. The randomness of wireless channels and user movements are used to generate cryptographic keys.

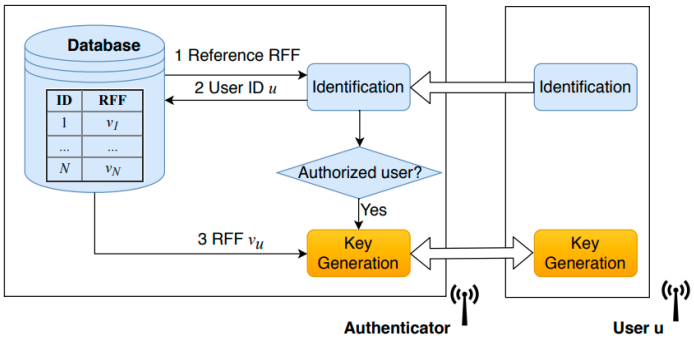

Fig.2. RFF and Key Generation [3]

RFF and key generation methods depend on the physical layer of the wireless communications protocol and integrated security framework to combine the RFF identification and key generation as given in Fig.2. Key generation performance is improved through the RFF database while the authenticator validates the identity of the user by accessing the RFF of the specific user in the database, and this information is used for key generation.

2.4 MIMO TECHNIQUE

Massive MIMO systems use antenna arrays to enhance the spatial dimensions of wireless communication and make a powerful tool for physical layer security. For passive attacks,

matched filter pre-coding, AN injection, and channel inversion are used to degrade eavesdropper channels and improve secrecy rates, while active eavesdropping is still a big challenge due to pilot contamination attack [4], pilot contamination attack on MIMO setup is shown in Fig.3. Massive MIMO can secure the connectivity of legitimate users (LUs) by providing higher received signal power than eavesdroppers, while pilot contamination attacks remain a major challenge where an active attacker uses prior knowledge of pilot signals [8].

The directional modulation (DM) in MIMO systems uses a phased array at the physical layer for secure connectivity by combining digital modulation symbols directly in the radio frequency (RF) using phase shifter [23]. This method ensures that in the intended direction, the constellation points retain their relative positions and preserve the integrity of the digital modulation symbols. In unintended directions, the amplitude and phase of the constellation points are disordered to make the signal unintelligible and degrade eavesdropper performance while enhancing communication security.

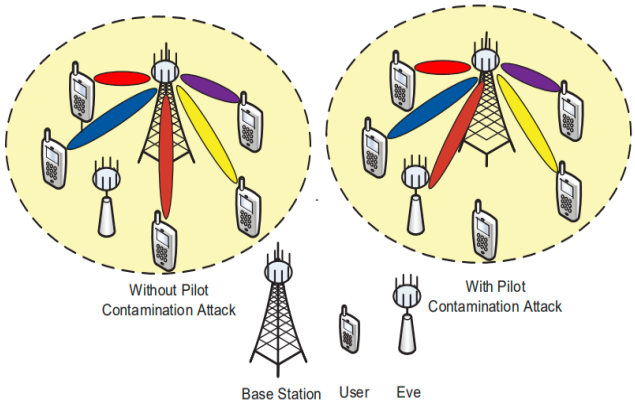

Fig.3. Pilot Contamination Attack on MIMO setup [4]

2.5 IOT WITH NOMA (NON-ORTHOGONAL MULTIPLE ACCESS)

NOMA systems face security risk when one user decodes information for another user and information leakage occurs, but NOMA protection with traditional encryption ensures secure and efficient simultaneous transmissions [4]. NOMA integration with IoT improves spectral efficiency, massive connectivity, low latency, and reduces signaling costs. User pairing in the NOMA system assigns a near and far user to a single resource block to balance system efficiency and complexity. However, pilot contamination can disrupt SIC performance, which can cause information leakage or decoding failures [8]. In frequency hopping, the base station assigns a unique sequence to each user, and allows dynamic switching and SIC decoding to enhance security and prevent eavesdropping [19]. RIS-assisted NOMA technique solves the issue of non-conclusive eavesdroppers and enhances the spectrum efficiency for 6G. The security performance is determined through SOP and ASC to show that an increasing number of RIS metasurface elements and the average SNR at the access point improve the system performance [17].

2.6 SECRET KEY GENERATION FOR IOT APPLICATIONS

The SKG technique consists of three phases, such as advantage distillation for extracting the channel parameters, information reconciliation for agreeing authorized parties on a key, and privacy amplification improves security by reducing any residual information [7]. In the pilot exchange phase, both sender and receiver use channel parameters as wireless fingerprints for proximity detection and SKG. Sender PUF generates a unique hardware fingerprint and forms a robust authentication framework. A session key is generated after successful authentication, and legitimate users use the session key and channel characteristics for secure communication [7]. This approach ensures efficient and secure communication for IoT systems by combining wireless and hardware security features.

There are five steps for secret key generation [28]: channel probing, randomness extraction, quantization, information reconciliation, and privacy amplification. Physical layer key generation can be secured against active attacks by using random probing signals to hide CSI. This technique combines user-generated randomness and channel randomness to generate a shared secret key and provide stronger security than existing techniques, which depend on constant probing signals [28].

2.7 RECONFIGURABLE INTELLIGENT SURFACE (RIS)

RIS are used to enhance communication performance, increase system secrecy, and effectively counter eavesdropping attacks in IoT systems. In the RIS setup, the system has no direct link between the access point (AP) and the IoT device or eavesdropper due to obstacles or barriers. The AP transmits with power ‘Ps’ to the IoT device over the subcarrier, constrained by maximum total power ‘Pmax’ and peak power ‘Ppeak’ on each subcarrier. The CSI for all channel power gains is assumed to be available at both the AP and IoT devices [5]. This practical system model demonstrates that RIS can optimize communication performance while mitigating security risks in IoT environments.

The analysis of SOP and ASC of RIS in the presence of an eavesdropper indicates that increasing the number of reflecting elements in the RIS significantly enhances security [5]. RIS-aided NOMA networks highlight the role of Deep Neural Networks (DNN) in optimizing power allocation for secure communication [6]. RIS-assisted communication system consists of a base station (BS), user equipment (UE), RIS controller, and a metasurface. The RIS is a two-dimensional surface with low-cost passive elements which can adjust the phase and angle of incident signals, RIS setup is shown in the following Fig.4. The constructive addition of signals for legitimate users or destructive interference for unauthorized users can enhance physical layer security by improving signal power and reducing interference [16].

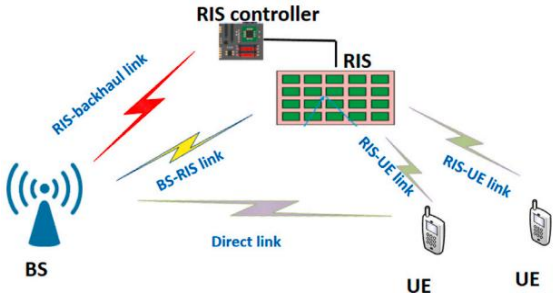

Fig.4. RIS Model [16]

The RIS-assisted NOMA system has good security performance compared to both RIS-assisted Orthogonal Multiple Access (OMA) and conventional NOMA systems. This makes it a suitable solution for real-world applications to offer secure and efficient connectivity for a large number of devices [17]. RIS can direct transmitted signals toward the receiver while canceling interference from jammers or reducing the signal-to-noise ratio (SNR) at eavesdroppers. Parameters such as transmit power, modulation, number of RIS elements, reflection coefficients, phase, angle, subcarriers, coding rate, and RF bandwidth can be adjusted based on channel conditions to enhance security [34].

2.8 QUANTUM COMPUTING AND FEDERATED LEARNING (FL)

Federated Learning (FL) has emerged as the best solution to enhance IoT security and efficiency. FL in IoT networks encounters challenges such as communication overhead, device heterogeneity, and vulnerabilities to adversarial attacks, where malicious entities can infer private data [9]. Addressing these issues requires robust techniques to ensure secure model aggregation and trust mechanisms within the FL framework. Quantum-empowered FL uses quantum algorithms to secure data exchange and ensure robust protection against adversarial attacks [9]. Quantum techniques can optimize resource allocation in heterogeneous IoT networks, reduce computational latency, and improve model convergence rates.

2.9 INTRUSION DETECTION SYSTEM (IDS) FO IOT NETWORKS

IDS is a technological solution for IoT security which is implemented via software, hardware, or both for the detection and response of malicious activities within a network. Intrusion Detection and Prevention Systems (IDPS) is used for monitoring network traffic, identifying potential threats, and detecting malicious behaviors and unauthorized access attempts. IDS has two categories, one is Signature-based Intrusion Detection Systems (SIDS) which identify known attack patterns, and the other is Anomaly-based Intrusion Detection Systems (AIDS) which detect deviations from normal behavior [11]. Significant improvements have been made through AI implementation to address cyber security threats and ensure security. AIDS is becoming an emerging solution to guarantee IoT security including server, cloud applications, connecting nodes, sensors and devices.

Deep Learning-based IDS (DL-IDS) enhances security in IoT networks by identifying various attacks and threats such as Denial of Service (DoS), brute force attacks, HTTP flooding, and UDP/TCP flooding. The IDS using deep learning can detect anomalies in IoT networks and mitigate intrusions [11] as shown in Fig.5. DL-based IDS provides scalable and efficient security measures in resource-limited networks and optimizes performance for large-scale networks to enhance IoT security.

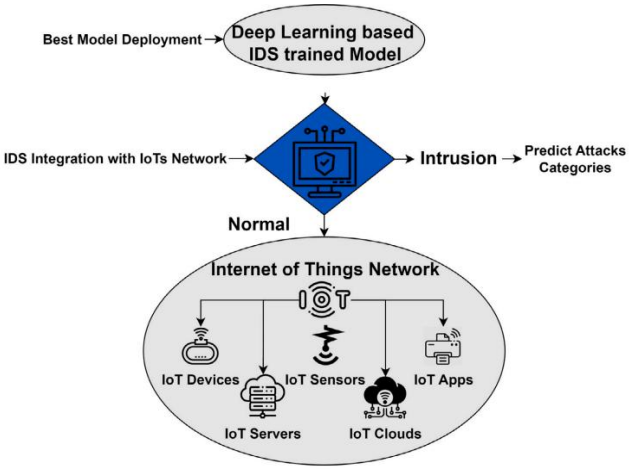

Fig.5. DL-based IDS for IoT Networks [11]

2.10 IOT NETWORKS SECURITY USING WFRFT-BASED GAUSSIAN TAG EMBEDDED AUTHENTICATION

Gaussian Tag Embedded Authentication (GTEA) is presented using weighted fractional Fourier transform (WFRFT). A low-power Gaussian WFRFT tag is embedded into the message signal for intended receiver authentication at the physical layer without alerting potential attackers. Security analysis of GTEA scheme shows resilience against spoofing and replay attacks to ensure robust protection for IoT communications [27]. WFRFT effectively counters impairments from carrier frequency offset (CFO) and mitigates inter-symbol and inter-carrier interference (ISI/ICI) in doubly selective channels. These capabilities highlight WFRFT as a powerful tool for interference suppression and enhancing physical-layer security [27].

2.11 COOPERATIVE JAMMING (CJ) AND COOPEARTIVE BEAMFORMING (CB) FOR PHYSICAL LAYER SECURITY IN IOT NETWORKS

In multi-hop IoT networks, two hybrid-duplex jamming nodes secure each transmitted symbol against colluding eavesdroppers. The proposed strategy outperforms the conventional Single Jamming (SJ) approach without increasing power consumption. CJ enhances network security to ensure resilience across various eavesdropper densities under fixed SNR conditions. It provides robust protection against eavesdroppers with different secrecy rate thresholds and minimal performance loss as the number of hops increases [21]. Cooperative Beamforming (CB) based physical layer security (PLS) schemes ensure high secrecy rates in IoT devices with limited power and hardware. However, their performance significantly drops when eavesdroppers are close to the intended receiver. CB-based PLS scheme with artificial noise injections is proposed to address this issue and operate in a distributed manner to reduce overhead in large IoT networks, CB-

based PLS with AN is shown in the given Fig.6. By analyzing the virtual antenna array (VAA) and deriving a closed-form secrecy rate expression, the scheme optimizes performance even with CSI errors. It achieves up to twice the secrecy rate of conventional CB-based PLS methods when the eavesdropper's angle is near the intended receiver's, highlighting its robustness in vulnerable scenarios [24].

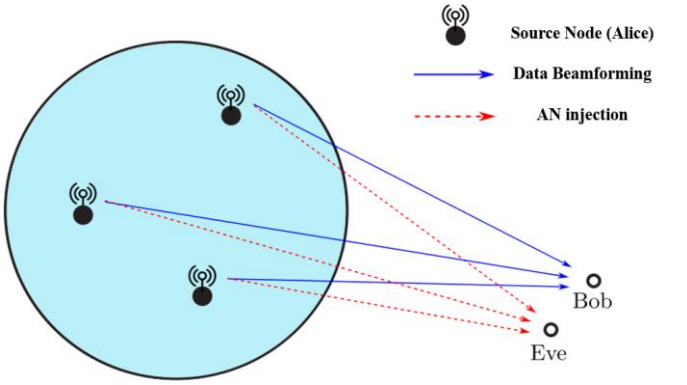

Fig.6. CB-based PLS with AN [24]

3. COMPARISON AND ANALYSIS OF TECHNIQUES AND APPROACHES

3.1 PERFORMANCE ANALYSIS OF NOISE AGGREGATION AND CONSTELLATION ROTATION METHOD

The noise aggregation method offers key advantages over traditional AN-based approaches by using the natural noise present in wireless channels and eliminating the need for extra power to generate artificial noise. This approach makes it a highly energy-efficient solution for IoT applications [1]. The constellation rotation method enhances data confidentiality by using the signal space degrees of freedom and reducing the energy burden of transmitting artificial noise. Both techniques are low-cost, energy-efficient, and suitable for IoT networks. The constellation rotation method allows adaptive power distribution between information and noise signals to offer a flexible solution for security and reliability [1]. The AN injection needs instantaneous CSI and additional power, resulting in moderate implementation complexity and potential interference to legitimate nodes. The Channel Aware Encryption (CAE) method demonstrates strong performance in IoT networks by balancing energy efficiency, low computational complexity, and robust security [12].

3.2 PERFORMANCE ANALYSIS OF RFF AND KEY GENERATION

RFF identification is a reliable authentication method in IoT networks that also facilitates secure cryptographic key generation. Both RFF and key generation techniques can be integrated into a unified framework to enhance communication security and improve the performance of key generation [3]. A practical implementation of this method is observed in smart home networks where devices such as mobile phones, televisions, and smart bulbs connect to a Wi-Fi AP that serves as an authenticator. Only registered devices are granted access, while unregistered devices are restricted and flagged as unauthorized. For successful authentication, the AP collaborates with legitimate devices to generate encryption keys [3]. The stationary devices like TVs and bulbs exhibit minimal channel variations; the movement of people within the environment introduces enough randomness to support robust key generation and maintain secure communication within the IoT network.

Channel-based and RFF physical layer authentication methods depend on the natural randomness of wireless channels and hardware imperfections, which are often uncontrollable and can limit reliability. For improving authentication performance, researchers have proposed embedding a unique tag within IoT devices to enable more reliable identification [16]. A method has been introduced for the physical layer identification of resource-constrained IoT nodes using a digital PUF integrated into the transmitter design [36]. This method allows for controlled manipulation of the RFF probability distribution to enhance RFF uniqueness and expand the dynamic range of the identification space. As a result, it delivers competitive authentication performance while significantly improving reliability, uniqueness, and overall identification capability for IoT security.

3.3 IoT WITH MIMO AND NOMA

In massive MIMO systems, sparsity and directionality are more advantageous for the physical layer's security of IoT networks. These properties allow an access point (AP) or base station (BS) to differentiate between legitimate users and attackers and make it easier to detect threats like pilot contamination in NOMA scenarios. In massive MIMO and NOMA systems, beamforming and SIC rely on precise CSI via pilot sequences [8]. Various detection mechanisms have been developed, including random pilot signal generation using phase-shift keying (PSK) symbols, where the AP detects anomalies in phase transitions to identify attackers. Attacker detection through specialized beamformers allows the AP to identify channel estimation disruptions by observing unexpected signal degradation at the legitimate user [8].

In MIMO systems, DM technique enhances physical layer security by offering a low probability of interception and preventing eavesdroppers from retrieving intelligible information [23]. Antenna subset modulation, a variant of DM, further secures communication by using only a selected subset of antennas for beamforming, focusing transmission energy toward the intended user while reducing exposure to unintended directions [23].

3.4 KEY GENEARTION CALLEGES AND SOLUTIONS

SKG schemes in wireless systems are vulnerable to DoS attacks such as jamming and Man-in-the-Middle (MiM) injection attacks. The physical layer security techniques, such as channel authentication, pilot signal randomization, and artificial noise injection, these techniques impede the attacker's channel while preserving legitimate links [7]. To address the challenges of reactive jamming, legitimate users (Alice and Bob) can perform SKG using randomized pilots across subcarriers and apply jamming detection schemes, such as variance analysis or comparison with known signal patterns to estimate and counteract Mallory's strategy before SKG begins [7]. To enhance IoT sensor security, a method has been proposed that combines public key

cryptography using Public Key Infrastructure (PKI) at the controller and identity-based cryptography (IBC) for resource-constrained sensors [13]. In this setup, PKI use a certificate authority (CA) to bind public keys to user identities, while IBC derives public keys from identity data such as IP addresses, with secret keys generated by a trusted private key generator (PKG). A novel approach integrates Feature Extraction with Equalized Fuzzy C-Means (FE-EFCM) vector quantization to enable efficient and secure key generation in IoT networks [26]. FE-EFCM outperforms traditional methods like scalar quantization and PCA K-Means to achieve lower Bit Error Rates (BER), enhance security, and reduce communication overhead and susceptibility to eavesdropping.

3.5 RIS PERFORMANCE ANALYSIS

The SOP is an important performance metric for RIS-enabled systems using physical layer security. Deploying multiple RIS units can enhance signal coverage and improve the quality of communication for legitimate users. A single RIS deployment for short-range and limited coverage IoT networks is a cost-effective and efficient solution. Increasing the number of RIS elements significantly strengthens the reflected signals, providing more degrees of freedom to amplify the main channel and suppress the wiretap channel, especially under higher average SNR conditions at AP [5]. This shows that multi-element RIS systems can improve security and overall performance in IoT networks.

The integration of RIS in 6G networks introduces significant security vulnerabilities, as attackers may utilize RIS to amplify threats. The attackers can strategically place RIS near transmitters to enhance eavesdropping by optimizing phase shifts to increase signal power, and compromise secrecy rates. RIS can also intensify jamming attacks by redirecting and amplifying interference signals to reduce the signal-to-interference-plus-noise ratio (SINR) for legitimate users [16]. The RIS enables advanced pilot contamination attacks (PCA) by changing channel responses to perform pilot spoofing, making PCA defenses ineffective and causing severe threats to MIMO systems. The vulnerabilities may arise from hardware or software loopholes which result to various attacks including jamming, spoofing, and eavesdropping.

RIS enhances spectrum efficiency through virtual line-of-sight (LoS) links between base stations and mobile users, passively reflecting incident signals to compensate for power loss over long distances. RIS operates in a passive mode, reshaping signals through phase shift control without requiring power amplifiers. This energy-efficient approach makes RIS a cost-effective solution for IoT physical layer security. RIS is also highly compatible with emerging technologies such as full-duplex, NOMA, and massive MIMO where the flexible design of RIS makes easy deployment and implementation [16]. RIS improves wireless security without information leakage to eavesdroppers and effectively cancels unwanted signals through precise reflection adjustments.

3.6 DL-BASED IDS AS AN EMERGING SOLUTION FOR IOT SECURITY

DL-based IDS, including Feed Forward Neural Networks (FFNN), Long Short-Term Memory (LSTM), and Random Neural Networks (RandNN), have shown high effectiveness in identifying cyber threats in IoT networks. The RandNN explores hidden patterns through random connections and LSTM captures temporal dynamics, FFNN outperforms both by accurately classifying attacks through complex feature learning [11]. These models enhance real-time threat detection, and future research may adopt advanced techniques like CNNs, RNNs, federated learning, hybrid architectures, and adversarial defenses to further boost detection accuracy and system resilience.

3.7 MITIGATING JAMMING, SYBIL, MIM, AND SPOOFING ATTACKS

Jamming, Sybil, and spoofing attacks are the serious threats at the physical layer of IoT networks. Countermeasures in WSNs include signal quality analysis and threshold-based detection for jamming, signal strength-based sender localization for Sybil attacks, and MAC signal strength verification for spoofing [13]. Physical layer vulnerabilities such as eavesdropping, tag cloning, and physical tampering in RFID systems also create significant risks due to weak authentication mechanisms [22]. The security requirements like confidentiality, integrity, and availability are threatened by attacks such as spoofing, jamming, and man-in-the-middle, which can be mitigated through encryption, authentication, beamforming, AN, and anti-jamming methods [16] as shown in the Fig.7.

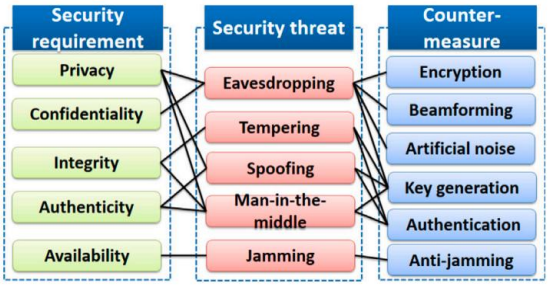

Fig.7. Security Threats and Countermeasures [16]

ML and AI techniques offer powerful tools to counter physical layer threats in IoT. For example, logistic regression and Generative Adversarial Networks (GANs) enhance spoofing detection and authentication, deep reinforcement learning is effective against jamming, while interference-based threats are also mitigated using ML algorithms [20]. Advanced schemes like Cooperative Jamming (CJ) using hybrid-duplex relays in multi-hop networks have shown superior performance compared to traditional jamming approaches without increasing power consumption [21]. The physical layer key generation processes are vulnerable to active attacks such as Disruptive Jamming (DJ), Manipulative Jamming (MJ), and Channel Manipulation (CM), which degrade or compromise the key exchange process. Techniques like channel hopping, spread spectrum, and RSS-based key extraction in rich multipath environments are effective countermeasures [28]. In smart IoT systems, threats such as MiTM, jamming, and replay attacks are addressed using random key generation, ML-based methods, and physical layer security (PLS) techniques like CAE, AN, ON–OFF switching, and secure space-time coding [37].

3.8 ANALYSIS OF SECURE BEAMFORMING AND COOPERATIVE JAMMING

Secure beamforming is an anti-eavesdropping technique that operates in the spatial domain by optimizing the transmission direction to maximize the channel quality difference between the legitimate receiver and an eavesdropper [38]. Cooperative jamming (CJ) introduces artificial noise into the system to degrade the eavesdropper signal quality, even without requiring CSI at the transmitter. The CJ uses multiple relay nodes as distributed beamformers where each independently transmits jamming signals to improve information confidentiality with moderate complexity and additional power usage [38]. RIS-based secure beamforming can enhance the secrecy rate by degrading the eavesdropper channel while improving legitimate signal quality [34]. Cooperative relaying and jamming offer spatial diversity-based security improvements for IoT networks. RIS-enabled cooperative jamming setup has also shown effectiveness in securing communications in IoT networks [34].

4. CONCLUSION

The rapid integration of IoT devices and networks is facing several challenges and security threats at the physical layer, such as eavesdropping, jamming, spoofing, unauthorized access, pilot contamination, and man-in-the-middle attacks. Eavesdropping enables attackers to intercept sensitive information, while jamming restricts legitimate communication and connectivity. Spoofing and unauthorized access allow adversaries to impersonate legitimate devices and gain unauthorized network entry. Pilot contamination and MITM attacks further threaten communication integrity by manipulating signal transmissions. These challenges, threats, and attacks are addressed via various physical layer security techniques and approaches. Noise aggregation and anti-eavesdropping techniques use channel randomness and interference to degrade the attacker's signal quality without requiring extra power. RFF ensures secure authentication through device-specific signal characteristics, while advanced MIMO and NOMA systems improve communication robustness by enhancing diversity and spectral efficiency.

RIS allows dynamic signal propagation control to strengthen secure links and connectivity at the physical layer of IoT networks. Secret key generation methods use inherent channel randomness to establish shared cryptographic keys between legitimate users. Cooperative strategies like jamming and beamforming offer added protection by using spatial diversity to disrupt eavesdroppers and enhance legitimate communication. The emerging technologies and techniques, such as DL-based IDS, AI and ML-based techniques, quantum computing, Federated Learning, and GTEA have shown promising solutions for real-time threat detection and mitigation, and reliable authentication. These technologies and techniques provide secure and reliable solutions for IoT networks and devices against threats and attacks.

REFERENCES

[1] L. Sun and Q. Du, “A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions”, *Entropy*, Vol. 20, No. 10, pp. 730-745, 2018.

[2] T. Pecorella, L. Brilli and L. Mucchi, “The Role of Physical Layer Security in IoT: A Novel Perspective”, *Information*, Vol. 7, No. 3, pp. 49-64, 2016.

[3] J. Zhang, S. Rajendran, Z. Sun, R. Woods and L. Hanzo, “Physical Layer Security for the Internet of Things: Authentication and Key Generation”, *IEEE Wireless Communications*, Vol. 26, No. 5, pp. 92-98, 2019.

[4] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.K. Wong and X. Gao, “A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead”, *IEEE Journal on Selected Areas in Communications*, Vol. 36, No. 4, pp. 679-695, 2018.

[5] D.T. Do, A.T. Le, N.D.X. Ha and N.N. Dao, “Physical Layer Security for Internet of Things via Reconfigurable Intelligent Surface”, *Future Generation Computer Systems*, Vol. 126, pp. 330-339, 2022

[6] M.S. Kumar, R. Ramanathan and M. Jayakumar, “Key Less Physical Layer Security for Wireless Networks: A Survey”, *Engineering Science and Technology an International Journal*, Vol. 35, pp. 101260-101266, 2022.

[7] M. Mitev, “Physical Layer Security for IoT Applications”, Master Thesis, School of Computer Science and Electronic Engineering, University of Essex, pp. 1-89, 2020.

[8] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao and K. Zeng, “Physical Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities”, *IEEE Internet of Things Journal*, Vol. 6, No. 5, pp. 1-7, 2019.

[9] Danish Javeed, Muhammad Shahid Saeed, I. Ahmad, M. Adil, P. Kumar and A.K.M. Najmul Islam, “Quantum-Empowered Federated Learning and 6G Wireless Networks for IoT Security: Concept, Challenges and Future Directions”, *Future Generation Computer Systems*, Vol. 128, pp. 1-34, 2024.

[10] A. Rahdari, A. Jalili, Mehdi Esnaashari, Mehdi Gheisari, A.A. Vorobeva, Z. Fang, P. Sun, V.M. Korzhuk, I. Popov, Z. Wu and T. Hamid, “Security and Privacy Challenges in SDN-Enabled IoT Systems: Causes, Proposed Solutions, and Future Directions”, *Computers, Materials and Continua*, Vol. 80, No. 2, pp. 2511-2533, 2024.

[11] S.A. Bakhsh, M.A. Khan, F. Ahmed, M.S. Alshehri, H. Ali and J. Ahmad, “Enhancing IoT Network Security through Deep Learning-Powered Intrusion Detection System”, *Internet of Things*, Vol. 24, No. 10, pp. 100936-100946, 2023.

[12] A. Mukherjee, “Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints”, *Proceedings of the IEEE*, Vol. 103, No. 10, pp. 1747-1761, 2015.

[13] A. Srhir, Tomader Mazri and M. Benbrahim, “Security in the IoT: State-of-the-Art, Issues, Solutions, and Challenges”, *International Journal of Advanced Computer Science and Applications*, Vol. 14, No. 5, pp. 1-13, 2023.

[14] Y. Harbi, Z. Aliouat, A. Refoufi and S. Harous, "Recent Security Trends in Internet of Things: A Comprehensive Survey", *IEEE Access*, Vol. 9, pp. 113292-113314, 2021.

[15] Z. Wei, C. Masouros, F. Liu, S. Chatzinotas and B. Ottersten, "Energy- and Cost-Efficient Physical Layer Security in the Era of IoT: The Role of Interference", *IEEE Communications Magazine*, Vol. 58, No. 4, pp. 81-87, 2020.

[16] S. Zhang, W. Huang and Y. Liu, "A Systematic Survey on Physical Layer Security Oriented to Reconfigurable Intelligent Surface Empowered 6G", *Proceedings of International Conference on Computers and Security*, pp. 104100-104108, 2024.

[17] A.T. Le, T.D. Hieu, T.N. Nguyen, T.L. Le, S.Q. Nguyen and Miroslav Voznak, "Physical Layer Security Analysis for RIS-Aided NOMA Systems with Non-Colluding Eavesdroppers", *Computer Communications*, Vol. 219, pp. 194-203, 2024.

[18] Omar Adel Ibrahim, S. Sciancalepore and Roberto Di Pietro, "MAG-PUFs: Authenticating IoT Devices via Electromagnetic Physical Unclonable Functions and Deep Learning", *Computers and Security*, Vol. 143, pp. 103905-103909, 2024.

[19] Amani Benamor, Oussama Habachi, Jean-Pierre Cances and Vahid Meghdadi, "Physical Layer Security for Confidential Transmissions in Frequency Hopping-Based Downlink NOMA Networks", *Computer Networks*, Vol. 67, pp. 110821-110839, 2024.

[20] L.P. Rachakonda, M. Siddula and V. Sathya, "A Comprehensive Study on IoT Privacy and Security Challenges with Focus on Spectrum Sharing in Next-Generation Networks(5G/6G/Beyond)", *High-Confidence Computing*, Vol. 4, No. 2, pp. 100220-100240, 2024.

[21] Z. Abdullah, G. Chen and J.A. Chambers, "A Cooperative Jamming Scheme for Physical Layer Security enhancement in Multihop IoT Networks with Colluding Eavesdroppers", *Proceedings of International Workshop on IEEE Statistical Signal Processing*, pp. 1-5, 2021.

[22] F. Mehdipour, "A Review of IoT Security Challenges and Solutions", *Proceedings of International Conference on Electronics, Communications and Computations*, pp. 34-45, 2020.

[23] J.M. Hamamreh, H.M. Furqan and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey", *IEEE Communications Surveys and Tutorials*, Vol. 21, No. 2, pp. 1773-1828, 2019.

[24] G. Jang, D. Kim, I.H. Lee and H. Jung, "Cooperative Beamforming with Artificial Noise Injection for Physical-Layer Security", *IEEE Access*, Vol. 11, pp. 22553-22573, 2023.

[25] S.M. Zanjani, Hossein Shahinzadeh, Seyed Mohamad Kargar, Majid Moazzami, F. Ebrahimi and M. Hemmati, "Internet of Things Security: A Review on Challenges, Solutions and Research Directions", *Proceedings of International Conference on Internet of Things and Applications*, pp. 1-8, 2023.

[26] G. Bagheri, Ali Khandan Boroujeni and S. Kopsell, "Machine Learning-Based Vector Quantization for Secret Key Generation in Physical Layer Security", *Proceedings of International Conference on Global Information Infrastructure and Networking*, pp. 1-5, 2024.

[27] N. Zhang, X. Fang, Y. Wang, S. Wu, H. Wu, D. Kar and H. Zhang, "Physical Layer Authentication for Internet of Things via WFRFT-based Gaussian Tag Embedding", *IEEE Internet of Things Journal*, Vol. 45, pp. 1-13, 2020.

[28] K. Zeng, "Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities", *IEEE Communications Magazine*, Vol. 53, No. 6, pp. 33-39, 2015.

[29] A.M. Ashraf, W.M. Elmedany and M.S. Sharif, "Secure IoT Data Transmission at Physical Layer using RC6 Encryption Technique", *Proceedings of International Conference on Future Internet of Things and Cloud*, pp. 307-315, 2022.

[30] R. Nicole, "Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions", *IEEE Access*, Vol. 11, pp. 39295-39317, 2023.

[31] S.B. Sadkhan and Z. Salam, "Security and Privacy in Internet of Things-Status, Challenges", *Proceedings of International Conference on Engineering Technology and their Applications*, pp. 1-6, 2021.

[32] S.A. Kumar, T. Vealey and H. Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions", *Proceedings of International Conference on System Sciences*, pp. 1-4, 2016.

[33] K. Yu, J. Yu and C. Luo, "The Impact of Mobility on Physical Layer Security of 5G IoT Networks", *IEEE ACM Transactions on Networking*, Vol. 31, No. 3, pp. 1042-1055, 2023.

[34] W. Khalid, M.A.U. Rehman, T.V. Chien, Z. Kaleem, H. Lee and H. Yu, "Reconfigurable Intelligent Surface for Physical Layer Security in 6G-IoT: Designs, Issues, and Advances", *IEEE Internet of Things Journal*, Vol. 56, No. 2, pp. 1-14, 2023.

[35] J.P.A. Yaacoub, H.N. Noura, O. Salman and A. Chehab, "Ethical Hacking for IoT: Security Issues, Challenges, Solutions and Recommendations", *Internet of Things and Cyber-Physical Systems*, Vol. 3, No. 1, pp. 1-15, 2023.

[36] Q. Zhou, Y. He, K. Yang and T. Chi, "Physical-Layer Identification of Wireless IoT Nodes Through PUF-Controlled Transmitter Spectral Regrowth", *IEEE Transactions on Microwave Theory and Techniques*, Vol. 57, pp. 1-11, 2023.

[37] S.N. Islam, Z. Baig and S. Zeadally, "Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures", *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 12, pp. 6522-6530, 2019.

[38] L. Sun and Q. Du, "Physical Layer Security with its Applications in 5G Networks: A Review", *China Communications*, Vol. 14, No. 12, pp. 1-14, 2017.