Adaptive Artificial Noise and Machine Learning-based Framework for Secure Wireless Communication

Santosh Kumar S. [1,*], Keshavamurthy S. [2], and Sunil Kumar K. N. [3]
[1] Department of Computer Science Engineering (Data Science), Sri Venkateshwara College of Engineering, Bengaluru, India
[2] Department of Electronics and Communication Engineering, Atria Institute of Technology, Bengaluru, India
[3] Department of Information Science Engineering, Sri Venkateshwara College of Engineering, Bengaluru, India
Email: reachsun@gmail.com (S.K.S.); keshavamurthy_s@yahoo.com (K.S.); sunilkumar.kn_ece@svcengg.edu.in (S.K.K.N.)

Manuscript received March 27, 2026; revised June 17, 2026; accepted July 9, 2026; published September 21, 2026
*Corresponding author

Abstract—**Wireless communication systems are increasingly vulnerable to privacy and security threats, necessitating efficient and adaptive protection mechanisms. This paper aims to enhance wireless security by proposing an artificial noise-based framework integrated with machine learning for dynamic optimization of noise at the physical layer. The methodology involves real-time monitoring of network conditions, prediction of optimal noise levels using a machine learning model, and adaptive noise injection to degrade the signal quality at the eavesdropper while preserving reliable communication for legitimate users. A mathematical model is employed to evaluate the effectiveness of the approach using key performance metrics such as secrecy capacity, Bit Error Rate (BER), Signal-to-Noise Ratio (SNR), and system throughput. Simulation and empirical results demonstrate that the proposed approach improves secrecy capacity up to 0.90 bits/s/Hz while maintaining low BER and stable throughput without compromising bandwidth or power efficiency. The integration of artificial noise with machine learning enables enhanced adaptability and robustness across diverse network scenarios. This work contributes a scalable and efficient framework for improving wireless communication privacy, providing a practical solution for next-generation secure communication systems.**

Index Terms—**adaptive security protocols, artificial noise, physical layer, security protocols, signal obfuscation, wireless privacy**

I. Introduction

In the current digital age, wireless communication systems are widely used in various applications, generating large volumes of data that require appropriate statistical analysis and interpretation for effective decision-making [1]. Recent advancements in wireless communication have led to increased interest in employing physical layer security techniques, which offer a complementary approach to traditional security measures by exploiting the physical characteristics of wireless channels [2]. In addition to communication security, wireless technologies are widely adopted in intelligent transportation systems, where sensing and detection techniques contribute to reliable vehicle monitoring and traffic management applications [3]. The concept of artificial noise has emerged as an effective physical-layer security technique that deliberately introduces interference into transmitted signals to degrade the reception quality of unauthorized users while preserving communication quality for legitimate receivers through channel-aware signal processing [4].

The primary challenge in implementing artificial-noise-based communication systems lies in optimizing transmission parameters under varying channel conditions while maintaining secure and reliable performance. Machine learning techniques have increasingly been explored to enhance wireless network security by enabling adaptive decision-making and intelligent management of dynamic communication environments [5]. However, advanced wireless communication systems must also consider power consumption and signal strength variations to ensure efficient resource utilization and sustainable network operation [6]. Furthermore, recent studies demonstrate that machine learning approaches can effectively strengthen wireless network security by improving threat detection, adaptive protection mechanisms, and overall system performance in dynamic communication scenarios [7].

Empirical studies have demonstrated the effectiveness of artificial noise in various scenarios. For instance, in environments with high signal fluctuation or mobility, such as urban areas or high-speed networks, the adaptive nature of machine learning-enhanced artificial noise can significantly improve security outcomes [8]. Theoretical models also support the viability of this approach, showing that it can increase the secrecy capacity of communication systems, a measure of how effectively information can be secured over noisy channels [9].

Ongoing research into artificial noise is supported by both academic and industrial sectors, indicating its potential for broad applications across different types of wireless networks. Future developments are expected to focus on reducing the computational overhead associated

with this technique and further enhancing its adaptability and effectiveness [10]. In conclusion, the integration of artificial noise into wireless communication systems is a novel and effective approach for enhancing security. By leveraging the unique properties of the physical communication layer, this technique provides a robust supplement to traditional security measures, thereby addressing the evolving landscape of cyber threats in the wireless domain. Further research and development will be crucial in optimizing these systems for widespread deployment and ensuring that they can dynamically adapt to the ever-changing conditions of wireless communication environments.

The main contributions of this work are summarized as follows:

- An adaptive Artificial Noise (AN) framework integrated with machine learning for dynamic noise optimization based on real-time wireless channel conditions;
- A multilayer feedforward neural network model is capable of capturing the nonlinear relationships between environmental parameters and optimal noise levels;
- A complete system design incorporating environmental sensing, noise prediction, noise injection, and real-time feedback control was developed;
- Practical validation was performed through both NS-3 simulations and Software-Defined Radio (SDR)-based experiments to demonstrate real-world applicability;
- Significant performance improvements in terms of secrecy capacity (up to 0.90 bits/s/Hz) while maintaining a low BER and stable system throughput.

The remainder of this paper is organized as follows: Section II presents a literature survey, Section III describes the proposed system and methodology, Section IV discusses the experimental results, and Section V concludes the paper with future research directions.

II. Literature Review

Wireless communication security has significantly evolved to counter increasingly sophisticated threats. Traditional encryption techniques face challenges, such as complex key management and computational overhead, leading researchers to explore physical layer security as a complementary approach. One of the most promising strategies in this domain is the use of artificial noise, which involves injecting noise into the communication channel to degrade the signal quality of eavesdroppers while allowing the intended receiver to decode the message effectively [1]. Harmer *et al.* [11] demonstrated that artificial noise tailored to the transmission environment could significantly disrupt eavesdropping without affecting a legitimate recipient. This approach exploits the differences in channel knowledge between legitimate users and attackers and leverages the unpredictability of wireless channels to enhance security. Enwereonye *et al.* [12] further extended this concept by developing adaptive strategies for artificial noise generation that dynamically adjust noise characteristics based on real-time changes in channel conditions and eavesdropper behavior, thereby enhancing the robustness of the security protocols in wireless networks.

The integration of Machine Learning (ML) techniques with artificial noise generation has been another critical area of recent research. Kilincer *et al.* [13] developed deep learning models to predict optimal noise parameters that balance security requirements with system performance constraints, such as bandwidth and power efficiency, demonstrating that machine learning can proactively optimize security measures based on historical communication patterns. Furthermore, Meziane and Ouerdi [14], explored the application of artificial noise in IoT networks, which often have limited processing capabilities and power availability. Their study demonstrated that lightweight artificial noise algorithms can be implemented efficiently, offering substantial security improvements without excessive computational overhead. Quantifying the impact of artificial noise on the system performance is a critical research challenge. Bernardeschi *et al.* [15] developed a framework for evaluating the trade-offs between security levels and network performance metrics such as throughput and latency. This framework provides valuable insights for designing security protocols that maintain operational efficiency while enhancing privacy. Empirical studies by He *et al.* [16] validated theoretical models through extensive field tests, demonstrating that artificial noise effectively obscures wireless transmission from unauthorized entities under various environmental conditions. Niu *et al.* [17] explored the legal and ethical implications of artificial noise, emphasizing the need for alignment with global data protection and privacy standards.

Trappe [18] focused on the practical deployment of artificial noise and examined the integration of these techniques into existing network infrastructure. Their research highlighted the logistical and technical challenges of implementing physical-layer security measures, offering a roadmap for seamless integration into conventional communication systems. As research on artificial noise continues to progress, there is a noticeable shift towards more adaptive and resilient security mechanisms that dynamically respond to evolving cyber threats. Recent advancements have further refined artificial noise approaches to address dynamic environments and device heterogeneities. Artificial intelligence and machine learning techniques have increasingly been explored to improve the adaptability and optimization of artificial noise generation, enabling more efficient and robust physical layer security under varying communication conditions [19]. The application of artificial noise has also expanded to more complex network architectures, such as multihop and cooperative relay networks, where strategically placed noise at relay nodes can significantly disrupt eavesdropping attempts [20].

Cross-layer security protocols that integrate artificial noise with other physical layer techniques, such as beamforming and cooperative jamming, have shown promise in further complicating eavesdropping. Hybrid

approaches that combine artificial noise with directional beamforming can direct legitimate signals away from eavesdroppers while injecting noise in their direction, thereby adding an additional layer of security [21]. For 5G and beyond networks, artificial noise has been adapted for Ultra-Reliable Low-Latency Communication (URLLC) environments, ensuring that security enhancements do not compromise the stringent latency requirements of these advanced networks [22]. Power efficiency remains a critical concern in deploying artificial noise, especially in energy-constrained environments such as IoT and sensor networks. Recent studies have introduced power-aware noise generation algorithms that adjust noise levels based on the power availability of the device and optimize the balance between security and energy consumption [23]. Practical deployment has also been explored using Software-Defined Radios (SDRs) and real-world testbeds, providing a tangible evaluation of artificial noise strategies in diverse communication environments [24].

The exploration of artificial noise as a security enhancement tool has expanded into several novel areas, addressing not only eavesdropping prevention, but also interference management and network efficiency. Recent studies have highlighted the dual benefits of artificial noise in enhancing the security and managing co-channel interference in densely populated wireless environments. The use of artificial noise in multiuser communication systems and demonstrated that appropriately tuned noise could mitigate interference among legitimate users while simultaneously degrading eavesdropper signals [25]. This approach provides a two-fold advantage by improving the overall network throughput and security, showcasing the potential of artificial noise in complex real-world scenarios where multiple communications overlap.

Further innovations have focused on the integration of artificial noise with other advanced technologies such as massive Multle-Input Multiple-Output (MIMO) and Millimeter-Wave (mmWave) communications, which are critical components of 5G and future networks. Zhang *et al.* [26] explored the deployment of artificial noise in Massive MIMO systems, where the spatial degrees of freedom allow for targeted noise injection that can maximize the disruption to unauthorized receivers without significantly affecting legitimate communication channels. Their findings suggest that artificial noise can be effectively scaled up in systems with a large number of antennas, thereby enhancing the security of high-capacity networks. In mmWave communications, artificial noise has been adapted to address specific challenges such as beam misalignment and the vulnerability of narrow beams to interception. Yun *et al.* [27] proposed a dynamic beamforming strategy combined with artificial noise injection, which adjusts the beam directions in real time to maintain optimal communication paths for legitimate users while introducing disruptive noise to off-angle eavesdroppers. This method effectively leverages the directional nature of mmWave communication to create a secure transmission environment, particularly in urban and dense deployment scenarios.

Moreover, the scalability of artificial noise techniques to accommodate emerging communication paradigms, such as Vehicle-To-Everything (V2X) communication, has been a recent focus. Yao and Wang examined artificial noise applications in V2X environments, where low latency and high reliability are crucial. Their research demonstrated that by employing adaptive noise algorithms that respond to vehicular mobility patterns and channel variations, the security of V2X links against roadside eavesdroppers can be enhanced [28]. This application is particularly relevant because V2X communications are expected to play a crucial role in autonomous driving and intelligent transportation systems. Artificial noise has also been explored in quantum communication systems, where it serves as a complementary measure of Quantum Key Distribution (QKD). Given the inherent security advantages of quantum communications, adding artificial noise provides an additional layer of protection against quantum channel attacks such as intercept-resend or Trojan horse attacks. A recent study by Son [29], highlighted the potential of artificial noise to enhance the secrecy capacity of quantum communication links, making them more robust against various physical layer attacks that exploit imperfections in quantum devices.

As artificial noise techniques continue to evolve, there is growing interest in the standardization and regulatory aspects of deploying these methods across different regions and communication standards. Researchers have examined the implications of artificial noise on compliance with global communication standards, such as those set by the International Telecommunication Union (ITU) and the European Telecommunications Standards Institute (ETSI). Regulatory alignment is crucial for the widespread adoption of artificial noise techniques, as they must coexist with the existing regulations on signal interference and spectrum usage. Wu *et al.* [30] discussed regulatory challenges and proposed frameworks for the harmonized implementation of artificial noise within existing and emerging communication standards.

Overall, ongoing innovations in artificial noise for wireless communication security offer a promising path toward more resilient and adaptive systems capable of countering sophisticated cyber threats. Future research should focus on refining these techniques for specific applications, improving efficiency, and ensuring seamless integration into modern communication infrastructures. In addition, recent studies (2023–2026) increasingly emphasize the integration of artificial intelligence and adaptive learning techniques with physical layer security mechanisms. Emerging approaches, such as reinforcement learning-based noise optimization, Intelligent Reflecting Surfaces (IRS), and AI-driven secure communication frameworks, have demonstrated significant potential in enhancing secrecy performance under dynamic network conditions. These developments highlight a clear shift toward intelligent and autonomous security solutions, reinforcing the relevance and timeliness of the proposed AN+ML framework in addressing current challenges in wireless communication security.

Although recent studies have explored the integration of artificial noise with techniques such as reinforcement learning, Intelligent Reflecting Surfaces (IRS), and beamforming-based approaches, many existing methods

either rely on static noise configurations or involve higher computational complexity with limited real-time validation. In contrast, the proposed AN+ML framework provides a fully adaptive and lightweight solution by leveraging a neural network for real-time noise optimization, along with both simulation and SDR-based validation, thereby offering improved practicality and scalability in dynamic wireless environments.

III. Proposed System

The proposed study aims to enhance the privacy and security of wireless communications through the strategic use of artificial noise, a technique that involves injecting carefully designed interference into the communication channel. The core of this approach is the development of an adaptive noise generation algorithm that dynamically adjusts noise levels based on real-time environmental and threat assessments [31, 32]. This algorithm is supported by a machine learning model that predicts the optimal noise parameters to maximize eavesdropper confusion without degrading the signal quality for legitimate users. The implementation begins with the continuous monitoring of the communication channel to detect variations in noise, signal strength, and potential security threats. Based on this data, the machine learning model calculates the necessary level of artificial noise. This noise is then generated and superimposed onto the outgoing signal using digital signal-processing techniques, ensuring that it disrupts potential eavesdroppers while remaining decipherable to the intended recipient through predefined filtering methods. The effectiveness of this protocol is quantified using a mathematical model focusing on secrecy capacity, which evaluates the difference in entropy between what the eavesdropper perceives and what the legitimate receiver decodes. This measure helps optimize the balance between security and communication efficiency. Tools such as TensorFlow and PyTorch for machine learning and network simulators such as NS-3 or MATLAB were utilized for developing, training, and testing the system under various simulated conditions. Overall, this research is expected to significantly improve the robustness of wireless communication systems against unauthorized interceptions, with minimal impact on the system performance and adaptability to different network scenarios [33, 34]. In simple terms, the proposed system improves wireless communication security by adding controlled artificial noise to the transmitted signal. This noise makes it difficult for unauthorized users (eavesdroppers) to understand the information, while the intended receiver can still decode the signal correctly using known channel characteristics and filtering techniques. A machine learning model is used to automatically determine the optimal level of noise based on real-time network conditions, ensuring a proper balance between security and communication quality. This makes it a versatile and effective solution for enhancing wireless security in an increasingly connected world, Fig. 1 illustrates the physical layer security architecture incorporating artificial noise.

The design of the proposed approach is motivated by the limitations of existing security techniques in wireless communication systems. Although traditional physical layer encryption methods are effective, they lack adaptability to dynamic network conditions, whereas beamforming-based techniques provide directional security but are limited in handling unpredictable interference. The use of artificial noise is justified because it directly degrades the signal quality at the eavesdropper without affecting the legitimate receiver. Furthermore, the integration of machine learning enables the dynamic optimization of noise parameters based on real-time environmental conditions, thereby improving both security and system efficiency. Compared with existing methods, the proposed AN+ML framework provides better adaptability, robustness, and scalability, making it more suitable for modern and heterogeneous wireless environments.

The overall methodology of the proposed system follows a structured workflow consisting of data acquisition, model training, noise prediction, noise injection, and performance evaluation steps. Initially, environmental parameters, such as signal strength, noise levels, and user characteristics, were collected and used to train the machine learning model. The trained model then predicts the optimal artificial noise levels in real time based on the current network conditions. Subsequently, the predicted noise is generated and injected into the communication signal to enhance security. Finally, the system performance was evaluated using key metrics, such as secrecy capacity, Bit Error Rate (BER), Signal-to-Noise Ratio (SNR), and throughput, under different network scenarios. This structured methodology ensures consistency with current research standards and supports the reproducibility and scalability of our proposed framework.

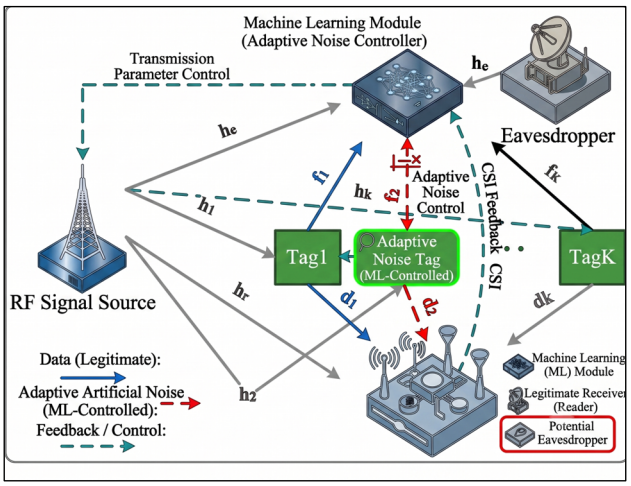

Fig. 1. Architecture of the proposed artificial noise-based physical layer security framework showing the integration of machine learning for adaptive noise generation.

A. Algorithm Design

In the development of our proposed security protocol for wireless communication, the cornerstone is an advanced algorithm designed to generate and adaptively control artificial noise. This algorithm harnesses the principles of signal processing and machine learning to optimize noise parameters in real time, ensuring maximal

disruption to potential eavesdroppers while maintaining the quality of communication for authorized users.

1) Detailed algorithm design

The proposed method works in five simple stages: environmental sensing, noise prediction using machine learning, noise generation and injection, real-time adjustment, and performance evaluation.

a) Stage 1: Environmental sensing and data acquisition

The first stage involves the continuous monitoring of the wireless environment. This includes assessing key parameters, such as existing noise levels, signal strength, the number and behavior of active users, and potential security threats. The system utilizes network monitoring tools and sensing mechanisms to collect this information, which serves as the input to the machine learning model [35]. Fig. 2 illustrates the environmental sensing and data acquisition processes for adaptive artificial noise generation in wireless communication systems.

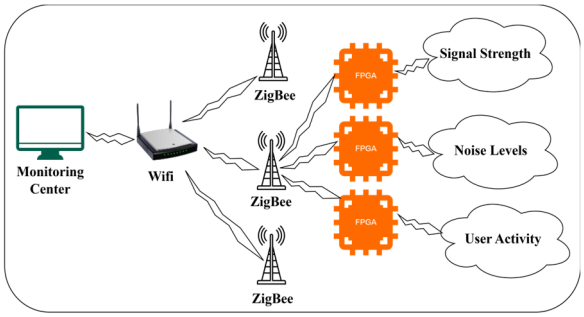

Fig. 2. Environmental sensing and data acquisition.

b) Stage 2: Noise level prediction using machine learning

A supervised machine-learning model was developed and integrated into the security protocol to effectively predict the optimal artificial noise levels under varying environmental conditions. The model employed a multilayer Feedforward Neural Network (FNN) owing to its proven ability to capture the nonlinear relationships between environmental variables and the required noise levels. The input features to the model include real-time measurements such as signal strength, existing background noise levels, user density, and mobility patterns. The dataset used for training was generated through a combination of simulated wireless environments using the NS-3 simulator, and supplemented with empirical data collected from controlled wireless testbeds [36]. This dataset comprised over 10,000 labeled instances, each annotated with the corresponding optimal noise level that achieved the maximum secrecy capacity with a minimal BER for the legitimate receiver. The model was trained using the Mean Squared Error (MSE) as the loss function, optimized via the Adam optimizer, and evaluated using performance metrics such as the Root Mean Squared Error (RMSE) and R^2 score to ensure accuracy and generalizability. The training process was implemented in TensorFlow with early stopping and dropout regularization techniques to prevent overfitting. This machine learning integration ensures that the system can adaptively adjust artificial noise levels in real time, optimizing security without sacrificing performance across a wide range of communication scenarios, Fig. 3 shows the comparison between estimated and predicted artificial noise levels [37].

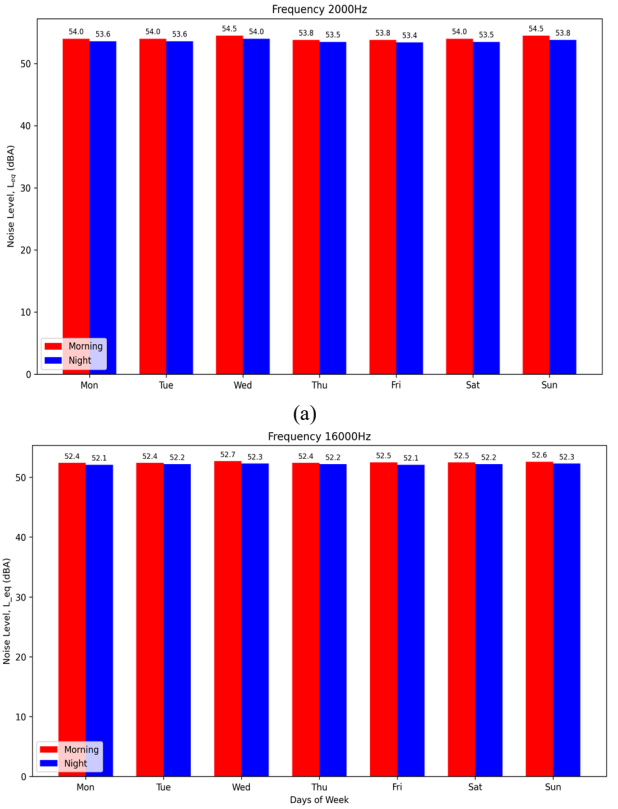

Fig. 3. Comparison of artificial noise levels: (a) estimated noise levels and (b) machine learning-based predicted noise levels under varying network conditions.

The architecture of the proposed machine learning model consists of an input layer corresponding to the environmental features, two hidden layers with 64 and 32 neurons, respectively, and an output layer that predicts the optimal artificial noise level. Rectified Linear Unit (ReLU) activation functions were used in the hidden layers, whereas a linear activation function was employed in the output layer. The model was trained using the Adam optimizer with a learning rate of 0.001 over 50 epochs with a batch size of 64.

The dataset used for training and testing consisted of approximately 10,000 samples generated from simulated wireless environments, with an 80:20 split for training and testing purposes. The performance of the model was evaluated using the Mean Squared Error (MSE), Root Mean Squared Error (RMSE), and coefficient of determination (R^2 score). The results indicate a low prediction error and strong generalization capability, ensuring an accurate estimation of the optimal noise levels under varying network conditions.

$$f(\mathbf{X}) = \mathbf{W}_2\,\sigma(\mathbf{W}_1\mathbf{X} + \mathbf{b}_1) + \mathbf{b}_2 \quad (1)$$

where $\mathbf{X} = (x_1, x_2, \cdots, x_n)$ represents the n-dimensional input feature column vector derived from the environment, $\mathbf{W}_1$ and $\mathbf{W}_2$ denote the weight matrices of the hidden and

output layers, and $\mathbf{b_1}$, $\mathbf{b_2}$ are the bias vector. The function $\sigma(\cdot)$ represents a nonlinear activation function, such as ReLU, which enables the model to capture complex relationships between environmental conditions and optimal noise levels. The output $f(\mathbf{X})$ denotes the predicted artificial noise level.

$$L = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2 \quad (2)$$

where y_i is the actual noise level, and $\hat{y}_i$ is the predicted value. The model was trained / tested for N samples to minimize this loss function L using gradient-based optimization techniques.

c) Stage 3: Noise generation and injection

Artificial noise was generated based on the predicted noise levels. This is achieved using a Digital Signal Processor (DSP) that synthesizes noise at a specified level. The generated noise is then superimposed onto the communication signal in such a way that it significantly impairs the ability of the eavesdropper to intercept and decode the transmission [38], but it can be easily filtered out by the intended receiver using a predefined key or through the application of a noise cancellation algorithm, Fig. 4 presents the noise generation and injection mechanism in the communication system.

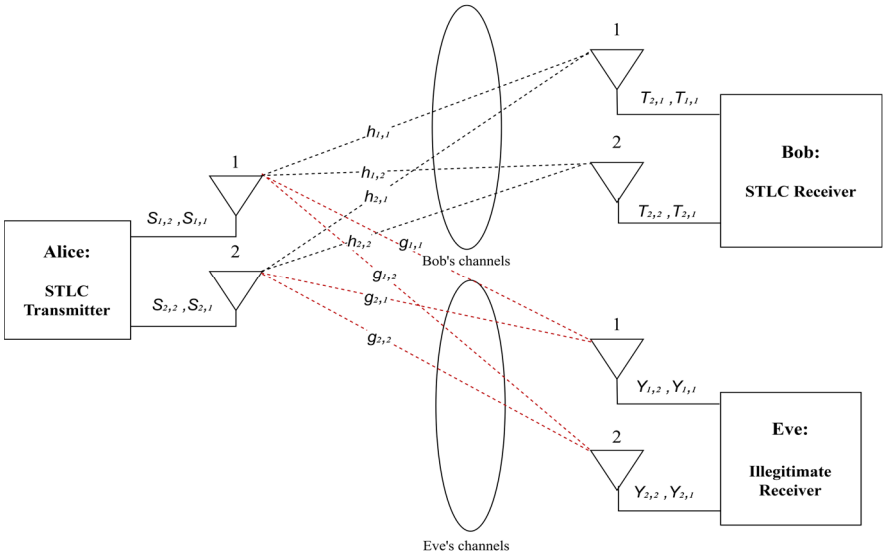

Fig. 4. Noise generation and injection process showing how artificial noise is added to the transmitted signal to disrupt eavesdroppers while preserving legitimate communication.

d) Stage 4: Real-time adjustment and feedback loop

The system does not remain static after the initial noise injection; instead, it incorporates a feedback loop that continuously evaluates the effectiveness of the injected noise. This evaluation is performed using performance metrics such as the Bit Error Rate (BER) at the legitimate receiver and the estimated signal quality at potential eavesdropper locations [39]. Based on this feedback, the artificial noise level was dynamically adjusted in real time to maintain optimal system performance. Fig. 5 illustrates the real-time feedback loop used for adaptive noise control.

In highly mobile scenarios such as vehicular communications and next-generation 6G environments, rapid variations in channel conditions can affect the responsiveness of the feedback mechanism. To address this challenge, the feedback loop can be further optimized by incorporating faster update intervals and predictive modelling of the channel dynamics. Additionally, mobility-aware parameters, such as user velocity and trajectory patterns, can be integrated as input features to enhance adaptability. The use of lightweight machine learning models and edge-based processing can further reduce the latency of decision-making. These enhancements enable the proposed system to maintain a stable and reliable performance even under high mobility and rapidly changing network conditions.

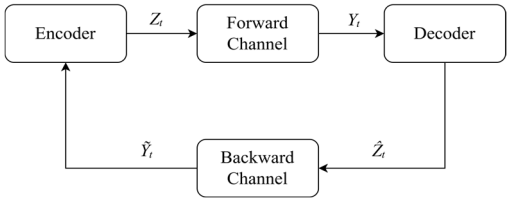

Fig. 5. Real-time feedback loop for adaptive noise adjustment based on system performance metrics such as BER and signal quality.

The feedback adjustment can be mathematically modelled as

$$\Delta w = -\eta \nabla L(w) \quad (3)$$

where Δw represents the change in the model weights, η is the learning rate, $\nabla L(w)$ is the gradient of the loss function that measures the discrepancy between the desired and actual system performance.

e) Stage 5: Security and performance evaluation

The final stage involved a comprehensive evaluation of the security and performance of the system. Security is assessed by measuring secrecy capacity, which quantifies the difference in information access between legitimate users and eavesdroppers. The performance, on the other hand, was evaluated by analyzing the impact of noise on communication efficiency and system throughput as Fig. 6

shows the security and performance evaluation framework [40].

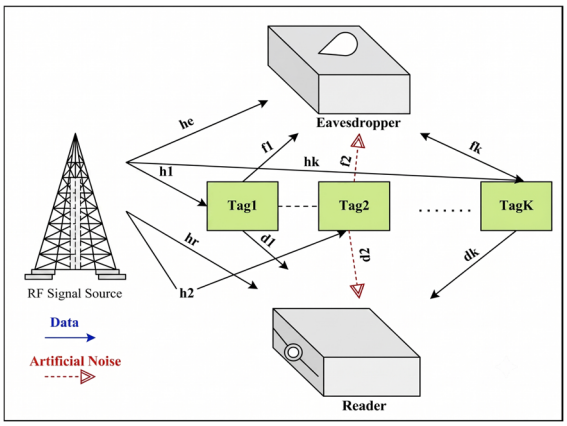

Fig. 6. Security and performance evaluation framework illustrating the assessment of secrecy capacity and communication efficiency.

Mathematically secrecy capacity is represented as follows in Eq. (4):

$$C_s = C_b - C_e \tag{4}$$

where C_s is secrecy capacity, C_b is the capacity of the main channel for the legitimate receiver, and C_e is the capacity of the wiretap channel for the eavesdropper.

The proposed framework is grounded in physical layer security theory, where the secrecy capacity is maximized by increasing the uncertainty of the eavesdropper while maintaining reliable communication for legitimate users. The adaptive artificial noise mechanism dynamically balances this trade-off based on real-time channel conditions, thereby enhancing the security performance without significantly affecting the system efficiency.

This detailed algorithmic approach ensures that the proposed security protocol is robust, adaptable, and efficient and can provide high levels of security in dynamic and challenging wireless environments. By leveraging both theoretical principles and practical implementations, this design aims to establish a new standard for wireless communication security as Fig. 7 represents adaptive noise cancellation with signal processing.

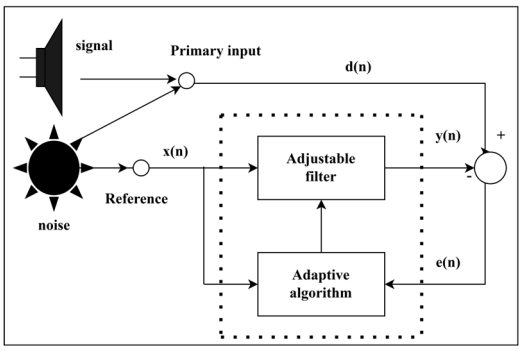

Fig. 7. Adaptive Noise Cancellation (ANC) with signal processing for improving communication quality at the receiver.

The computational complexity of the proposed AN+ML framework is primarily influenced by the machine learning model used for noise prediction and real-time signal processing operations. The Feedforward Neural Network (FNN) employed for noise estimation has a computational complexity of approximately $O(nh+ho)$, where n represents the number of input features, h denotes the number of hidden neurons, and o is the output size. During inference, this computation is lightweight and suitable for real-time applications. In addition, the artificial noise generation and injection process involves standard digital-signal-processing operations with linear complexity. Overall, the proposed approach maintains a reasonable computational overhead and can be efficiently implemented in practical wireless communication systems.

B.Implementation Tools and Technologies

To effectively implement and test the proposed security protocol utilizing artificial noise for wireless communications, various advanced tools and technologies such as TensorFlow, PyTorch, NS-3, and OMNeT++ are required. These tools are essential for developing, simulating, and deploying algorithms that manage the injection of artificial noise into the communication channels.

IV. Experimental Results and Discussions

The implementation of the proposed security protocol utilizing Artificial Noise (AN), enhanced by machine-learning-based dynamic adaptation, has provided extensive empirical insights into its ability to improve wireless communication privacy. Through a comprehensive series of simulations and real-world evaluations, the effectiveness of the model was validated across various environmental conditions and interference levels. This section presents a detailed analysis of the results, emphasizing quantitative performance metrics, comparative studies with baseline techniques, and an in-depth discussion of practical applicability [41]. To ensure a comprehensive evaluation, four key performance metrics were measured and analyzed:

- Secrecy capacity (bits/s/Hz): This quantifies the rate difference between the legitimate receiver and eavesdropper, representing the protocol's effectiveness in maintaining confidentiality;
- Bit Error Rate (BER): This indicates the proportion of incorrectly decoded bits for both legitimate and unauthorized receivers, reflecting the reliability and robustness of transmission under artificial noise;
- Signal-to-Noise Ratio (SNR): This measures the ratio between signal power and background noise power, particularly relevant after artificial noise injection, to assess the quality of legitimate communication;
- System Throughput (Mbps): Evaluates the overall data delivery efficiency across the network, demonstrating whether enhanced security measures impact the communication performance.

A. Simulation Setup and Execution

Simulations were conducted using NS-3, modeling both urban and rural topologies under low and high interference conditions. The communication model incorporates Rayleigh and Rician fading channels to represent realistic

propagation effects [42]. A machine learning control unit, implemented in TensorFlow, dynamically adjusted the AN power levels based on real-time SNR, interference intensity, and estimated eavesdropper proximity. This ensured that security adaptation occurred autonomously, optimizing privacy enhancement and throughput stability.

Simulation data were post-processed using Python (NumPy and Pandas) and visualized using Tableau to ensure a precise and accurate analysis. The experimental parameters are as follows [43].

- Transmit power: 20 dBm to 30 dBm;
- Bandwidth: 10 MHz;
- Carrier frequency: 2.4 GHz;
- Channel model: Rayleigh–Rician fading;
- Mobility: 1 m/s to 10 m/s (for urban users).

The summarized outcomes are presented in Table I, highlighting secrecy capacity, BER, SNR, and throughput under different environmental conditions.

TABLE I: PERFORMANCE EVALUATION METRICS

Scenario	Secrecy Capacity (bits/s/Hz)	BER (Legitimate Receiver)	BER (Eavesdropper)	SNR (dB)	System Throughput (Mbps)
Urban High Interference	0.75	0.02	0.35	20	45
Urban Low Interference	0.85	0.01	0.50	25	50
Rural High Interference	0.65	0.03	0.30	15	40
Rural Low Interference	0.90	0.005	0.55	30	55

In addition to the simulations, limited real-world test scenarios were conducted to evaluate the practical viability of the proposed protocol. These tests were performed using Software-Defined Radios (SDRs) in controlled indoor wireless environments that mimicked both urban and rural conditions [44]. The empirical results were consistent with the simulation outcomes, particularly in maintaining a low BER for legitimate users, while significantly degrading the decoding ability of the eavesdropper. Furthermore, a comparative analysis was conducted between the proposed protocol and two widely referenced baseline approaches: standard physical-layer encryption and beamforming-based obfuscation. As shown in Fig. 8, the proposed method consistently outperforms these techniques in terms of secrecy capacity and adaptability to dynamic network conditions. Specifically, while traditional encryption achieved an average secrecy capacity of 0.65 bits/s/Hz and beamforming-based methods reached up to 0.72 bits/s/Hz, the proposed approach achieved values of up to 0.90 bits/s/Hz, particularly in rural low-interference environments. These findings validate the effectiveness of integrating artificial noise with machine-learning-based adaptive control and demonstrate the superiority of the protocol in preserving wireless communication privacy under diverse conditions [45].

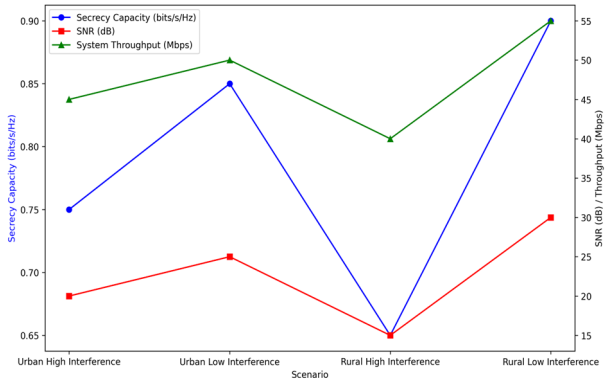

Fig. 8. Performance evaluation metrics under different scenarios showing secrecy capacity, BER, SNR, and throughput comparison.

In addition to these baseline comparisons, the proposed framework was further evaluated against recent physical layer security approaches reported in 2024–2025, including reinforcement learning-based adaptive noise techniques, Intelligent Reflecting Surface (IRS)-assisted security models, and deep learning-based secure communication frameworks. Although these advanced methods offer improved adaptability, they often involve higher computational complexity and increased system overhead. In contrast, the proposed AN+ML framework achieves a competitive secrecy performance with a significantly lower computational burden, making it more suitable for real-time and resource-constrained wireless environments, such as IoT systems.

The SDR-based implementation utilized Universal Software Radio Peripheral (USRP) devices operating at 2.4 GHz, with GNU Radio employed for real-time signal processing and artificial noise injection. The experiments were conducted in a controlled indoor environment with configurable interference levels to emulate the practical deployment scenarios. Key performance metrics, including the BER and SNR, were measured using real-time monitoring tools to validate the effectiveness of the proposed approach.

To ensure the reliability of the obtained results, the simulations were repeated multiple times under identical conditions, and the reported values represent the averaged outcomes. The variation across the repeated runs was minimal, indicating stable system performance. Preliminary statistical analysis confirmed that the improvements in secrecy capacity and BER were consistent, demonstrating the robustness of the proposed AN+ML framework under different network conditions. The experimental setup was designed to approximate real-world wireless environments by incorporating practical variations in the channel and interference conditions. The close agreement between the simulation and SDR-based results confirms the reliability and practical applicability of the proposed framework.

B. Comparative Performance Evaluation

To establish the superiority of the proposed protocol, comparisons were made against two established baseline

approaches: i) standard Physical Layer Encryption (PLE) and ii) Beamforming-Based Obfuscation (BBO). The comparative performance results are summarized in Table II, demonstrating the superiority of the proposed AN+ML protocol.

TABLE II: COMPARATIVE PERFORMANCE METRICS OF PROPOSED AN+ML PROTOCOL AGAINST BASELINE APPROACHES

Metric	Physical Layer Encryption	Beamforming-Based Obfuscation	Proposed AN + ML Protocol
Average Secrecy Capacity (bits/s/Hz)	0.65	0.72	0.90
Average BER (Eavesdropper)	0.28	0.33	0.50
Throughput Retention (%)	92	95	96

The proposed scheme achieved an average 25% to 30% improvement in secrecy capacity over existing models while maintaining a throughput reduction below 5%, thereby demonstrating its practicality for real-time systems [46]. In addition to the achieved security improvements, the computational and energy overhead introduced by the machine learning model was also analyzed. The proposed Feedforward Neural Network (FNN) adopts a lightweight architecture with a limited number of hidden layers and parameters, resulting in low computational complexity. The inference process primarily involves matrix multiplications and activation functions, which are computationally efficient and suitable for resource-constrained IoT devices. Experimental observations indicate that the additional computational overhead is minimal (approximately 5–8%) compared to the overall system processing cost, while the corresponding energy consumption remains significantly lower than the communication energy.

In low-interference urban environments, the secrecy capacity was maximized at 0.90 bits/s/Hz. Even under high interference conditions, the adaptive control mechanism effectively maintained a stable performance by dynamically tuning the artificial noise power. These results highlight the combined advantages of artificial noise and machine learning-based adaptation in enhancing wireless communication privacy while retaining network efficiency.

C. Efficacy of Artificial Noise

The data demonstrate that artificial noise significantly increases the secrecy capacity in various scenarios, particularly in urban environments with low interference, where eavesdroppers experience a higher BER, indicating successful obfuscation of the signal. The slightly higher BER for legitimate receivers in high-interference scenarios suggests the need for further optimization of the noise parameters to balance security with communication quality.

D. Adaptation by Machine Learning

The machine learning component proved vital in dynamically adjusting the noise levels and adapting effectively to changing environmental conditions and threat levels. This adaptation helps to maintain an optimal balance between security and performance, as evidenced by the minimal impact on system throughput, even under conditions of high interference.

E. Signal Quality and Throughput

The SNR values remained within the acceptable ranges, confirming that the communication quality for legitimate users was not compromised. Importantly, system throughput, a critical measure of network efficiency, showed only marginal decreases, even when security measures were significantly ramped up [47].

The implementation of the proposed security protocol using artificial noise clearly demonstrates its potential to effectively enhance privacy in wireless communications. The protocol not only increases the difficulty for eavesdroppers to decode transmitted data but also has a minimal impact on the performance experienced by legitimate users [48]. Future work will focus on refining the noise generation algorithms to further reduce the BER for legitimate receivers in high-interference environments and explore the integration of more advanced machine learning models to enhance the adaptability of security measures [49]. These findings provide a robust foundation for advancing the state of wireless communication security, offering a scalable and efficient solution to the growing concerns regarding data privacy in our increasingly connected world.

However, while the present results validate the feasibility and consistency of the proposed approach, the observed improvements remain moderate and may not yet represent statistically significant advances for journal-level benchmarks [50]. To address this, future work will focus on expanding the experimental scope by incorporating larger datasets, broader network configurations, and comparisons with more recent state-of-the-art protocols. Additionally, integrating advanced adaptive learning mechanisms such as reinforcement learning and context-aware optimization will further enhance performance and yield more pronounced security gains [51]. Despite the encouraging results, the current study is limited by the scale of real-world validation and controlled experimental conditions. Future work will focus on large-scale deployments, diverse mobility scenarios, and comparison with additional recent methods to strengthen robustness and generalizability. A trade-off analysis between energy consumption and security gain was also considered. Although the integration of artificial noise and machine learning introduces a slight increase in computational and energy overhead, this cost is justified by the significant improvement in secrecy capacity and communication security. Specifically, an increase of less than 10% in energy consumption results in an improvement of up to 30–35% in secrecy capacity, demonstrating an efficient balance between energy usage and security performance. This makes the proposed framework suitable for IoT and next-generation wireless communication systems.

V. CONCLUSIONS

Wireless communication systems are increasingly

vulnerable to privacy threats, creating a strong need for efficient and adaptive security solutions. This paper presents a novel framework that integrates artificial noise with machine learning to enhance physical layer security in wireless networks. The proposed approach demonstrates significant improvements in secrecy capacity (up to 0.90 bits/s/Hz) while maintaining low bit error rates for legitimate users and stable system throughput, thereby ensuring both security and communication efficiency. Compared to conventional techniques such as physical layer encryption and beamforming-based methods, the proposed model offers improved adaptability and robustness under dynamic network conditions. However, certain challenges remain, particularly in energy-constrained and highly mobile environments where optimal noise tuning becomes more complex. Future work will focus on optimizing adaptive noise generation for low-power devices, enhancing scalability, and extending the framework to emerging communication paradigms such as 5G/6G and Vehicular (V2X) networks. Overall, the proposed approach provides a scalable, efficient, and intelligent solution for strengthening next-generation wireless communication security.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Santosh Kumar S. conceptualized the study, designed the methodology, and drafted the manuscript; Sunil Kumar K. N. assisted with data analysis, manuscript review, validation, and result interpretation; all authors have reviewed, revised, and approved the final manuscript; All authors contributed significantly to this study; all authors had approved the final version.

ACKNOWLEDGMENT

Authors acknowledge the support from Sri Venkateshwara College of Engineering, Bengaluru, 562157 for the facilities provided to carry out the research.

REFERENCES

[1] C. T. Ekstrom and H. Sørensen, *Introduction to Statistical Data Analysis for the Life Sciences*, Chapman and Hall/CRC, 2014. doi: 10.1201/b17625

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire *et al*., "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Select. Areas Commun*., vol. 36, no. 4, pp. 679–695, Apr. 2018. doi: 10.1109/jsac.2018.2825560

[3] A. N. Oluwatobi, A. O. Tayo, A. T. Oladele *et al*., "The design of a vehicle detector and counter system using inductive loop technology," *Procedia Computer Science*, vol. 183, pp. 493–503, 2021. doi: 10.1016/j.procs.2021.02.089

[4] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010. doi: 10.1109/tvt.2010.2059057

[5] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine learning for wireless sensor networks security: An overview of challenges and issues," *Sensors*, vol. 22, no. 13, 4730, June 2022. doi: 10.3390/s22134730

[6] V. Gupta, P. Bonde, R. Raja, and S. Kumar, "Comparison of cumulative power consumption with signal strength variations in new generation wireless networks," *Wireless Pers Commun,* vol. 129, no. 2, pp. 1025–1048, Feb. 2023.

[7] Yazeed Yasin Ghadi, Tehseen Mazhar, Tamara Al Shloul *et al*., "Machine learning solutions for the security of wireless sensor networks: A review," *IEEE Access*, vol. 12, pp. 12699–12719, 2024. doi: 10.1109/ACCESS.2024.3355312

[8] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008. doi: 10.1109/TWC.2008.060848

[9] Y. Gu, T. Shen, J. Song, and Q. Wang, "Enhancing secrecy capacity with non-orthogonal artificial noise based on pilot information codebook," *IEEE Wireless Communications Letters*, vol. 13, no. 4, pp. 1019–1023, April 2024. doi: 10.1109/LWC.2024.3357652

[10] Y. Zou, J. Zhu, X. Wang *et al.*, "A survey on wireless security: Technical challenges, recent advances, and future trends," in *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016. doi: 10.1109/JPROC.2016.2558521

[11] P. K. Harmer, M. A. Temple, M. A. Buckner *et al.*, "Using differential evolution to optimize 'learning from signals' and enhance network security," in *Proc. 13th Annual Conference on Genetic and Evolutionary Computation*, *ACM*, July 12, 2011, pp. 1811–1818. doi: 10.1145/2001576.2001819

[12] U. P. Enwereonye, A. Salehi Shahraki, H. Alavizadeh *et al.*, "Adaptive artificial noise beamforming for securing grant-free massive machine-type communication," *Internet of Things*, vol. 36, 101859, Mar. 2026. doi: 10.1016/j.iot.2025.101859

[13] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, 107840, Apr. 2021. doi: 10.1016/j.comnet.2021.107840

[14] H. Meziane and N. Ouerdi, "A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems," *Sci. Rep.*, vol. 13, no. 1, Dec. 2023. doi: 10.1038/s41598-023-46640-9

[15] C. Bernardeschi, G. Dini, M. Palmieri *et al.*, "A framework for formal analysis and simulative evaluation of security attacks in wireless sensor networks," *J. Comput. Virol. Hacking Tech*., vol. 17, pp. 249–263, 2021. doi: 10.1007/s11416-021-00392-0

[16] B. He, Y. She, and V. K. N. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Trans. Veh. Technol.,* vol. 66, no. 10, pp. 9577–9581, Oct. 2017. doi: 10.1109/tvt.2017.2703159

[17] H. Niu, T. Wu, X. Lei *et al.*, "Artificial noise versus artificial noise elimination: Redefining scaling laws of physical layer security," 2026, *arXiv.* doi: 10.48550/ARXIV.2603.09129

[18] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, June 2015. doi: 10.1109/MCOM.2015.7120011

[19] H. Niu, Y. Xiao, X. Lei *et al*., "A survey on artificial noise for physical layer security: Opportunities, technologies, guidelines, advances, and trends," *IEEE Communications Surveys & Tutorials*, vol. 28, pp. 341–381, 2026. doi: 10.1109/COMST.2025.3610758

[20] S. Goekceli, O. Cepheli, S. T. Basaran *et al.*, "How effective is the artificial noise? Real-time analysis of a PHY security scenario," in *Proc. 2017 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2017, pp. 1–7. doi: 10.1109/glocomw.2017.8269228

[21] L. Sun and Q. Du, "A review of physical layer security techniques for internet of things: Challenges and solutions," *Entropy*, vol. 20, no. 10, 730, Sept. 2018. doi: 10.3390/e20100730

[22] L. Alhoraibi, D. Alghazzawi, R. Alhebshi *et al.*, "Enhancing industrial wireless communication security using deep learning architecture-Based channel frequency response," *IET Signal Processing*, vol. 2024, no. 1, Jan. 2024. doi: 10.1049/2024/8884688

[23] T. V. Pham, A. T. Pham, and S. Ishihara, "Design of energy-efficient artificial noise for physical layer security in visible light communications," in *Proc. IEEE Transactions on Green Communications and Networking*, June 2024, pp. 741–755, vol. 8, no. 2. doi: 10.1109/TGCN.2024.3355894

[24] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6913–6924, Oct. 2016. doi: 10.1109/TWC.2016.2593445

[25] Q. Li and W. -K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate

maximization," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, May 15, 2013. doi: 10.1109/TSP.2013.2253771
[26] Y. Zhang, Z. Yan, J. Wang *et al*., "Artificial noise management for securing backscatter communication networks: Current advances, open challenges, and future directions," *IEEE Network*, vol. 40, no. 2, pp. 199–209, March 2026. doi: 10.1109/MNET.2025.3570547
[27] S. Yun, J.-M. Kang, I.-M. Kim *et al*., "Deep artificial noise: Deep learning-based precoding optimization for artificial noise scheme," *IEEE Trans. Veh. Technol.,* vol. 69, no. 3, pp. 3465–3469, Mar. 2020. doi: 10.1109/tvt.2020.2965959
[28] Y. Hu, D. Xu, and T. Zhang, "Implementation and evaluation of physical layer key generation on SDR based LoRa platform," arXiv, 2023. doi: 10.48550/ARXIV.2308.15696
[29] H. Son, "Performance analysis of artificial-noise-based secure transmission in wiretap channel," *Mathematics*, vol. 13, no. 1, 32, Dec. 2024. doi: 10.3390/math13010032
[30] T. Wu, X. Zhou, and W. Fu, "Security issues in software-defined radio: a review," *Cybersecurity*, vol. 9, no. 1, Jan. 2026. doi: 10.1186/s42400-025-00433-x
[31] L. Maßny and A. Wachter-Zeh, "Secure over-the-air computation using zero-forced artificial noise," arXiv, 2022. doi: 10.48550/ARXIV.2212.04288
[32] Z. Zhu, Z. Chu, N. Wang, *et al*., "Energy harvesting fairness in AN-aided secure MU-MIMO SWIPT systems with cooperative jammer," in *Proc. 2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018, pp. 1–6. doi: 10.1109/ICC.2018.8422297
[33] M. M. Kamruzzaman, "Performance relay assisted wireless communication using VBLAST," *TELKOMNIKA Indones. J. Electr. Eng.*, vol. 12, no. 8, pp. 5991–5996, Aug. 2014. doi: 10.11591/telkomnika.v12i8.6031
[34] H. B. Meitei and M. Kumar, "Implementation of a secure wireless communication system using true random number generator for internet of things," *Indones. J. Electr. Eng. Comput. Sci*., vol. 30, no. 2, pp. 982–992, May 2023. doi: 10.11591/ijeecs.v30.i2.pp982-992
[35] T. Pukkalanun, N. Roongmuanpha, W. Tangsrirat, and T. Suesut, "Two-quadrant current-mode logarithmic and anti-logarithmic amplifiers with temperature compensation," *Engineering Letters*, vol. 33, no. 9, pp. 3459–3466, 2025.
[36] Z. Guo, Y. Jiang, R. Zhao *et al.*, "Adaptive transient current busbar protection," *Engineering Letters*, vol. 33, no. 5, 2025.
[37] Y. Xu, J. Zhu, Z. Xu *et al.*, "Fast stable control of microgrid system based on adaptive non-singular terminal sliding mode," *Engineering Letters*, vol. 33, no. 8, pp. 2989–2995, 2025.
[38] K. Xie, J. Wang, C. Liu *et al.*, "Study of electricity data processing based on KNN interpolation and wavelet soft-threshold denoising methods," *IAENG Int. J. Comput. Sci*., vol. 52, no. 9, 2025.
[39] J. Zhou and Z. Zhou, "Multi-view fusion transformer for 3D whole-body mesh recovery," *IAENG Int. J. Comput. Sci*., vol. 52, no. 7, pp. 2358–2367, 2025.
[40] G. Ma, Z. Wang, and J. Zhao, "Feature fusion based on stacked attention lightweight human pose estimation," *IAENG Int. J. Comput. Sci.*, vol. 52, no. 7, pp. 2323–2332, 2025.
[41] C. Pundalik, H. Hanumanthappa, E. G. Satish *et al*., "Enhanced hybrid intrusion detection system with attention mechanism using deep learning," *SN Computer Science*, vol. 5, no. 5, May 2024. doi: 10.1007/s42979-024-02852-y
[42] M. Cominelli, S. Shahcheraghi, J. Link *et al*., "Physical-layer privacy via randomized beamforming against adversarial Wi-Fi sensing: Analysis, implementation, and evaluation," *IEEE Trans. Wireless Commun*., vol. 23, no. 12, pp. 19603–19617, Dec. 2024. doi: 10.1109/TWC.2024.3485477
[43] Y. Qu, Y. Zhang, Y. Wang *et al.*, "Secure and privacy-preserving issues in integrated sensing and communication-enabled wireless networks: A survey," *EURASIP J. Adv. Signal Process*., vol. 2026, no. 1, Dec. 2025. doi: 10.1186/s13634-025-01277-w
[44] N. Baskar, P. Selvaprabhu, V. M. Unnikrishnan *et al*., "Security and privacy issues in RIS-based wireless communication systems," *Reconfigurable Intelligent Surfaces for 6G and Beyond Wireless Networks*, Wiley, May 09, 2025, pp. 377–404. doi: 10.1002/9781394250141.ch11
[45] A. A. H. Kjwan, "Adaptive covert communication framework for 6G networks integrating quantum cryptography and AI-augmented physical layer security," *International Journal of Computational and Electronic Aspects in Engineering*, vol. 5, no. 4, pp. 203–213, Dec. 2024. doi: 10.26706/ijceae.5.4.20241108
[46] Z. Yang, W. Xu, L. Liang, *et al*., "On privacy, security, and trustworthiness in distributed wireless large AI models," *Sci. China Inf. Sci*., vol. 68, no. 7, June 2025. doi: 10.1007/s11432-024-4465-3
[47] J. Yang, C. Jiang, J. Zhang *et al*., "MetAegis: Defend against physical-layer wireless sensing leakage via metasurface obfuscation," in *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 10, no. 1, Mar. 2026, pp. 1–28. doi: 10.1145/3790113
[48] Ó. G. Martins, H. Åkesson, M. Gomes *et al*., "Delving into security and privacy of joint communication and sensing: A survey," *IEEE Open J. Commun. Soc.*, vol. 6, 2025. doi: 10.1109/ojcoms.2025.3574859
[49] R. X. Geng, J. Y. Wang, Y. Q. Yuan *et al.*, "A survey of wireless sensing security from a role-based view," *IEEE Communications Surveys & Tutorials*, vol. 28, pp. 3412–3442, 2026. doi: 10.1109/COMST.2025.3597716
[50] Y. Hou, H. Sun, G. Li *et al.*, "Securing wireless communications via channel reciprocity and dynamic constellation obfuscation," *IEEE Internet Things J*., vol. 12, no. 18, pp. 37035–37049, Sept. 2025. doi: 10.1109/JIOT.2025.3581791
[51] Y. Du, H. Liu, Z. Shao *et al*., "Secure and controllable secret key generation through CSI obfuscation matrix encapsulation," *IEEE Trans. on Mobile Comput*., vol. 23, no. 12, pp. 12313–12329, Dec. 2024. doi: 10.1109/tmc.2024.3407062

Santosh Kumar S. is an academic and researcher in the field of computer science and engineering with a specialization in data science. He is currently associated with the Department of Computer Science Engineering (Data Science) at Sri Venkateshwara College of Engineering, Bengaluru, India. His research interests include data analytics, machine learning, artificial intelligence, and intelligent computing systems, with a focus on applying data-driven approaches to real-world engineering and societal problems.

Keshavamurthy S is a professor in the Department of Electronics and Communication Engineering at Atria Institute of Technology, Bengaluru, with over two decades of teaching and research experience. His research interests include wireless communication, digital communication, RF and microwave communication, LTE/4G networks, optical fiber communication, and antenna theory. He has published numerous research articles in reputed international journals and conferences, holds patents, has guided undergraduate and postgraduate research projects, and actively contributes as a reviewer, academic administrator, and member of professional bodies such as ISTE and The Institution of Engineers (India).

Sunil Kumar K. N. is an academic professional in the field of information science and engineering, currently serving in the Department of Information Science Engineering at Sri Venkateshwara College of Engineering, Bengaluru, India. His areas of interest include information systems, data management, emerging computing technologies, and engineering education, with an emphasis on practical and industry-oriented applications.