TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 24, No. 1, February 2026, pp. 196~205
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v24i1.27340

Advancements in physical layer key generation: a review on channel reciprocity and IoT security techniques

Syed Shafaq Ali Shah[1], Ajab Noor[2], Ruiyue Liang[3], Rahmat Ullah Zadran[4]
[1]School of Cyber Science and Engineering, Southeast University, Nanjing, China
[2]Department of Computer Science, University of Science and Technology Bannu, Bannu, Pakistan
[3]School of Computer Science and Technology, Changchun University of Science and Technology, Changchun, China
[4]School of software Engineering, FAST National University of Computer and Emerging Science, Islamabad, Pakistan

Article Info

Article history:

Received Jul 1, 2025
Revised Oct 21, 2025
Accepted Dec 8, 2025

Keywords:

Internet of things
Key generation
Physical layer security
Security protocols
Wireless channel reciprocity
Wireless communication

ABSTRACT

With the burgeoning internet of things (IoT), securing communication becomes paramount. Traditional cryptography does not meet computational needs and brute-force attacks. This review explores the state-of-the-art physical layer secret key generation (PLKG) that takes advantage of the inherent reciprocity and randomness of wireless channels. We investigate cutting-edge techniques such as feature extraction networks, domain-adversarial training, and deep learning-based approaches, evaluating their effects on the security and efficiency of key generation. In addition to these methods, the review addresses real-world challenges such as multi-user scenarios, reconciliation overhead, and inconsistent channel measurement. We believe that improved key generation rates and security can be achieved through the use of millimeter wave technology and full-duplex communication. To strengthen the robustness of key generation, the paper concludes by suggesting future directions, such as incorporating more random sources, such as physiological signals and sensor data. This comprehensive overview offers deep insights into the state-of-the-art and paves the way for reliable communication in ever more complicated IoT settings.

Corresponding Author:

Ajab Noor
Department of Computer Science, University of Science and Technology Bannu
Bannu, 28100, Pakistan
Email: ajabnoor051@gmail.com

1. INTRODUCTION

The rapid expansion of the internet of things (IoT) is significantly changing the way we live, work, and interact with technology. By connecting everyday objects such as home appliances, medical devices, vehicles, and industrial machines to the internet, as shown in Figure 1, IoT is creating smarter and more responsive environments. These technologies are now playing a key role in areas such as smart homes, healthcare, transportation, agriculture, and smart cities. This fast growth is made possible by improvements in wireless communication, cloud and edge computing, artificial intelligence (AI), and low-power electronics. Recent studies predict that in 2025, there will be more than 30 billion connected IoT devices worldwide, with a potential economic impact of up to 12.6 trillion per year by 2030 [1]-[3]. However, despite its transformative potential, the IoT paradigm introduces a host of complex challenges that have placed it at the forefront of global research and development efforts. Among the most pressing concerns is the inherent vulnerability of the wireless communication medium. Due to the broadcast nature of the wireless channel, it introduces numerous threats such as eavesdropping, denial of service, jamming, and spoofing that require

secure communication methods [4]-[6]. Traditional public-key cryptography relies on complex mathematical algorithms to secure communication between devices, requiring significant computational power and memory for encryption and decryption processes. While highly effective in conventional computing environments, these techniques become impractical for resource-constrained devices, such as those commonly found in IoT networks, where power and memory are limited. This limitation highlights the need for alternative security approaches that can provide robust protection while being lightweight and efficient, motivating the exploration of new solutions beyond traditional cryptographic methods [7]-[9].

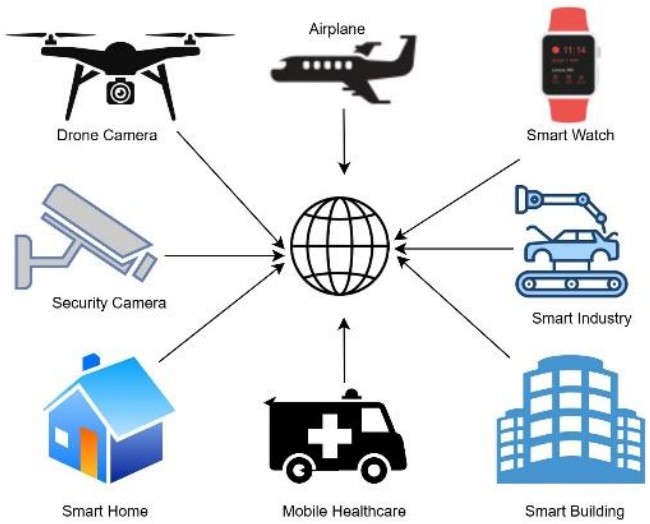


Figure 1. The application of IoT

Research developed a new lightweight technique in the 1990s called physical layer key generation (PLKG) [10], which leverages the inherent properties of wireless channels to establish secure keys between legitimate communicating parties called Alice and Bob [11]-[13]. In simple terms, PLKG uses the physical characteristics of wireless communication channels to generate a secret key between legitimate parties security. In PLKG it's important to observe high reciprocal channel features between two communicating parties. O'Shea and Hoydis [14] learn the channel feature between two communication parties by using the autoencoder, which results greater in knowledge acquisition. Zhang *et al*. [15] designed key generation model to reduce the impact of noise effect in channel reciprocity. Similarly, He *et al*. [16] used autoencoder to reduce the noise from channel state information (CSI) data. Zhou and Zeng [17] used a hybrid deep learning model autoencoder and domain adversarial neural network to enhance the channel reciprocity and secure the key from Eva. Chen *et al*. [18] designed a new approach called bidirectional convergence feature learning (BCFL) to improve the key generation rate (KGR) and reduce noise impact.

Despite the promising potential of physical layer key generation for secure wireless communications, several practical challenges continue to hinder its widespread adoption. CSI in the real world is often contaminated with substantial channel noise and weakly correlated, which existing methods struggle to eliminate effectively. Moreover, the current state of art technique [15]-[18] have difficulty adapting to intricate fluctuations in channel conditions, which can cause overfitting when the training and testing scenarios differ. These challenges are amplified in complex IoT environments, where conventional methods lack the flexibility to address data distribution shifts, causing models to become tailored to specific environments rather than being broadly generalizable. Moreover, conventional static quantization schemes struggle to adapt to rapidly changing wireless environments, which further degrades key generation performance and increasing bit disagreement rate (BDR). Given the rapid evolution of IoT applications and the increasing security threats they face, there is a pressing need for lightweight, scalable, generalized and secure PLKG frameworks tailored to real-world environments.

The purpose of this systematic review is to discuss the problem in the current state of art technique and provide a solution to solve the problem in existing research. This work highlights innovative approaches such as deep learning, domain-adversarial learning, and hybrid techniques, emphasizing their implications for securing IoT networks and beyond. By synthesizing current research efforts, identifying existing gaps, and suggesting promising future directions, this review aims to deepen understanding of PLKG methodologies

and foster the development of practical, robust, and secure key generation schemes suitable for increasingly complex wireless ecosystems. The key contributions of this review are summarized as follows:

- Reviews and synthesizes existing PLKG techniques, highlighting their strengths and limitations.
- Analyzes lightweight designs and their suitability for resource-constrained IoT environments.
- Compares quantization methods across studies in terms of KGR, BDR, and entropy performance.
- Examines the role of deep learning integration in improving robustness and adaptability in PLKG.
- Identifies open challenges, hybrid approaches, and future research directions, including cross-scenario generalization and lightweight solutions.

This review is structured as follows: section 2 presents the fundamentals of PLKG. Section 3 reviews the current state-of-the-art techniques, including deep learning approaches, hybrid deep learning models, and channel reciprocity-based methods. The section 4 provides a detailed discussion of results and analyses. Section 5 addresses open challenges and research gaps in the field. Finally, the paper concludes with a summary of key findings and outlines future research directions.

2. FUNDATMENTALS OF PLKG

Physical layer key generation is a new cryptographic method that utilizes randomness and reciprocity of wireless channels to derive secret keys between two legitimate communicating parties. Compared to conventional key exchange protocols depending on complex algorithms and computational hardness. PLKG draws common entropy from the physical wireless environment and therefore naturally aligns with the demands of lightweight and low-power applications such as the IoT. The security of PLKG arises from the inability of an adversary, located more than half a wavelength away, to observe the same channel characteristics due to the inherent spatial decorrelation of the wireless medium.

There are usually four basic steps in the key generation process: channel probing, quantization, information reconciliation, and privacy amplification, as illustrated in Figure 2. Channel probing is the first step, where both communicating parties send their pilot signals to estimate their channel state. The quantization step converts the continuous-valued channel measurement into binary strings (initial keys). Information reconciliation is applied in order to cure any mismatching bits between the two strings with the assistance of error correction codes so that both parties have an equal key. Privacy amplification is then applied to compress the shared string, removing any potential leakage and enhancing secrecy.

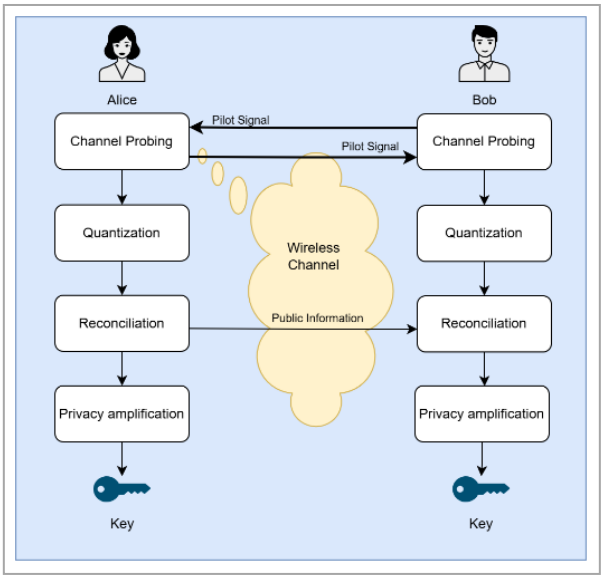


Figure 2. Four-stage physical layer key generation process, including channel probing, quantization, reconciliation, and privacy amplification

PLKG relies on three physical-layer principles channel reciprocity, temporal variation, and spatial de-correlation, each playing a critical role in ensuring secure and reliable key generation. These principles are discussed below in detail.

2.1. Reciprocity of wireless channels

Channel reciprocity is the property that the wireless channel response from node A to node B is roughly equal to that from node B to node A when measured within the channel coherence time [13]. This allows both devices to independently see well-correlated CSI and derive symmetric keys without key exchange. Reciprocity holds in time division duplexing (TDD) systems under ideal conditions; however, practical impairments such as hardware mismatches, antenna calibration errors, and oscillator drift cause asymmetries that lead to greater BDR. Mathematically, channel reciprocity can be expressed as:

$$H_{AB}(t) \approx H_{BA}(t) \quad (1)$$

where, $H_{AB}(t)$ and $H_{BA}(t)$ represent the complex channel responses from Alice to Bob and from Bob to Alice at time t, respectively.

2.2. Temporal variation and entropy

Temporal variation accounts for the time-varying nature of the wireless channel due to factors such as movement, multipath propagation, and changes in environmental conditions. The dynamics introduce randomness into the measurements of the channel, which is required for secure key generation. The use of rapid and random temporal changes guarantees high entropy and protection from predictability and replay attacks. However, in quasi-static or indoor environments where the channel is not highly fluctuating, the lack of randomness can limit key freshness and create security vulnerabilities. Mathematically, temporal variation can be expressed as:

$$E[H(t)H^*(t+\Delta t)] \to 0 \; as \; \Delta t \gg T_c \quad (2)$$

This (2) expresses that the autocorrelation between the current and future channel responses diminishes as the time delay Δt exceeds the coherence time T_c, promoting temporal randomness.

2.3. Spatial decorrelation for eavesdropper resistance

Spatial decorrelation ensures that wireless channel characteristics experienced by an adversary at a different physical location are uncorrelated with those observed by legitimate users. This spatial uniqueness is fabricated through multipath scattering and is very likely to take place when the distance from the legitimate devices to the eavesdropper is greater than half a wavelength. Therefore, even adjacent passive attackers cannot get the same key, which provides a physical-layer security against eavesdropping. This is a fundamental characteristic of the confidentiality properties of PLKG in wireless networks. Mathematically, spatial decorrelation can be expressed as:

$$E[H(x)H^*(x+\Delta x)] \to 0 \; as \; \Delta x \; > \lambda/2 \quad (3)$$

where, $H(x)$ denotes the channel at position x, and λ is the signal wavelength. The expectation tends to zero when the spatial separation Δx exceeds $\lambda/2$, indicating statistical independence.

3. PHYSICAL LAYER KEY GENERATION TECHNIQUES

The following section provides a systematic overview of the most significant key generation techniques in wireless communication, categorized into traditional signal processing techniques, deep learning-based techniques, and domain adaptation techniques. Each set of techniques is criticized based on their approach, applicability, and limitations in real-world applications.

3.1. Traditional signal processing-based techniques

Traditional PLKG techniques rely on handcrafted signal features such as received signal strength (RSS) and CSI. These approaches typically involve signal quantization, randomness extraction, and key reconciliation to produce symmetric secret keys between communicating parties.

Jana *et al.* [19] reported one of the initial empirical studies on RSS-based PLKG, citing the fallibility of signal reciprocity in real-world environments. They observed temporal noise, hardware fluctuations, and interference significantly affecting the dependability of key generation, making it in most instances, with high bit mismatch rates. To solve these disadvantages, Zhao *et al.* [20] proposed secret key extraction from channel estimates (SKECE), a CSI-based approach that takes advantage of subcarrier-level channel estimates and adaptive stream alignment to provide higher key generation throughput and resilience. This approach circumvents costly reconciliation but depends on the availability of fine-grained CSI, which is not available

and may not be provided in commercial off-the-shelf equipment. It is also established on this foundation that Lin *et al.* [21] presented an RSS-based scheme with wavelet shrinkage denoising and adaptive guard-band quantization. Their scheme improves the BDR and KGR while maintaining the design light and hardware friendly. However, the reliance on RSS also limits its entropy and robustness in static or low-variation environments. Overall, while traditional signal processing methods offer low complexity and intuitive design, they often underperform in highly dynamic or noisy conditions due to their reliance on manually engineered features and their sensitivity to environmental variability [22].

3.2. Deep learning-based methods

Temporal deep learning has recently gained much attention in physical layer key generation due to its superior feature extraction ability and robustness to noise, non-reciprocity, and environmental uncertainty [10], [16], [23], [24]. Deep learning methods are different from traditional ones that rely heavily on hand-engineered signal processing chains in that they learn optimal representations from raw CSI directly and hence manual feature engineering is avoided [25].

One of the foundational contributions to the application of deep learning in wireless communications was made by O'Shea and Hoydis [14], who proposed modeling the entire communication system as an autoencoder. This groundbreaking study presented the concept of end-to-end neural network-based cooperative learning of modulation, channel effects, and decoding. Their method showed that it is possible to use data-driven models to capture complicated channel characteristics, even if it was not primarily focused on key generation. This laid the conceptual foundation for the application of deep learning in PLKG.

Building on this foundation, Zhang *et al.* [15] proposed KGNet, one of the earliest deep learning models explicitly designed for PLKG. Aimed at frequency division duplexing (FDD) systems where conventional channel reciprocity does not naturally exist, KGNet learns a deterministic mapping between uplink and downlink CSI using a lightweight feedforward neural network. The approach maintains computational efficiency appropriate for IoT contexts while striking a positive trade-off between KGR and BDR.

To address adversarial threats in spatially correlated scenarios, Zhou and Zeng [17] introduced the domain-adversarial autoencoder (DAAE), which combines an encoder-decoder structure with adversarial learning. By extracting domain-invariant reciprocal features, DAAE seeks to improve secrecy performance even in the presence of nearby eavesdroppers. Although the model appears promising, it can only be evaluated in a single spatial configuration, and its BDR is higher than some of the current methods, suggesting that it needs to be more widely generalized.

Recognizing the limitations of handcrafted preprocessing under real-world channel impairments, He *et al.* [16] developed CRLNet, a multibranch autoencoder architecture equipped with a non-reciprocity learning module and a hybrid loss function. CRLNet, which was created for TDD-orthogonal frequency division multiplexing (OFDM) systems, efficiently reduces asymmetries in channel estimations caused by noise and hardware. It has proven to perform better in a variety of settings, surpassing traditional models in terms of robustness under different signal-to-noise ratios (SNRs), key error rate (KER), and KGR.

More recently, Chen *et al.* [18] introduced the BCFL framework, which applies convolutional neural networks (CNNs) to enhance feature convergence and noise suppression. By using a unique multiple quantization approach, BCFL greatly increases key generation randomness and throughput without adding to the computing burden. IoT applications that are resource-constrained and latency-sensitive find it especially appealing due to its effective execution.

Despite their advances, deep learning–based PLKG schemes face several practical challenges. These include the need for large volumes of synchronized training data, the risk of overfitting in diverse deployment scenarios, and the difficulty of ensuring model generalizability. Addressing these challenges will require continued exploration into self-supervised learning, cross-domain adaptation, lightweight network architectures, and adversarial robustness to ensure scalable and secure key generation across heterogeneous wireless systems.

3.3. Domain adaptation and cross-scenario learning

Current developments in physical layer key generation emphasize how important domain adaptation is to guaranteeing model durability in a variety of wireless environments. Models that have been pre-trained in one environment can be refined with little additional data in new domains thanks to the successful application of transfer learning techniques to solve domain shifts. For instance, Li *et al.* [26] proposed a cross-domain PLKG framework tailored for IoT devices, where transfer learning is leveraged to adapt key generation models efficiently under varying environmental and device conditions. This method is useful in situations where resources are limited since it significantly reduces the burden of data collecting while preserving high key agreement rates.

In addition to transfer learning, formal domain adaptation frameworks are starting to appear that seek invariant feature representations for PLKG across various networks. Several recent studies have developed adversarial and discrepancy minimization-based models, which mathematically formalize domain shifts and demonstrate improved generalization in real-world heterogeneous wireless networks. These domain adaptation methods, by aligning feature distributions between source and target domains, show promise in overcoming the challenges posed by environmental dynamics and hardware heterogeneity, thus paving the way for scalable and robust PLKG systems in practical deployments.

4. RESULTS AND DISCUSSION

In This section consolidates comparative results from the literature on physical-layer key generation, comparing KGR, BDR, model generalization, and computational complexity. We discuss signal-processing and deep learning–based techniques, including domain-adversarial learning, and interpret their implications for IoT security and scalability.

The trajectory of PLKG has seen substantial progress, yet persistent challenges remain. RSS-based approaches such as adaptive quantization with cascade and privacy amplification achieved high KGR in dynamic environments but consistently underperformed in static ones, suffering from elevated BDR [19]. Subsequent refinements, including wavelet preprocessing with modified guard-band quantization [21] and Fourier/smoothing-based curve fitting [27], improved stability and randomness quality, thereby reducing mismatch errors. However, these gains were accompanied by significant preprocessing costs and scalability issues, raising concerns for low-power IoT devices where computational budgets are minimal. Even with careful preprocessing, the reliance on environment dynamics remains a bottleneck, making these methods ill-suited for heterogeneous deployment scenarios where both high KGR and low BDR are simultaneously required. This highlights a fundamental limitation of RSS-based designs: their lack of robustness across different environmental conditions.

CSI-driven and deep learning–based schemes have emerged to mitigate these shortcomings. CSI-based techniques, notably SKECE, demonstrated markedly higher key rates and lower communication overhead compared to RSS approaches, achieving consistent randomness validation even in static settings [20]. Deep learning approaches, such as autoencoder-based models for physical-layer representation learning [14], reciprocity-mapping networks like KGNet [15] and CRLNet [16], as well as bidirectional CNN convergence models [18], have expanded the design space by capturing non-linear channel correlations. These methods reported improved KGR and reduced KER, but they face prohibitive computational complexity and training overhead. Furthermore, their generalization ability across diverse environments remains largely unverified, with most evaluations constrained to specific datasets or controlled scenarios. Although DAAE introduced explicit cross-domain adaptation [17], it still reported high BDR under practical conditions, underlining the difficulty of ensuring stable performance across deployment contexts. Collectively, while CSI and deep learning methods mark clear improvements, none provide a universally reliable solution balancing low BDR, high KGR, and cross-domain generalization.

Table 1 summarizes and compares representative PLKG techniques reported in the literature in terms of KGR, BDR/KER, model generalization, and computational complexity. This comparison highlights the trade-offs between performance, robustness, and computational cost across traditional signal-processing and deep learning–based approaches. As shown in Table 1, RSS-based schemes generally offer low computational complexity but suffer from higher BDR in static environments, while deep learning–based approaches achieve improved KGR at the expense of increased model complexity and limited generalization.

Recent advances have also explored application-driven and calibration-oriented solutions. Hardware calibration schemes [28] reduced systematic impairments and achieved lower BDR, while automatic identification system (AIS)-focused PLKG [29] optimized KGR in maritime unicast environments with lightweight complexity. These works show promising application-specific adaptability but highlight another gap: lack of universality. Their effectiveness is tightly bound to constrained domains (hardware-specific settings or maritime networks), leaving unresolved the broader challenge of building a generalizable model. Furthermore, CNN-based architectures used for convergence-driven PLKG [18] and calibration pipelines [28] impose heavy inference and resource demands, which contradict the scaling trends of IoT devices becoming increasingly resource-constrained. In summary, despite diverse methodological innovations, no existing approach has successfully unified environmental robustness, lightweight complexity, and strong randomness guarantees. This underscores a pressing need for models that can achieve cross-environment stability with both low BDR and high KGR while remaining computationally viable for next-generation IoT deployments.

Table 1. Comparative summary of PLKG techniques in terms of KGR, BDR/KER, model generalization, and computational complexity

Study	Technique	KGR (as reported)	BDR/KER	Model generalization	Computational complexity
[19]	RSS-based adaptive quantization with Cascade and privacy amplification	High KGR	High errors in static	Limited generalization	Low
[20]	CSI-based SKECE	Much higher key rate than RSS in both static and mobile	Generally low mismatch	Testing in different environments	Medium
[14]	Deep learning PLKG	N/R	Not discussed in terms of BDR/KER	Instead explores robustness, convergence	Limited
[21]	RSS with wavelet preprocessing multi-channel quantization scheme for key generation (MCQSG)	Much higher KGR than prior RSS schemes	Lower BDR	Limited discussion on model generalization	High pre-processing needed
[27]	RSS with curve fitting (Fourier/simple moving average (SMA))	Efficient with multi-bit quantization	BDR markedly reduced via preprocessing; National Institute of Standards and Technology (NIST) tests passed	Limited discussion on model generalization	Large amount of preprocessing cost
[15]	KGNet (deep learning mapping for FDD reciprocity)	Medium	Lower KER across SNRs	Limited discussion on model generalization	High complexity
[16]	Deep learning based channel reciprocity learning (CRLNet)	Improved KGR	Lower KER	Limited discussion on model generalization	Medium
[17]	DAAE	N/R	Weaker eve correlation shown	High BDR and explicit cross-domain generalization in spatially correlated channels	High complexity
[18]	Bidirectional convergence CNN for PLKG	Higher KGR	High KER	Limited discussion on model generalization	Require substantial training data
[28]	Deep learning–based hardware calibration	N/R	Low BDR	Limited discussion on model generalization	High computation cost
[29]	PLKG for AIS unicast	Reported good KGR	Reported low BDR for the testing data	Limited to ships, not generalized across different domains	Low complexity

5. OPEN CHALLENGES AND RESEARCH GAPS

Even with significant advancements in PLKG, several issues still exist, especially with the rapid evolution of wireless standards and increasingly dynamic communication environments. One prominent gap lies in multi-user key generation within 5G, millimeter-wave (mmWave), and multiple input multiple output (MIMO) systems. Most existing PLKG schemes predominantly focus on point-to-point communication scenarios. However, real-world implementations frequently entail intricate multi-user and multi-antenna setups, where secure key extraction is hampered by elements like interference, intricate beamforming, and channel asymmetries. The applicability of current frameworks in sophisticated wireless networks is limited since they have not yet adequately addressed these issues.

Static or high-mobility situations, like interior fixed settings or vehicle networks with fast Doppler changes, present another significant issue for FDD systems. Even though newer techniques like deep reciprocity learning and KGNet try to address problems caused by non-reciprocal channels in FDD, key consistency is still challenging. This is especially true in scenarios where channel reciprocity is inherently weak or severely distorted, undermining the generation of robust shared keys.

Since the majority of models are designed for small-scale fading and find it difficult to adjust to the unpredictability produced by obstacles, movement, and urban settings in the real world, the effects of large-scale fading such as shadowing and path loss—are still underexplored. Furthermore, current PLKG research frequently lacks rigorous security validation; formal information-theoretic proofs and adversarial robustness evaluations, particularly against active or learning-based attacks, are rarely addressed, despite the frequent reporting of performance metrics like KDR and KGR. Moreover, PLKG actual implementation in end-to-end

secure systems is limited by a continuing gap between the wireless and cryptographic communities that makes it difficult to integrate with accepted security protocols.

6. FUTURE RESEARCH DIRECTIONS

To advance PLKG toward practical deployment, future research should prioritize scalable and interdisciplinary solutions. Expanding PLKG to support multi-user, MIMO, and cooperative systems is essential, particularly by leveraging spatial diversity and beamforming in 5G/6G networks to enhance entropy extraction. Robust learning methods, such as meta-learning and self-supervised techniques, should be developed to handle non-reciprocal and static channels, especially in FDD or low-mobility scenarios. Incorporating environmental awareness through context data or multimodal sensing can improve stability under large-scale fading. Lightweight, on-device models using pruning, quantization, or knowledge distillation are critical for resource-constrained IoT and edge devices. Federated and collaborative learning can further reduce centralization risks while enhancing model generalization. Crucially, PLKG must be integrated into complete security frameworks, including authentication, reconciliation, and post-quantum encryption. Finally, extensive real-world testing in dynamic environments, supported by industry-academia collaboration, is vital for validating robustness and driving standardization.

7. CONCLUSION

This review has explored the progression of physical-layer key generation PLKG techniques, highlighting the transition from traditional RSS and CSI-based signal processing approaches to advanced deep learning and domain adaptation frameworks. While classical methods offer simplicity and low complexity, they often struggle in dynamic or heterogeneous environments. In contrast, deep learning models such as autoencoders, reciprocity learning networks, and domain-adversarial architectures have demonstrated strong potential in improving key reliability and robustness by learning from raw, non-reciprocal channel features.

Despite these advancements, several open challenges remain. Existing models lack scalability in complex scenarios such as multi-user MIMO, FDD, and large-scale fading environments. Furthermore, high training costs, limited real-world testing, and weak integration with cryptographic protocols hinder practical deployment. Future research should prioritize the development of lightweight, generalizable models, explore federated and on-device learning techniques, and bridge the gap between wireless signal processing and formal cryptographic systems. Addressing these gaps will be essential for building secure, scalable, and adaptive PLKG solutions for next-generation wireless networks.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Syed Shafaq Ali Shah	✓		✓		✓		✓		✓	✓	✓			
Ajab Noor						✓				✓	✓	✓		
Ruiyue Liang					✓					✓				
Rahmat Ullah Zadran		✓								✓				

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] Cisco, *Cisco Annual Internet Report (2018–2023)*. San Jose, CA, USA: Cisco, 2023. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf

[2] M. Chui, M. Collins, and M. Patel, *The Internet of Things: Catching Up to an Accelerating Opportunity*. McKinsey & Company, Nov. 2021.

[3] IoT Analytics, "State of IoT Spring 2024," 2024. IoT Analytics, [Online]. Available: https://iot-analytics.com/product/state-of-iot-spring-2024/

[4] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," *Signals and Communication Technology*. Springer US, pp. 103–135. doi: 10.1007/978-0-387-33112-6_5.

[5] R. Zhang and Y.-C. Liang, "Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 88–102, Feb. 2008, doi: 10.1109/JSTSP.2007.914894.

[6] H.-N. Dai, H. Wang, H. Xiao, X. Li, and Q. Wang, "On eavesdropping attacks in wireless networks," in *2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES)*, IEEE, Aug. 2016, pp. 138–141. doi: 10.1109/CSE-EUC-DCABES.2016.173.

[7] L. Chen, J. Ji, and Z. Zhang, *Wireless Network Security: Theories and Applications*. Berlin, Germany: Springer, 2013, doi: 10.1007/978-3-642-36511-9.

[8] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015, doi: 10.1109/COMST.2015.2388550.

[9] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, doi: 10.1109/JPROC.2016.2558521.

[10] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993, doi: 10.1109/18.256484.

[11] H. Zhao, E. Guo, Z. Lian, Y. Zhao, X. Huang, and C. Su, "A review and implementation of physical layer channel key generation in the Internet of Things," *Journal of Information Security and Applications*, vol. 83, p. 103779, Jun. 2024, doi: 10.1016/j.jisa.2024.103779.

[12] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014, doi: 10.1109/SURV.2014.012314.00178.

[13] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, New York, NY, USA: ACM, Sep. 2008, pp. 128–139. doi: 10.1145/1409944.1409960.

[14] T. O'Shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 563–575, Dec. 2017, doi: 10.1109/TCCN.2017.2758370.

[15] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, "Deep-learning-based physical-layer secret key generation for FDD systems," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6081–6094, Apr. 2022, doi: 10.1109/JIOT.2021.3109272.

[16] H. He *et al.*, "Deep learning-based channel reciprocity learning for physical layer secret key generation," *Security and Communication Networks*, vol. 2022, p. 1844345, Mar. 2022, doi: 10.1155/2022/1844345.

[17] J. Zhou and X. Zeng, "Physical-layer secret key generation based on domain-adversarial training of autoencoder for spatial correlated channels," *Applied Intelligence*, vol. 53, no. 5, pp. 5304–5319, Jun. 2022, doi: 10.1007/s10489-022-03777-w.

[18] Y. Chen *et al.*, "Physical-layer secret key generation based on bidirectional convergence feature learning convolutional network," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14846–14855, Aug. 2023, doi: 10.1109/JIOT.2023.3244993.

[19] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, pp. 321–332, 2009, doi: 10.1145/1614320.1614356.

[20] J. Zhao *et al*., "Efficient and Secure Key Extraction using CSI without Chasing down Errors," 2012, *arXiv*. doi: 10.48550/ARXIV.1208.0688.

[21] R. Lin, L. Xu, H. Fang, and C. Huang, "Efficient physical layer key generation technique in wireless communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, Jan. 2020, doi: 10.1186/s13638-019-1634-7.

[22] R. Meng *et al*., "A survey of Machine Learning-based Physical-Layer Authentication in wireless communications," J*ournal of Network and Computer Applications*, vol. 235, p. 104085, Mar. 2025, doi: 10.1016/j.jnca.2024.104085..

[23] N. Van Huynh *et al*., "Generative AI for Physical Layer Communications: A Survey," *IEEE Transactions on Cognitive Communications and Networking*, vol. 10, no. 3, pp. 706–728, Jun. 2024, doi: 10.1109/tccn.2024.3384500.

[24] C. Feng and L. Sun, "Physical layer key generation from wireless channels with non-ideal channel reciprocity: a deep learning based approach," in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, IEEE, Jun. 2022, pp. 1–6. doi: 10.1109/VTC2022-Spring54318.2022.9860995.

[25] R.-F. Liao *et al*., "Deep-Learning-Based Physical Layer Authentication for Industrial Wireless Sensor Networks," *Sensors*, vol. 19, no. 11, p. 2440, May 2019, doi: 10.3390/s19112440..

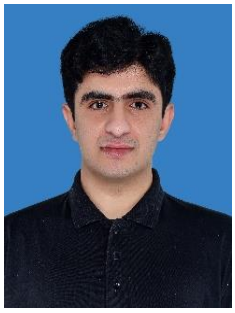
[26] J. Li, Y. Yang, and Z. Yan, "AI-Based Physical Layer Key Generation in Wireless Communications: Current Advances, Open Challenges, and Future Directions," *IEEE Wireless Communications*, vol. 31, no. 5, pp. 182–191, Oct. 2024, doi: 10.1109/mwc.013.2300448.

[27] F. Zhan, N. Yao, Z. Gao, and H. Yu, "Efficient key generation leveraging wireless channel reciprocity for MANETs," *Journal of Network and Computer Applications*, vol. 103, pp. 18–28, Feb. 2018, doi: 10.1016/j.jnca.2017.11.014.

[28] Y. Zheng, X. Wang, F. Dang, and X. Miao, "Enhancing physical-layer key generation accuracy through deep learning-based hardware calibration," in *Proceedings of the Workshop on Adaptive AIoT Systems*, New York, NY, USA: ACM, Jun. 2024, pp. 13–18. doi: 10.1145/3662007.3663883.

[29] J. Sun, Z. Yi, Z. Zhuang, and S. Jiang, "Securing automatic identification system communications using physical-layer key generation protocol," *Journal of Marine Science and Engineering*, vol. 13, no. 2, p. 386, Feb. 2025, doi: 10.3390/jmse13020386.

BIOGRAPHIES OF AUTHORS



Syed Shafaq Ali Shah received the Bachelor's degree in Computer Science from the University of Science and Technology, Bannu, Pakistan, and the Master's degree in Computer Applied Technology from Changchun University of Science and Technology (CUST), China. He is currently pursuing a Ph.D. in Cyberspace Security at Southeast University, Nanjing, China. His research interests include secret key generation, internet of things (iot) security, security protocols, and blockchain security. He can be contacted at email: syedshafaqshah479@gmail.com.

Ajab Noor received his Master of Computer Science degree and Master of Science degree in Computer Science from Gomal University, D.I. Khan, Pakistan. He is currently serving as a Lecturer at the University of Science and Bannu under the Higher Education Department, Khyber Pakhtunkhwa. His current re search interests include physical-layer key generation, security protocols, back log prioritization, sprint planning, and velocity prediction in Agile teams. He can be contacted at email: ajabnoor051@gmail.com.

Ruiyue Liang received the Bachelor' degree in the School of Software from Henan University, and she is currently studying the Master's degree in Computer Technology from Changchun University of Technology (CUST). Her research interests include intelligent information processing, secret key generation, and internet of things security. She can be contacted at email: liangry@mails.cust.edu.cn.

Rahmat Ullah Zadran received the Bachelor degree in Computer Science from the University of Science and Technology Bannu and his currently studying Master's degree in Software Engineering from the FAST National University of Computer and Emerging Science Islamabad. His research interests include secret key generation and security protocol. He can be contacted at email: syedshafaqshah2@gmail.com.