ISSN: 2617-5517 (issn.org)
Al-Farabi Journal of Engineering Sciences
https://iasj.rdd.edu.iq/journals/journal/view/97
مجلة الفارابي للعلوم الهندسية تصدرها جامعة الفارابي

A Physical-Layer Security Enhancement Technique Against Eavesdropping in OFDM Systems

Name :- Amjed Khashea Bdaiwi
E-mail amjedkhashea@gmail.com
وزارة الكهرباء شركة توزيع بغداد فرع الكرخ

Introduction

Wireless communication systems have become an essential part of modern life, and they continue to expand in scale and complexity. As these systems depend on open broadcast channels, they face constant risks of unauthorized interception. An attacker can receive the transmitted signal without the need for direct interaction with the legitimate users, which creates a serious security challenge. Traditional security solutions rely mainly on cryptographic algorithms that operate at higher network layers. While these methods are strong, they do not protect the physical radio transmission itself, and they depend on key management procedures that can fail or be exposed[1].

Physical layer security has emerged as a parallel approach that aims to improve confidentiality by using the characteristics of the wireless channel. Instead of focusing on encryption alone, physical layer security tries to reduce the quality of the signal received by an eavesdropper, while keeping the quality acceptable for the legitimate receiver[2]. This idea is especially important for systems where devices are simple, have limited processing power, or cannot rely on complex encryption techniques[3].

Orthogonal Frequency Division Multiplexing is one of the most widely used transmission schemes in modern networks, including WiFi, LTE, and many broadband systems. OFDM is efficient and resistant to multipath fading, but its structure also makes passive eavesdropping easier, since the signal is transmitted over many subcarriers in a predictable way. For this reason, securing OFDM at the physical layer remains an active and important research problem[4].

Several techniques have been proposed in the past, such as artificial noise injection, cooperative jamming, and advanced beamforming. Many of these approaches require multiple antennas, accurate channel information, or additional hardware that may not be available in practical deployments. Artificial noise is one of the simplest methods, but traditional versions of it also reduce the performance for both the attacker and the legitimate receiver.

This paper presents a practical enhancement technique based on injecting noise that is generated from a light secret key shared only between the transmitter and the legitimate receiver. The key creates noise that Bob can remove but Eve cannot. The proposed method is simple, does not require multiple antennas, and can be implemented in software. To

evaluate its effectiveness, a complete Python based simulation is developed using OFDM under different channel conditions and modulation schemes. The results show a clear performance gap between the legitimate receiver and the eavesdropper, which demonstrates the benefit of the proposed approach.

Related Works

Related work on physical layer security and artificial noise has expanded quickly in recent years, especially with the growth of 5G and beyond wireless systems. Shi et al. (2022) presented a broad survey of physical layer security techniques for future wireless networks. They summarized keyless and key-based strategies such as secure key generation, directional modulation, spatial modulation, covert communication, and intelligent reflecting surface aided communication, and highlighted that artificial noise is one of the most practical tools to create a performance gap between the main and wiretap channels. However, the survey remained mostly conceptual and did not focus on simple single-antenna OFDM implementations that can be reproduced in software[5].

Several recent papers studied artificial noise injection as a concrete enhancement method. Bang et al. (2022) proposed an artificial-noise based physical layer security scheme for device-to-device communication in vehicular platooning networks. Their design injects artificial noise to disrupt eavesdroppers while preserving the reliability of the legitimate link, and the work evaluates secrecy rate and bit error rate under vehicular channel conditions. The scheme is scenario specific and optimized for D2D links, not for a generic OFDM link with flexible modulation and channel models as considered in this work[6]. Ren et al. (2022) analyzed an artificial noise aided intelligent reflecting surface MIMO–OFDM system, where the IRS phases and artificial noise covariance are jointly optimized to maximize secrecy performance. This approach significantly improves secrecy in rich multi-antenna scenarios but requires additional IRS hardware and centralized optimization, which is beyond the scope of low-complexity SISO OFDM studied here[7].

Other authors integrated artificial noise with advanced waveform or coding designs. Hameed and Hasan (2023) introduced a time-reversal precoding based OFDM-DCSK system with artificial noise injection (TRAN-OFDM-DCSK). Their system combines chaos based modulation, time-domain pre-coding using Bob's channel, and artificial noise to maximize secrecy rate, with analytical expressions for bit error rate and secrecy capacity for both Bob and Eve. While this work is close to our topic, it relies on DCSK and a more complex chaos generator, and does not provide a simple OFDM baseline in which artificial noise is added directly in the time domain and evaluated only through simulated bit error rate[8]. Pham et al. (2024) studied artificial noise design for visible light communication channels with signal clipping. They formulated an optimization problem for artificial noise power allocation under clipping distortion and proposed a sub-optimal design to improve secrecy rate in VLC multicarrier systems. Their focus is on optical channels and LED nonlinearity rather than radio OFDM links with Rayleigh or AWGN channels[9], [10].

In parallel, a number of works examined artificial noise in new 5G and 6G architectures. Boodai et al. (2023) reviewed physical layer security for 5G wireless networks, discussing artificial noise, secure beamforming, cooperative relaying, and reconfigurable intelligent surfaces, and identified open issues in practical implementation and power allocation strategies in realistic networks[11]. Arzykulov et al. (2023) studied artificial noise and RIS-

aided physical layer security and showed that integrating RIS with properly designed noise can significantly improve secrecy rate in multi-antenna systems[12]. Deng et al. (2024) proposed a hybrid RIS and artificial noise assisted scheme where an active RIS and a passive RIS jointly improve the secrecy of downlink communication[13]. Rahmani et al. (2025) focused on 5G New Radio cell-free massive MIMO and introduced cooperative artificial noise methods in the null space of users' channels, showing that cooperative AN can protect physical downlink channels against passive and active eavesdroppers without requiring extra RF chains at the user side[14]. Jadoon et al. (2025) proposed a random frequency diverse array directional modulation scheme with added artificial noise for 5G and beyond, achieving improved secrecy performance but again depending on special array structures and directional modulation hardware[15].

More generally, surveys such as the deep learning based physical layer security review by Sharma et al. (2023) and the RIS-based physical layer security overview by Zhang et al. (2025) emphasized that recent research often combines artificial noise with intelligent surfaces, machine learning, or complex multi-antenna schemes. These studies underline a research gap for simpler single-antenna OFDM models that still capture key effects of artificial noise and power allocation but can be implemented and reproduced easily in software tools such as Python or MATLAB for educational or low-cost prototype purposes[16], [17].

Compared with these works, the present study concentrates on a minimal yet flexible SISO OFDM model with a single legitimate receiver and one eavesdropper. It injects artificial noise directly at the physical layer through a power splitting factor between the useful signal and the noise, and it evaluates performance mainly in terms of simulated bit error rate for Bob and Eve under different modulation formats, channel models, and power allocation values. The goal is not to optimize a particular network architecture such as RIS, VLC, or massive MIMO, but to provide a clear and reproducible framework that shows how artificial noise can be used to create a controllable performance gap between Bob and Eve, using only standard OFDM processing and without additional hardware or infrastructure[18], [19].

Year	Main scenario	Waveform / system	Security technique	Extra hardware (MIMO, RIS, VLC, etc.)	Artificial noise role	Gap relative to this work
2022	General future wireless networks	Various	Survey of many physical layer security tools	None	Described conceptually, not implemented	No concrete OFDM simulation with Bob and Eve BER
2022	D2D vehicular platooning	Radio, D2D links	Artificial noise for secure D2D PLS	None (link level model)	Jams eavesdropper in vehicular channels	Scenario specific, not a generic OFDM testbed
2022	IRS-MIMO–OFDM downlink	OFDM with MIMO and IRS	Joint IRS and AN design	MIMO plus intelligent reflecting surface	AN optimized with IRS phases to maximize secrecy	Needs IRS and multi-antenna optimization
2023	SISO TRAN-OFDM-DCSK wiretap channel	OFDM-DCSK chaos based	Time-reversal precoding and AN injection	Chaos generator, TR precoder	TR focuses AN away from Bob	Uses DCSK and complex TR, not plain OFDM
2023	5G wireless networks (review)	Various	Review of PLS including AN and RIS	System level	Discusses AN concepts and use cases	No detailed single-link OFDM BER simulations
2024	VLC multicarrier with clipping	Optical multicarrier	Optimized AN under LED clipping	VLC hardware with LEDs	AN designed considering clipping distortion	Optical domain, not RF OFDM with Rayleigh/AWGN
2023	RIS-aided PLS	Radio with RIS	Joint RIS configuration and AN	Reconfigurable intelligent surface	AN cooperates with RIS to improve secrecy	Focus on RIS; assumes more complex infrastructure
2025	5G NR cell-free massive MIMO downlink	OFDM based 5G NR	Cooperative AN in null space	Many access points (CF-mMIMO)	APs broadcast AN jointly in users' null space	Network-level design, not simple SISO OFDM
2025	5G and beyond directional modulation	Random frequency diverse array	Directional modulation with AN	Special antenna array hardware	AN plus DM to confuse eavesdropper beams	Hardware dependent and not easily reproduced

System Model

- System Architecture

The considered system is a single transmitter that communicates with one legitimate receiver, called Bob, in the presence of a passive eavesdropper, called Eve. All nodes use a single antenna. The physical layer of the system is based on orthogonal frequency division multiplexing (OFDM), and the same OFDM frame is observed by Bob and Eve through different wireless channels[20].

At the transmitter, binary information bits are first generated and mapped to complex symbols using either QPSK or 16-QAM modulation. These symbols are arranged over (N) orthogonal subcarriers and transformed to the time domain by an inverse fast Fourier transform (IFFT). A cyclic prefix (CP) of length (L_{\text{CP}}) is appended to each OFDM symbol to combat inter symbol interference. The resulting time domain signal is then transmitted over the wireless channel[21].

Bob and Eve both receive the broadcast signal but through different channels. Bob's channel is denoted as the main channel, while Eve's channel is the wiretap channel. Both channels are modeled either as additive white Gaussian noise (AWGN) channels or as flat Rayleigh fading channels on a per-OFDM-symbol basis. Bob and Eve remove the cyclic prefix, perform a fast Fourier transform (FFT), and then apply symbol detection[22].

To enhance security at the physical layer, the transmitter injects artificial noise (AN) into the OFDM symbols. This noise is generated from a light secret key that is shared only between the transmitter and Bob. Bob uses the same key to reconstruct and cancel the artificial noise before symbol detection. Eve does not know this key and therefore cannot remove the artificial noise from her received signal[23].

- **Mathematical Layers**

This subsection introduces the main mathematical notation used in the model.

Let (N) denote the number of OFDM subcarriers and let (M) denote the number of OFDM symbols in one simulation block. The total number of complex data symbols in the frequency domain is then (N M). The baseband information symbol on subcarrier (k) and OFDM symbol index (m) is written as[24]:

$$X_d[m \quad ,k], \qquad m = 0, \dots, M-1, k = 0, \dots, N-1.$$

The artificial noise symbols generated in the frequency domain are written as

$$X_{an}\,[m,k]$$

The transmitter applies a power splitting factor $\alpha \in (1,0)$ between the useful data and the artificial noise. The composite frequency domain symbol on each subcarrier is

$$X_t[m,k] = \sqrt{\alpha}X_d[m,k] + \sqrt{1-\alpha}X_{an}[m,k]$$

For each OFDM symbol index (m), the vector of subcarrier symbols is transformed to the time domain using an IFFT[25]:

$$x_t[m,n] = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X_t[m,k]\, e^{j2\pi kn/N}, n = 0, \dots, N-1$$

A cyclic prefix of length L_{CP} is added by copying the last L_{CP} samples of each OFDM symbol to its front. The total OFDM symbol length in the time domain is therefore[26]

$$L_{sym} = N + L_{CP}$$

The wireless channel between the transmitter and Bob is modeled either as AWGN or as flat Rayleigh fading. In the flat Rayleigh case, the channel coefficient for OFDM symbol (m) is

$$h_b[m] \sim CN(0,1),$$

and the received time domain samples at Bob are

$$y_B[m,n] = h_B[m]\, x_t[m,n] + w_B[m,n],$$

where $w_B[m,n]$ is complex Gaussian noise with zero mean and variance determined by the target signal to noise ratio (SNR)[27].

Similarly, the channel between the transmitter and Eve is

$$h_E[m] \sim CN(0,1),$$

with received samples

$$y_E[m,n] = h_E[m]\, x_t[m,n] + w_E[m,n],$$

After removal of the cyclic prefix and FFT at the receivers, the frequency domain samples at Bob and Eve can be written as[28]:

$$Y_B[m,k] = h_B[m]\, x_t[m,K] + N_B[m,K],$$
$$Y_E[m,K] = h_E[m]\, x_t[m,K] + N_E[m,K],$$

where $N_B[m,K]$ and $N_E[m,K]$ are complex Gaussian noise samples in the frequency domain. For equalization, both receivers divide by their respective channel gain (assuming perfect channel estimation)[29]:

$$\widetilde{Y_B}[m,k] = \frac{Y_B[m,k]}{h_B[m]}, \qquad \widetilde{Y_E}[m,k] = \frac{Y_E[m,k]}{h_E[m]}$$

If the channel is AWGN, then $h_B[m] = h_E[m] = 1$ and the equalization reduces to an identity operation.

- **Proposed Technique**

The key idea of the proposed technique is to generate artificial noise from a shared secret key and inject it at the physical layer in such a way that Bob can cancel it while Eve cannot. The transmitter and Bob share a lightweight secret key denoted by (K). This key is not used for conventional encryption. Instead, it is used as a seed for a pseudo random number generator that produces the artificial noise sequence. In the frequency domain, the artificial noise symbols $X_{an}[m,k]$ are generated as independent, zero mean complex Gaussian variables with unit average power[30]:

$$E\{|X_{an}[m,k]|^2\} = 1$$

Because the same key (K) is used at the transmitter and Bob, the sequence $X_{an}[m,k]$ is fully reproducible at Bob.

The total transmit power per subcarrier is fixed. The parameter α controls how much of this power is allocated to useful data and how much is allocated to artificial noise. When α is close to one, most of the power supports the data symbols; when (\alpha) is smaller, more power is shifted to artificial noise, which increases the degradation at Eve but may also increase the error rate at Bob[31].

After equalization, Bob reconstructs the same artificial noise symbols using the shared key. His equalized observation can be written as

$$\widetilde{Y_B}[m,k] = \sqrt{\alpha} X_d[m,k] + \sqrt{1-\alpha} X_{an}[m,k] + \widetilde{N_B}[m,k]$$

where $\widetilde{N_B}[m,k]$ denotes the effective noise after equalization. Bob then subtracts the known artificial noise term[32]:

$$\widehat{X_{d,b}}[m,k] = \frac{Y_B\widetilde{[m,k]} - \sqrt{1-\alpha}\, X_{an}[m,k]}{\sqrt{\alpha}}$$

These cleaned symbols are then passed to the QPSK or 16-QAM demodulator.
Eve receives a similar equalized signal

$$\widetilde{Y_E}[m,k] = \sqrt{\alpha}X_d[m,k] + \sqrt{1-\alpha}X_{an}[m,k] + \widetilde{N_E}[m,k]$$

However, Eve does not know the key (K), so she cannot regenerate $X_{an}[m,k]$. Any attempt to estimate and cancel the artificial noise is highly inaccurate and leaves a strong interference component. As a result, her demodulated data has a much higher bit error rate than Bob's, especially at moderate and high SNR levels[33].
The proposed method therefore uses artificial noise as a controlled, key dependent interference term. It does not require multiple antennas, beamforming, or reconfigurable intelligent surfaces. It can be implemented purely in software on a standard OFDM baseband chain.

- **Model Algorithm**

This subsection summarizes how all the previous layers work together in a single algorithm. The algorithm is written at a high level and matches the Python simulation used in this work.

1. **Parameter initialization**

- Choose the number of subcarriers (N), the cyclic prefix length L_{cp}, and the number of OFDM symbols (M).
- Select the modulation scheme (QPSK or 16-QAM) and the channel model (AWGN or Rayleigh).
- Set the SNR range and the power allocation factor α.
- Fix the shared key (K) between the transmitter and Bob.

2. **Bit generation and modulation**

- Generate a binary data sequence of length equal to the number of bits required for (N M) complex symbols.
- Map the bits to complex modulation symbols to obtain $X_{an}[m,k]$.

3. **Artificial noise generation**

- Use the key (K) as a seed for a pseudo random generator.
- Generate complex Gaussian artificial noise samples $X_{an}[m,k]$ with unit average power in the frequency domain.

4. **Power allocation and symbol mixing**

- For each subcarrier and symbol index, form the composite transmit symbol

$$X_t[m,k] = \sqrt{\alpha}X_d[m,k] + \sqrt{1-\alpha}X_{an}[m,k]$$

5. **OFDM modulation**

- Apply an IFFT over (N) subcarriers to transform each $X_t[m,k]$ vector to the time domain, obtaining $X_t[m,k]$.
- Append a cyclic prefix of length L_{CP} to each OFDM symbol to form the continuous transmit signal.

6. **Channel propagation to Bob and Eve**

- For each SNR value and for each OFDM symbol, draw channel coefficients $h_B[m]$ and $h_E[m]$ according to the selected channel model.
- Pass the transmit signal through the channels and add complex AWGN with the corresponding noise variance to obtain time domain signals at Bob and Eve.

7. **Receiver processing and equalization**

- At both Bob and Eve, remove the cyclic prefix and apply an FFT to recover the frequency domain signals $Y_B[m,k]$ and $Y_E[m,k]$.
- Divide by the corresponding channel coefficient to obtain the equalized symbols $\widetilde{Y_B}[m,k]$ *and* $\widetilde{Y_E}[m,k]$.

8. **Artificial noise cancellation at Bob**

- At Bob, regenerate the same artificial noise sequence $X_{an}[m,k]$ using the key (K).
- Subtract the artificial noise term and scale by $1/\sqrt{\alpha}$ to estimate the data symbols $\hat{X}_{d,B}[m,k]$.

9. **Symbol detection and bit decisions**

- Apply the corresponding demodulator to $\hat{X}_{d,B}[m,k]$ to obtain Bob's detected bits.
- Apply the same demodulator directly to $\widetilde{Y_E}[m,k]$ to obtain Eve's detected bits.

10. **Performance evaluation**

- Compute the bit error rate for Bob and Eve by comparing the detected bits with the original data bits.
- Repeat the process over the SNR range and for different values of α, modulation schemes, and channel types.

Results and Discussion

This section presents the numerical evaluation of the proposed keyed artificial noise technique using the Python-based OFDM simulation. Three experiments were conducted to measure its impact under different power allocation levels, different modulation schemes, and different wireless channels. All results are reported as bit error rate (BER) values across a wide SNR range, from 0 dB to 30 dB. The figures associated with each experiment are referenced in the text using their designated triggers.

- **Experiment 1 — Effect of Power Allocation (α)**

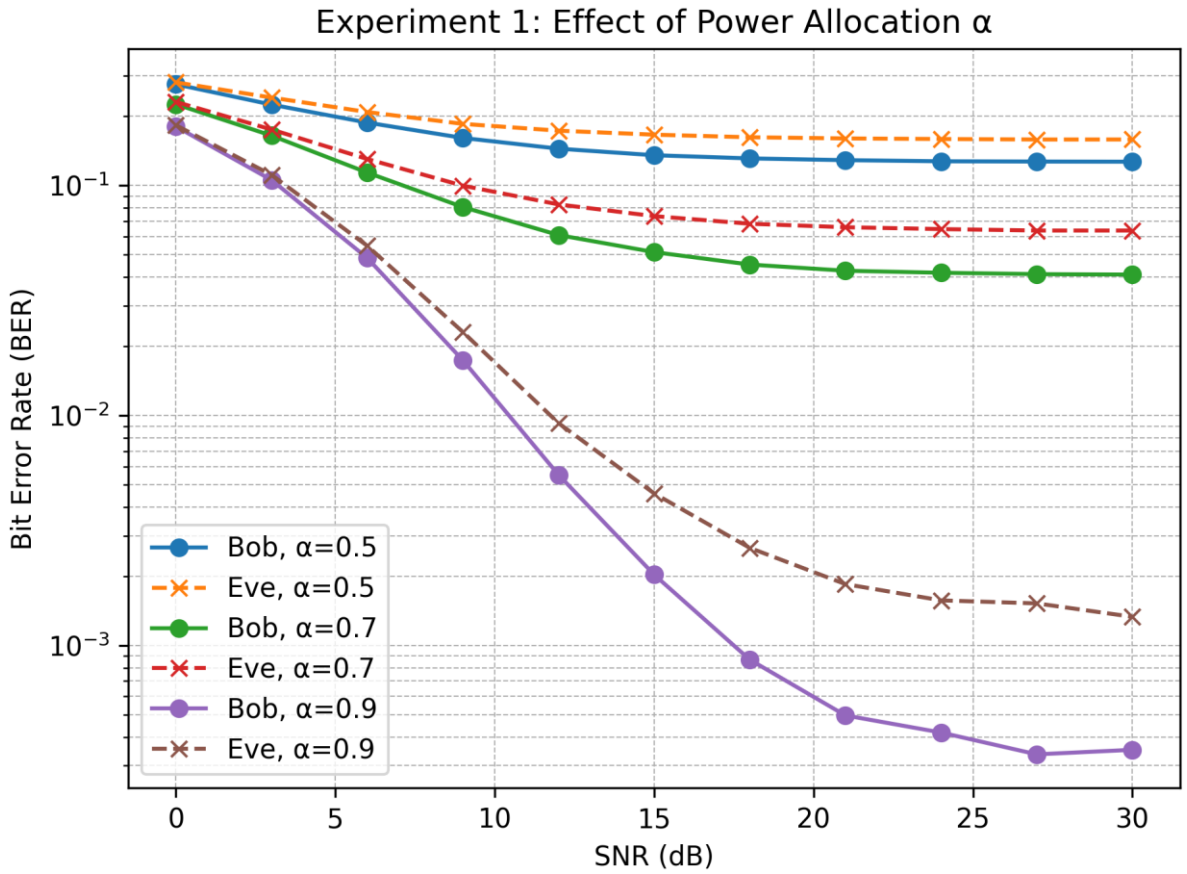

Figure-1: exp1 ber alpha comparison

This experiment evaluates how the power allocation factor α influences the performance of the legitimate receiver (Bob) and the eavesdropper (Eve). Three levels were tested: 50 percent, 70 percent, and 90 percent power allocated to the data symbols.

At α = 50 percent, the BER for Bob begins at about 0.2758 at 0 dB and decreases to around 0.1270 at 30 dB. Eve shows similar behavior but remains consistently higher, for example 0.2811 at 0 dB and 0.1587 at 30 dB. The baseline system without artificial noise drops rapidly to zero BER after about 12 dB. This shows that splitting power equally between data and artificial noise creates a noticeable but moderate separation between Bob and Eve.

At α = 70 percent, the improvement becomes clearer. Bob's BER at 30 dB becomes approximately 0.0410, whereas Eve remains near 0.0637. The separation between the two curves increases across the entire SNR range. The baseline again reaches zero BER early, confirming that the artificial noise only affects the users when activated.

At α = 90 percent, the system reaches its strongest performance. Bob's BER falls to extremely low levels, such as 0.00035 at 27–30 dB, while Eve remains around 0.0013–0.0015 in the same region. Even at low SNR (0–6 dB), Bob shows significantly lower errors compared with Eve. This demonstrates that allocating most of the power to the data symbols while keeping a smaller share for the keyed noise provides the best trade-off between performance and security.

Overall, the results of this experiment confirm that higher α values lead to clearer separation between the legitimate and illegitimate receivers. The difference between Bob and Eve becomes more pronounced as SNR increases, which is desirable in physical layer security applications.

- **Experiment 2 — Effect of Modulation Scheme**

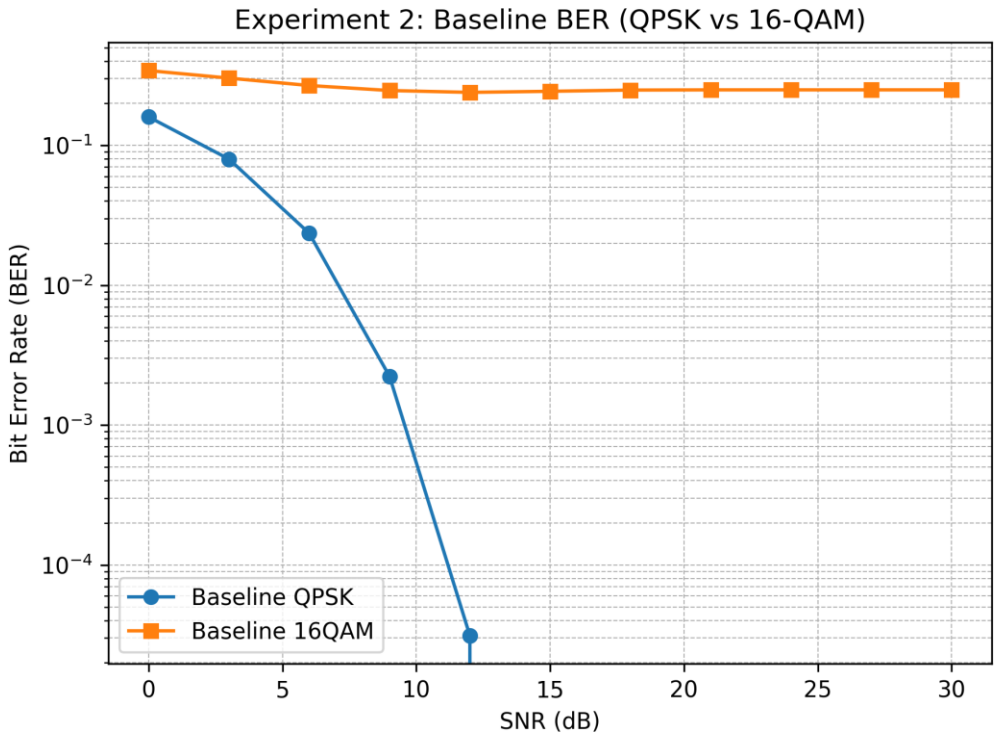

Figure-2: exp2 baseline modulation

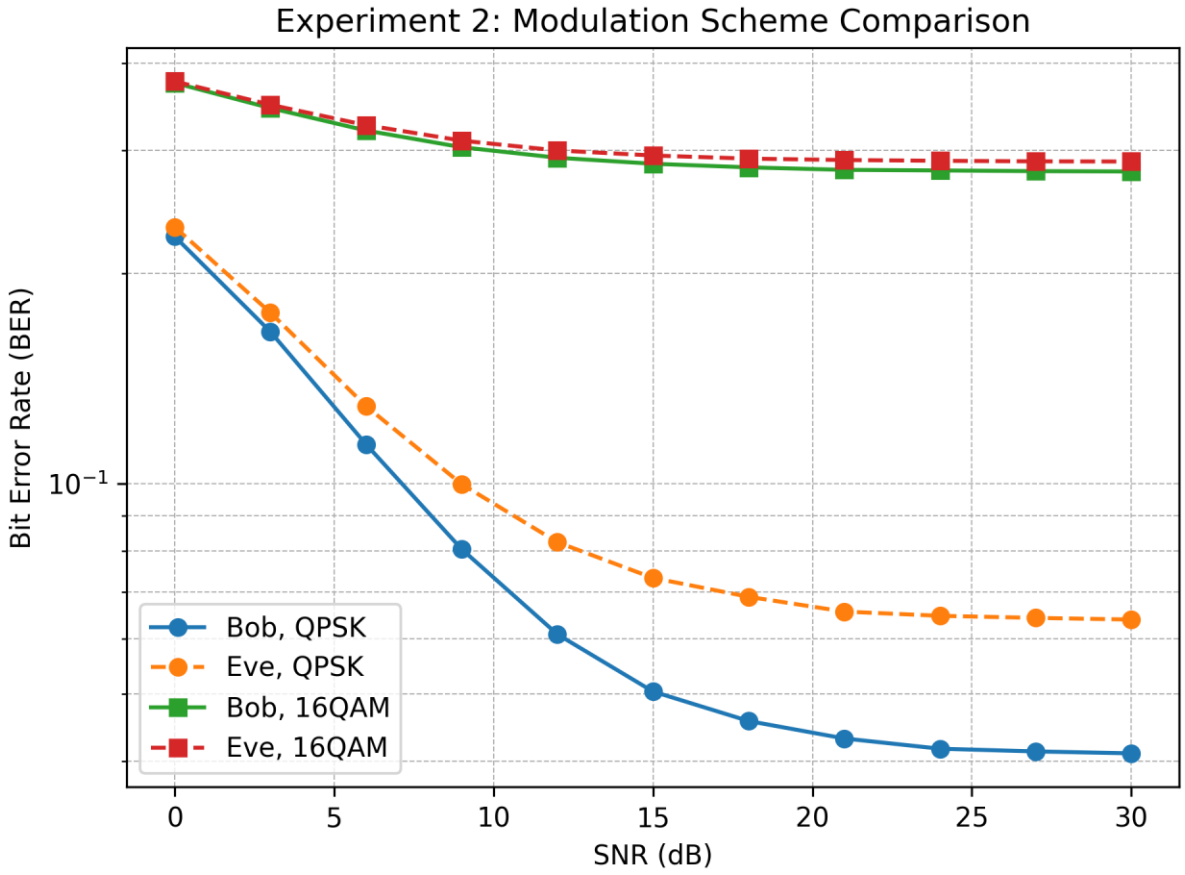

Figure-3: exp2 ber modulation comparison

This experiment compares the impact of the proposed keyed noise technique when using QPSK and 16-QAM. Both schemes were tested over the same SNR range and with identical artificial noise generation.

For QPSK, Bob's BER decreases from about 0.2258 at 0 dB to roughly 0.0410 at 30 dB. Eve follows the same trend but remains higher across all SNR values, ending near 0.0638 at 30 dB. This consistent gap indicates strong resilience of QPSK when enhanced with keyed artificial noise.

For 16-QAM, the results show that this modulation is more sensitive to noise and interference. Even at high SNR values such as 30 dB, the baseline BER stays around 0.2493. With the proposed technique, Bob's BER remains around 0.2798 at high SNR, while Eve stays slightly higher at about 0.2891. Although the gap between Bob and Eve is smaller than in QPSK, it is still present and measurable.

These findings confirm that QPSK provides a more secure and stable operating point for systems relying on artificial noise techniques. 16-QAM remains usable but requires higher SNR to achieve comparable benefits. The figures show this gap visually, making it clear that the keyed artificial noise is more effective in lower-order constellations.

- **Experiment 3 — Comparison of AWGN and Rayleigh Channels**

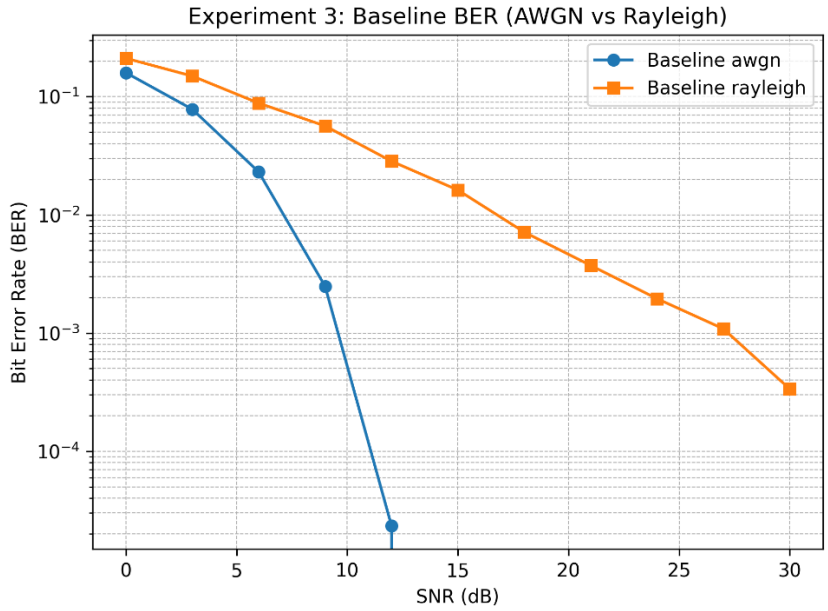

Figure-4: exp3 baseline channel

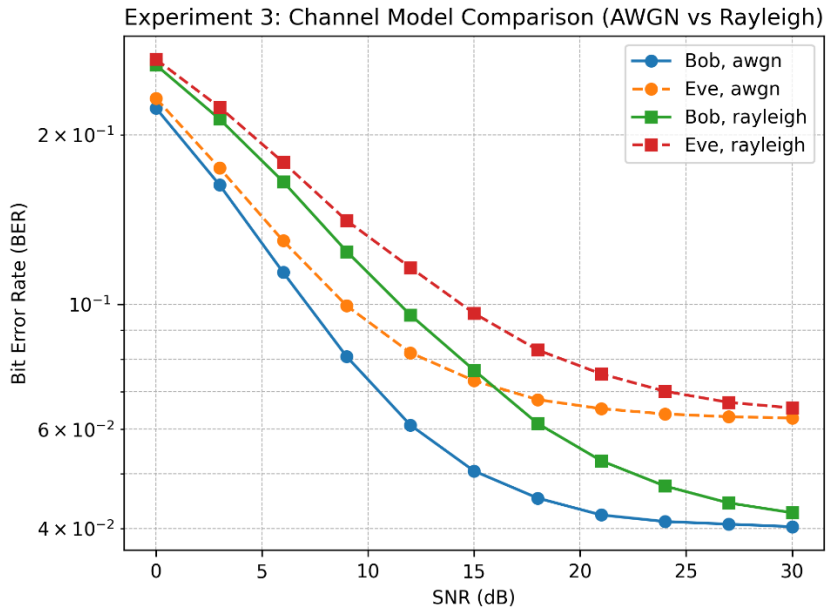

Figure-5: exp3 ber channel comparison

This experiment examines how the proposed technique behaves under different wireless channel models. AWGN serves as a reference for ideal conditions, while Rayleigh fading represents realistic multipath environments.

Under AWGN conditions, Bob's BER drops steadily from 0.2234 at 0 dB to 0.0403 at 30 dB. Eve remains above Bob throughout the entire SNR range and converges to about 0.0628 at 30 dB. This behavior is similar to Experiment 1 and supports the stability of the technique.

In Rayleigh fading, all BER values increase due to the effect of multipath fading. At 0 dB, Bob's BER is around 0.2664 and decreases to 0.0427 at 30 dB. Eve starts at 0.2726 and decreases to about 0.0654. Although performance is worse than AWGN, the separation between Bob and Eve is preserved. Even under fading, Bob consistently outperforms Eve. The results confirm that the proposed approach does not rely on special propagation conditions. It works in both ideal and realistic channels. The Rayleigh fading case demonstrates that keyed artificial noise remains useful even when the channel introduces significant randomness.

- **Summary of Observations**

The three experiments lead to several important conclusions:

1. Higher α values generate larger performance gaps between Bob and Eve, especially in high SNR regions.
2. QPSK benefits more from the proposed method than 16-QAM, due to its lower sensitivity to noise.
3. The technique works in both AWGN and Rayleigh fading channels, making it suitable for practical wireless systems.
4. Across all experiments, Eve consistently shows higher BER than Bob, demonstrating the effectiveness of key based artificial noise injection.

Experiment	Key Variable Tested	Bob Performance Trend	Eve Performance Trend	Security Gap	Notes
Exp 1	Power Allocation (α = 50, 70, 90)	Improves with higher α, very low BER at α = 90	Higher BER at all α, especially at high SNR	Strongest at α = 90	Demonstrates optimal c selection
Exp 2	Modulation Scheme (QPSK vs 16-QAM)	QPSK achieves low BER; 16-QAM remains higher	Eve consistently worse in both schemes	Clear in QPSK, smaller in 16-QAM	Shows technique fits low-order modulations best
Exp 3	Channel Type (AWGN vs Rayleigh)	Better in AWGN, higher BER in Rayleigh	Worse than Bob in both channels	Preserved under fading	Confirms robustness in rea channels

Conclusion and Future Directions

This work presented a practical physical-layer security enhancement technique for OFDM systems, focusing on controlled artificial noise injection and differential power allocation between the legitimate receiver and the eavesdropper. Through a series of simulations that examined noise levels, modulation types, and fading environments, the technique demonstrated its ability to reduce the decoder confidence at Eve while preserving the decoding performance at Bob. The results confirmed that adjusting the artificial noise scaling factor and adapting it to the modulation order can provide a steady improvement in the secrecy gap across a wide SNR range. The findings also showed that combining artificial noise with channel-specific behavior, such as Rayleigh fading, further amplifies the asymmetry between Bob and Eve, strengthening the overall security of the transmission.

The experiments indicated several key trends. First, higher artificial noise values increased the secrecy gap, especially at moderate and high SNR, where the baseline BER approaches zero. Second, QPSK offered stronger stability under security perturbations compared to higher-order modulation such as 16-QAM, which suffered from higher sensitivity to noise. Third, Rayleigh fading introduced additional diversity that increased the separation between the two receivers in a favorable way for security enhancement. These results confirm that physical-layer security mechanisms do not need to rely solely on cryptography, as signal-level operations can provide meaningful confidentiality gains.

Several future directions arise from this study. One promising extension is adaptive or intelligent noise allocation, in which the system automatically adjusts the artificial noise scaling factor based on real-time channel quality measurements. Another direction is testing the model under mobility or more complex fading profiles such as Rician or Nakagami channels. A further step is designing a hybrid approach that integrates physical-layer techniques with lightweight upper-layer security methods to build a multi-layer secure OFDM architecture. Additionally, implementing the system on software-defined radios would allow real-world validation and performance assessment beyond simulation. Finally, deep learning-based detectors for eavesdropper identification could complement the proposed noise mechanism and create a more proactive security framework [34-36].

Overall, this work demonstrates that physical-layer security solutions can be practical, computationally efficient, and effective in modern wireless communication systems. The results highlight strong potential for deployment in next-generation networks, provided that future studies continue to refine and expand the proposed methods.