

RESEARCH ARTICLE

Physical layer security using boundary technique for emerging wireless communication systems

Ismaeel Abiodun Sikiru¹  | Lukman Abiodun Olawoyin² | Nasir Faruk³ | Abdulkarim Ayopo Oloyede² | Abubakar Abdulkarim⁴ | Imam-Fulani Yusuf Olayinka² | Olugbenga Akinkunmi Sowande² | Salisu Garba⁵ | Agbotiname Lucky Imoize⁶ 

¹Department of Information and Communication Science, University of Ilorin, Ilorin, Nigeria

²Department of Telecommunication Science, University of Ilorin, Ilorin, Nigeria

³Department of Physics, Sule Lamido University, Kafin Hausa, Nigeria

⁴Department of Electrical Engineering, Ahmadu Bello University, Zaria, Nigeria

⁵Department of Computer Science, Sule Lamido University, Kafin Hausa, Nigeria

⁶Department of Electrical and Electronics Engineering, University of Lagos, Lagos, Nigeria

Correspondence

Ismaeel Abiodun Sikiru, Department of Information and Communication Science, University of Ilorin, Nigeria.

Email: ismaeel.as@unilorin.edu.ng

Abstract

The broadcast nature of radio propagation in wireless communication has been suspected as the loopholes of passive or active attacks by unauthorized users (eavesdroppers). The physical layer security techniques operate at the lowest stack of OSI layer against conventional cryptographic approaches, operating at the upper layer. However, techniques such as channel coding, power (directional antenna and artificial noise), and spread spectrum have been (and continuously) deployed to safeguard against sophisticated attacks. Most of these deployments are theoretical, and a few are enhanced for efficient security against an intruder. In this article, a boundary technique approach is proposed and applied to the physical layer to improve its secrecy-capacity and subdue adversary effects at the legitimate receiver. Hybrid performance metrics were adopted, and a Monte Carlo simulation was performed. The result obtained using secrecy outage probability, secrecy-capacity, and intercept-probability show that our proposed techniques enhance the secret transmission between the main transmitter and legitimate receiver. The simulation results were compared with the analytical methods. It was found that the channel between the transmitter and the main receiver has a better signal-to-noise ratio than the corresponding eavesdropper's channel. Conclusively, performance of the proposed technique is validated for applications in emerging wireless communication systems.

KEYWORDS

boundary technique, MISOME, physical layer, physical layer security, security enhancement techniques, wireless communication systems, wireless security systems

Abbreviations: 5G, Fifth generation; AN, Artificial noise; ARQ, Automatic repeat request; BAN, Body area network; BER, Bit error rate; BF, Beamforming; BWS, Body-worn sensors; CSI, Channel state information; CSR, Compromised secrecy region; D2D, Device-to-device; DF, Decode and forward; DSSS, Direct sequence spread spectrum; eMBB, Enhanced Mobile Broadband; FDR, Full-Duplex relays; FHSS, Frequency hopping spread spectrum; HDR, Half-Duplex relays; IEEE, Institute of electrical and electronics engineers; IoT, Internet of things; ISO, International organization of standardization; JRJS, Joint relay and Jammer selection; MER, Main-to-eavesdropper ratio; MIMO, Multiple input multiple output; MISOME, Multi-input, single-output, multi-eavesdropper; mMTC, Massive machine type communication; NOMA, Non-orthogonal multiple access; OFDM, Orthogonal frequency division multiplexing; OMA, Orthogonal multiple access; OSI, Open system interconnection; PLS, Physical layer security; PHY, Physical; PPP, Poison point processes; RF, Radio frequency; SNR, Signal-to-noise ratio; SOP, Secure outage probability; TSSRS, Two-stage secure relay selection; VANET, Vehicular ad hoc networks; UAV, Unmanned aerial vehicle; URLLC, Ultra-reliable low latency communication; WCS, Wireless communication system; WLAN, Wireless local area networks; WPAN, Wireless personal area networks.

1 | INTRODUCTION

Wireless communication is one of the most vibrant fields of research interest in the communication niche. The rise in the deployment of wireless communication systems (WCSs) has been attributed to its support for mobility and simplicity of deployment over a large distance compared to wired systems.¹ The wiring of all paths poses an additional cost for cabling plan changes.² The rapid advancement in the design of WCS orchestrates the emergence of WLANs (wireless local area networks), WPANs (wireless personal area networks), vehicular networks, and more. Wireless technology has been deployed in smart grid systems for data collection, demand management, and protection of power systems, among others. Therefore, the physical human presence in the communication arena is gradually reduced due to the deployment of communication systems that support remote management and interactive functions. However, all these remote functionalities have severe consequences to human safety, especially from malicious intrusion and confidentiality challenges.³ The open nature of the wireless communication channels has made them more accessible to various attacks and security issues despite the benefits posed to human lives.¹ For instance, hackers can now successfully infringe on the privacy of cellphone users and track users unguardedly, passively or actively. The current literature traces these challenges to two fundamental aspects—fading and interference.⁴ Several researchers have recently taken up the challenges to proffer security measures to these issues, welcoming diverse approaches such as cryptographic and physical layer security (PLS).

It is pretty understood that, despite the challenges attributed to the cryptographic approach, including a substantial computational burden, it is only effective at the upper layers of the OSI model.⁵ Cryptography was the initial principle to ensure confidentiality through safeguarding the communication system between the source, t and the legitimate destination, r against the eavesdropper, e . Notably, the fundamental attacker model is the essential attribute found in all cryptographic algorithms. Therefore, the transmitter enhances the message confidentiality by enciphering, which can only be deciphered by the legitimate receiver using the same shared or different key unknown to the eavesdropper. Toward this end, the need to safeguard the information exchange in wireless communication by exploring the features and properties of the physical (PHY) layer becomes imperative. Such features include frequency selection, carrier frequency generation, signal processing, signal detection and several modulations techniques. This reason corroborates the view of Lu⁶ in respect of PLS as the only alternative way out of the cryptographic approach's computational burden. Thus, this deployment makes PLS, at present, gain momentum as a security enhancement of the transmitted information without the requirement of cryptographic protocols.⁷

In an explicit term, Figure 1 depicts the wireless communication process between a transmitter and a receiver amidst an eavesdropper. An eavesdropper can hear a broadcast message transmitted via a wireless medium from a source node to the destination. Consequently, the eavesdroppers could extract the secret key of the transmitted message, leading to a compromise due to lack of confidentiality. In order to address this security vulnerability issue, PLS has been proposed to deploy secure transmission of sensitive user data from source to destination. In PLS, the *secrecy capacity* measures the difference between the main and the wiretap link capacities.^{8,9} In practice, perfect secrecy is desirable, and it can be achieved when the secrecy capacity is positive from the source to the destination. Shannon coding theorem is used to explain the idea of positive secrecy capacity. A receiver can only obtain the unique signal of the source provided the channel strength (from source to destination) is relatively larger than the data rate.

PLS can evolve under different deployed enhancement techniques. Illustratively, in the study,¹⁰ the security techniques were taxonomized based on the two major types of attacks. However, all security techniques for the PHY layer ruminate within the three fundamental aspects—frequency, spatial, and time domains. In order to have a secure PHY layer, direct sequence spread spectrum (DSSS), directional antenna, and frequency hopping spread spectrum (FHSS), have been proposed and deployed as anti-jamming active attacks.^{5,11} Active interference attacks have been guarded against via directional antenna, beamforming (BF), channel coding, and DSSS techniques. Despite a passive attack, eavesdropping has also been confronted by deploying BF, random antenna, random parameter, artificial noise (AN), and FHSS. It is interesting to note that the FHSS effectively against passive traffic analysis attacks. However, most of the deployed security techniques are theoretical against their practical application at the PHY layer,¹⁰ which is insufficient for the existing works in this niche.¹²

As a result, earlier works on PLS of wireless communication focusing on the security techniques enhancement are majorly in two perspectives—to study or propose security techniques. At the same time, very few are deployed on the security techniques enhancement, despite its importance, to mitigate against evolving attacks. Even the few works in the enhancement techniques are yet to maximally consider the angular location of the legitimate receiver to the

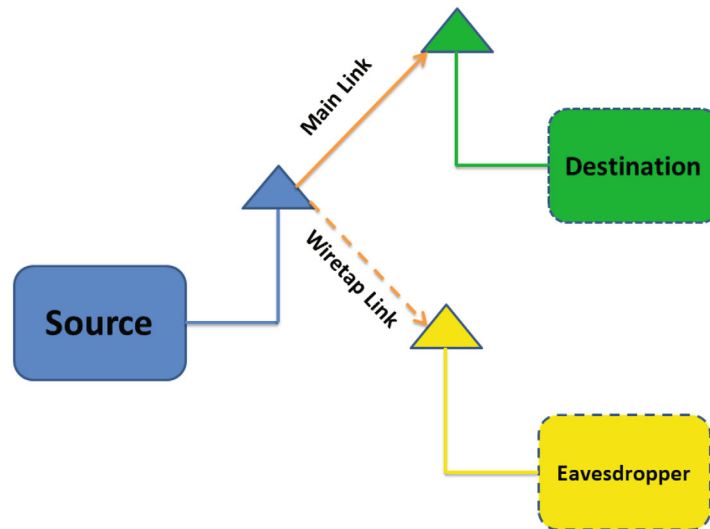


FIGURE 1 A WCS amidst an eavesdropper

legitimate transmitter and illegitimate party. This angular inconsideration, therefore, serves as the main motivation of this paper. The literature has revealed that the adversaries do “better” when the security measures silence the angular operation.¹³

The rest of the article is organized as follows: Section 2 presents the review of related literature; in Section 3, the methodology employed was provided. Section 4 presents the results, discussions, and contribution, and finally, Section 5 concludes the article.

2 | RELATED WORKS

Khan and Riaz¹⁰ conducted a comprehensive literature review to compare different PLS techniques in WCSs in the existing literature. The authors categorized the security techniques to combat the attacks in the PHY layer into time, spatial, and frequency domains. The work found that wide storage space, huge computing capability, and super hardware architectures are required to subdue the security challenges at the PHY layer. Additionally, it was observed that most of the current security techniques are theoretical and devoid of applicability to secure the PHY layer in WCSs. Vaezi et al.¹⁴ presented a survey on PLS in 5G wireless communications. The study covers PLS coding, mmWave communications, massive MIMO, heterogeneous networks, non-orthogonal multiple access (NOMA), and full-duplex mode. The findings from the survey revealed the robustness of PLS to any advanced passive and active eavesdropper. The flexibility of applying PLS for secret key generation in 5G technologies was highlighted. However, practical deployment and implementation of PLS were unprovided.

In another related work, Güvenkaya et al.¹⁵ presented a survey on the categorizations and applications of PLS techniques in message confidentiality. The survey presented a new framework for classifying PLS in an easy-to-understand format. Additionally, the work highlighted the new application scenarios of PLS techniques. However, the work did not cover practical deployment and experimentation.

Another related survey was reported by Wang and Xia¹⁶ recently. The work involves optimization approaches and signal processing techniques for wireless PLS. The optimization problems were categorized into the maximization of the secrecy rate, degradation of secrecy outage probability; relative consumption of power; and secure optimization of efficient energy. In addition, the authors discussed numerical optimizations toward addressing different security design issues in emerging wireless systems. Generally, key findings indicate that transmitters should be aware of the channel state information (CSI) of the eavesdropper for optimal performance of the proposed systems.¹⁷ However, in practice, these requirements are difficult to satisfy.

Zou et al.¹⁸ investigated diversity techniques to improve PLS against the conventional techniques (AN and BF). The choice of diversity techniques prevented higher additional power consumption and implementation complexity

characterized by AN and BF techniques. The study suggested cooperative relays for the enhanced and secure transmission of the signal from the transmitting point to the receiving end. Generally, the results revealed a direct relationship between the number of relays and the secrecy capacity. Also, the same relationship holds for the intercept probability of cooperative relay transmission and the number of relays. Overall, the results show that the importance of cooperative diversity in PLS to mitigate eavesdropping attacks cannot be overemphasized.

A comparative study¹⁹ presents specific approaches to enhance PLS in emerging WCSs. Codified channel capacity and computational complexity were introduced to examine PLS methods as performance metrics. The secret channel capacity is viable for measuring the confidentiality and availability of transmitted data. Results indicate that the computational complexity of the projected scheme can resist brute force attacks. Anti-jamming and error correction codes could be harnessed for data integrity preservation.

The work reported in Li²⁰ examined three mechanisms for PLS enhancement and employed an orthogonal frequency division multiplexing (OFDM) system to enhance the PLS. Additionally, the work proposed a security approach to reduce to the barest minimum the compromised secrecy region (CSR) in cooperative jamming without CSI. However, only one jammer was projected, making it impractical in an experimental setting. Zhang et al.²¹ examined cooperative wireless networks with jamming-dependent secure communications in another study. Two distributive auction-based power allocation schemes were projected. The friendly jammer was considered the auctioneer, while the sources were regarded as the bidders. The secrecy rate of the legitimate link was greatly improved by leveraging the friendly jammer. However, one of the projected auction-based power allocation schemes has weak resistance to attacks.

The work in²² uses the chaotic DSSS technique to enhance PLS. In the conventional scheme, it is still possible for intruders to recover chaotic sequences using blind estimation. However, the proposed technique provides adequate security for the DSSS system against detecting symbol periods from the eavesdropper. In Hu et al.,²³ a jammer was employed to combat multi-passive and scattered adversaries for secure downlink transmission from a control node to an Internet of Things (IoT) actuator. The idea of cooperative jamming was unleashed for secure transmission to enhance PLS. The design improves security (SOP) and power efficiency more than the conventional approach without cooperative jamming.

In Lee,²⁴ the idea of secure communications in three-hop wireless relaying systems was proposed. The work adopted full-duplex relays (FDRs) to enhance wireless PLS. Results show that the projected FDRs enhanced the secrecy rate more than the conventional half-duplex relays (HDRs). However, the cost of designing and implementing such relays remains a major point of concern. Also, Wang et al.²⁵ utilized mobile relaying to facilitate the secrecy capacity rate of a WCS. Transmit optimisation was employed for four nodes—source, destination, buffer-aided mobile relay, and eavesdropper channel setup. Cost and resource-efficient algorithms were developed, resulting in computationally efficient implementation. Wholesomely, the mobile relaying scheme shows remarkable improvements in the deployed processes of secrecy enhancement, unlike the immobile relaying scheme.

In a similar vein, the work²⁶ investigates the PLS of a cooperative relay network, whereby dual transmitters and receivers initiate communication amidst multi-adversaries, using a DF. The TSSRS-enhanced-NOMA system was designed to achieve the maximum secrecy capacity of single transmission-receiving pair. The design is able to deploy uncompromised synergized systems. Interestingly, the evaluation report of TSSRS-NOMA secrecy performance outperformed TSSRS-OMA in the low and medium regimes of the transmit power of the source and relay. In an extended application to cellular and satellite users,²⁷ proposed a joint BF optimization design for a NOMA-based satellite-terrestrial integrated network. In work, the produced-based BF scheme was able to obtain weight vectors and power coefficients with fast convergence. Progressively, Zhi et al.²⁸ explored reconfigurable intelligent surface (RIS) while applying joint BF design and optimization for RIS-aided hybrid satellite-terrestrial relay networks to minimize the total transmit power of the satellite and Base Station, and boost the received signal power without compromising the rate requirements of multiple blocked users.

In Wang et al.,²⁹ joint relays and jammer selection was employed as an enhancement technique for PLS. By employing two relaying strategies, numerical results projected the JRJS favorably compared to the TBRs scheme. Also, the JRJS shows more sensitivity to feedback delays. It was observed that the first-hop feedback delay guards against secrecy throughput loss, unlike the second hop. In contrast, while focusing on receiver performance with PLS in a Poisson field of interferers,¹³ results show that the receiver hidden at the given angle at high rates poses great benefits to the transmitted codewords. However, at low transmission rates, the reverse is the case. Although average secrecy capacity is advanced when the receiver is positioned at the angle where the CSI is known. Generally, results indicate that the boundaries technique enhances secrecy capacity for high data rates. Table 1 comprehensively summarizes the enhanced techniques for PLS and their application domain.

TABLE 1 Contributions and limitations of related works

Article	Application Domain	Contribution	Scope	Weakness
12,40,41	IoT	IoT-suitable PLS to replace cryptographic protocols	Review of the state-of-the-art in PLS for sensor networks	Unable to incorporate complex constraints in PLS
42	Mobile Communication.	A new authentication process (RF fingerprinting) was deployed to PLS to enhance future mobile communication systems	The application and merits of PLS in future mobile communication systems were discussed	PHY layer authentication could only be used for BS to UE authentication
43	Wireless networks (3G, 4G, & 5G)	PLS principles enabled scrambling-based technique is proposed to allow auto bootstrap and periodic network renewal.	Scrambling-based technique without initial authentication nor ARQ protocols.	Network bootstrapping challenges are still unresolved.
44		Flexible hierarchical security architecture for 5G-eMBB, MTC, and URLLC was proposed	PLS-assisted scheme based on the key streams and channel information in f-OFDM system	The cross-layer authentication is only appropriate to be performed on devices with limited computational ability under the mMTC scenario
13,45		Addressed current study of PLS applied approach on 5G technologies	Challenges for PLS research due to the evolution towards 5G wireless communications	Technical challenges such as polar code designs where eavesdropper's CSI is found at the source
46	Visible Light Communication (VLC)	PLS is deployed as VLC links as eavesdropping-proof in public areas or multiple-user scenarios	VLC links security enhancement	The study's scope was public areas or in multiple-user scenarios
47	Device-to-Device (D2D)	Stackelberg game is introduced to improve PLS for D2D communication	Iterative power allocation algorithm for cellular users and D2D pairs	The beamforming technique used is characterized by computational complexity
48	Body Area Network (BAN)	The game-theoretic framework was proposed to choose the best secure multi-hop route to the hub amidst wiretapping and attenuation effects. It also minimized SOP challenges. And it has better transmissions security of transmissions over star topology and IEEE 802.15.6	It only circumvents within the domain of wireless BANs	The framework cannot incorporate entire on-body WCSs among body-worn sensors (BWS), medical implant tools, and portable hubs
49	Vehicular ad-hoc Network (VANET)	The proposed design offers integrity and privacy for user information using a hash function and SHA-3, while PLS enhanced AES to secure key. The design was simple, scalable, and resourceful	They exploit the PLS to provide a better secure system for vehicular networks	The size of each broadcast message was limited to 1 KB per communication

TABLE 1 Contributions and limitations of related works

Article	Application Domain	Contribution	Scope	Weakness
50	Unmanned Aerial Vehicle (UAV)	PLS enhanced viewpoint was used to identify malicious UAV in future wireless networks in terms of eavesdropping and jamming attacks. Additionally, UAV-assisted terrestrial adversary detection, Malicious UAV detection, UAV spoofing, and UAV-aided wireless surveillance and intervention are suggested	PLS impact on the new security issues to future wireless networks in the deployment of UAVs	The technology is proposed for future wireless networks
45,51	5G NOMA	Investigated how PLS is applied to NOMA for random network security enhancement using a guard zone around the source node	PLS is applied to 5G NOMA by amplifying the guard zone or scaling down the client zone	The study did not give room for scalability in terms of protected and user zones

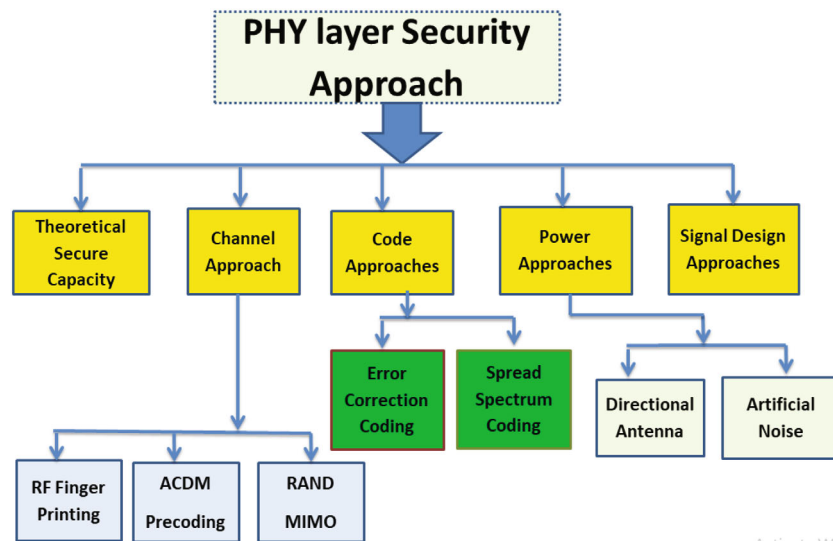


FIGURE 2 Categorized techniques of PLS enhancement

2.1 | Motivation of the study

The related works above show that several researchers have adopted and equally proposed different techniques to boost the secrecy capacity of the legitimate channel³⁰ at the PHY layer. These works have used different metrics to test their claims. Channel capacity and computational complexity have remained very common as the adopted metrics.¹⁹ Relatively diverse techniques implemented so far include signal processing techniques,¹⁶ diversity techniques,¹⁸ cooperative jamming,^{20,21,23,29} AN and BF,^{17,31,32} and boundary techniques.¹³ These enhancement techniques, among others, are summarized in Figure 2.

In the corroboratory approach of securing wireless communication at the PHY layer, angular location is now an essential consideration. We, therefore, deem it fit and timely important to subdue adversaries which find angular location a haven in relaying their effect. The author in Reference¹³ lightly pointed out that adversaries have found hiding at angular points “secure” while laying ambush on the legitimate parties. Unfortunately, with all the glorious efforts contributed so far in putting these attacks under control, the earlier researchers in this niche are yet to give the angular location of the legitimate receiver to the legitimate transmitter and the illegitimate party its needful attention toward ameliorating communication insecurity at the PHY layer. Hence, in this article, we focused on securing wireless communication at the PHY layer, from such angular location perspectives, as initiated in Equations (7) and (8).

3 | METHODOLOGY

3.1 | System model

The proposed boundary technique for PLS enhancement models a wireless network environment at the PHY layer, consisting of one transmitter T_x , one receiver R_x , an eavesdropper E , and multiple Interferers I . An angle θ , is in the angle $\angle T_x R_x E$, while angle ϕ , is formed in $\angle I R_x E$. The distance between the receiver point and eavesdropper is assigned as variable u . In the proposed model, the legitimate receiver has a single antenna, whereas the sender and eavesdropper have multiple antennas, described as the Multi-Input, Single-Output, Multi-Eavesdropper (MISOME) procedure.

Figure 3 gives the proposed boundary technique for PLS enhancement. Here, the transmit power is normalized to unity, and the performance is location-based. The receiver is considered at the varying locations of both the transmitter and eavesdropper. A typical wiretap channel model implemented includes MIMO wiretap channels, broadcast wiretap channels, and more.³³ In the MIMO channel with the transmitter, receiver, and eavesdropper having n_t , n_d , and n_e antennas, respectively, the received signals at the legitimate receiver, y_R , and eavesdropper, y_E , are defined in Equations (1) and (2):

$$y_R = H_R x_s + G_R, \quad (1)$$

$$y_E = H_E x_s + G_E. \quad (2)$$

Here, H_R defines the channel matrix of the legitimate receiver, H_E denotes the channel matrix to the eavesdropper, x_s represents the encrypted signal with the matrix constraint $E \{x_s x_s^H\} = P$, for $P_x \geq 0$ or an average power constraint $\overline{P_x} \geq P_{\max}$ for a peak power $P_{\max}$. G_R and G_E give the white Gaussian noise at the authorized receiver and eavesdropper, respectively. Assuming that one transmitter is supplied with n_t antennas in a broadcast wiretap channel, authorized users A , each equipped with n_{dt} antennas, and K eavesdroppers, each equipped with n_{ek} antennas, the broadcast channel follows Equations (3) and (4) defined in Reference 34

$$y_{R_a} = H_{R_a} x_s + G_{R_a}, \quad a = 1, 2, \dots, A \quad (3)$$

$$y_{E_k} = H_{E_k} x_s + G_{E_k}, \quad k = 1, 2, \dots, K \quad (4)$$

where x_s describes the encrypted signal tailored for the confidential message, with the matrix constraint $E \{x_s x_s^H\} = P$ for $P_x \geq 0$ or an average power constraint $\overline{P_x} \leq P_{\max}$ for a peak power $P_{\max}$, while y_E and y_E are the received signals at legitimate user a and eavesdropper k , respectively. H_E is $n_{Ea} \times n_t$ channel matrix to the user a , and H_{ek} is $n_{Ek} \times n_t$ channel matrix to eavesdropper k . G_R and G_E are the white Gaussian noise at the authorized receiver and eavesdropper, respectively. In an interference wiretap channel, the received signals of receiver R and the eavesdropper are given by Equations (5) and (6), respectively.

$$y_R = xR + \sum_{i=1}^n I_i w_i, \quad (5)$$

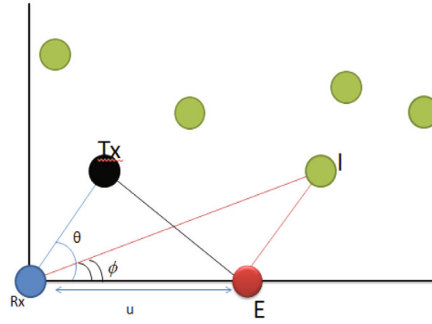


FIGURE 3 The proposed boundary technique for PLS enhancement

$$y_E = xE + \sum_{i=1}^n I_i w_i, \quad (6)$$

where y_R and y_E represent the signals received at the receiver and eavesdropper, respectively. x and w represent the information and noise signals from the transmitter and interferer. R denotes the legitimate receiver, I defines the interferer, and E is an eavesdropper. By applying boundary techniques, Equations (5) and (6) could be rewritten in terms of angles as given by Equations (7) and (8):

$$y_R = R(x + \sin \theta), \quad (7)$$

$$y_E = E(x + \cos \phi), \quad (8)$$

where $x \in \mathbb{C}^{n_t}$ is the information-bearing transmitted signals, θ is the receiver location angle between the transmitter and eavesdropper, and ϕ is the receiver location angle between the interferer and eavesdropper.

In order to strengthen the reach of signals to the legitimate receiver while also avoiding the attenuation, transmit power is induced. This further weakens the effect of signal reach to the eavesdropper. In this regard, the secrecy capacity in Figure 3 is enhanced as follows:

$$C_R = \log_2 \left(1 + \frac{P|h_R|^2}{\sigma_R^2} \right), \quad (9a)$$

$$C_E = \log_2 \left(1 + \frac{P|h_E|^2}{\sigma_E^2} \right), \quad (9b)$$

$$C_S = \log_2 \left(\frac{1 + \frac{P|h_R|^2}{\sigma_R^2}}{1 + \frac{P|h_E|^2}{\sigma_E^2}} \right). \quad (9c)$$

3.2 | Performance metrics

The performance of the proposed technique is done by evaluating the system secrecy performance through mathematical analysis of secrecy outage probability and nonzero secrecy capacity. The result obtained shows that secrecy communication can be enhanced in wireless communication using this proposed method.

3.3 | Secure outage probability (SOP)

Secure outage probability is key to addressing channel fading and imperfect CSI issues.³⁵ The SOP is a well-defined metric used to test when it becomes difficult to achieve secure transmission. The probability that a secrecy outage occurs defines

the SOP, and it describes when the instantaneous secrecy capacity, C_s , falls below the threshold secrecy rate, as defined in Equation (10).

$$P_{\text{out}} = P_r \left\{ \frac{1 + \gamma_R}{1 + \gamma} < \gamma_{\text{th}} \right\}, \quad (10)$$

where P_{out} is the SOP, P_r is the probability, γ_R depicts the SNR at the legitimate receiver, and γ_{th} is the threshold SNR.

We assumed that both channels are experiencing Nakagami- m fading channel but a different fading condition. The probability density function (PDF) of each channel is given by,^{31,32} respectively

$$f_{(\gamma_B)}(\gamma_B) = \frac{N}{\gamma_B} e^{-\left(\gamma_B/\bar{\gamma}_B\right)} \left[1 - \exp\left(-\frac{\gamma_B}{\bar{\gamma}_B}\right) \right]^{N-1} \quad (11)$$

$$f_{(\gamma_I)}(\gamma_I) = \frac{m_I^{N_I m_I} \gamma^{N_I m_I - 1} N}{\Gamma(N_I m_I) \bar{\gamma}_I^{m_I}} e^{-\left(m_I \gamma_I / \bar{\gamma}_I\right)} \left[1 - \frac{\Gamma(m_I, m_I \gamma_I / \bar{\gamma}_I)}{\Gamma(m_I)} \right]^{N-1} \quad (12)$$

The SOP of this system is evaluated so as to determine that the probability of the achievable secrecy rate is less than the predetermined secrecy rate. The outage secrecy probability is determined by using the expression given by.³⁶

$$\begin{aligned} P_{\text{out}}(R_S) &= P(C_S < R_S) \\ &= \sum_n P(R \cap \gamma_B) \\ &= P(C_S < R_S | \gamma_B) - (1 + P(C_S < R_S | \gamma_I, \gamma_{\text{BI}})) \end{aligned} \quad (13)$$

Equally, we have assumed that the channels are independent of each other but express the same fading condition. Such joint PDF can be expressed in Equation (14) as given by³⁷

$$P_{\text{out}}(R_S) = 1 - \int_0^\infty \int_z^\infty e^{-\gamma_{\text{BI}}} e^{-\gamma_{\text{EI}}} \delta \gamma_{\text{BI}} \delta \gamma_{\text{IE}}, \quad (14)$$

where $z = 2^{R_s} \left(\frac{\gamma_{\text{EI}} + \gamma_{\text{BI}}}{2\gamma_{\text{EI}} + \gamma_{\text{BI}}} \right) - \varpi$ and $\varpi = \sin^2 \beta + \cos^2 \beta$.

In order to determine the outage probability, Equations (11) and (12) are substituted into Equation (14), and the resulting mathematical expression derived was solved by using³⁵ equations. Then, the closed-form expression below is obtained:

$$\begin{aligned} P_{\text{out}}^{(F)} &\leq 1 - \exp^{-\rho E \Gamma R^2} \sum_{k=1}^K (-1)^{k+1} k C_K^k \\ &\int_0^\infty \frac{\frac{P_B}{d_{\text{BE}}^\alpha} (1 + \lambda_{\text{BB}}) + Kx \lambda_{\text{BB}}}{\left(\frac{P_B}{d_{\text{BE}}^\alpha} + Kx \lambda_{\text{BB}} \right)^2} \exp\left(\rho E R^2 \psi\left(\frac{x}{\theta - \phi}; \alpha; \frac{\delta \theta \delta \phi}{R^2} \right) - \frac{k d_{\text{BE}}^\alpha}{P^2 B} x \right) dx, \end{aligned} \quad (15)$$

where $\psi(z; \alpha; \delta) = \int_0^{2\pi} \int_0^1 \frac{z^{\alpha+1}}{z^\alpha + (z^2 + \delta^2 - 2z\delta \cos \theta)^{\phi/2}} \tan(\phi/\theta) dz d\theta$ and $\lambda_{\text{BB}} = E[|h_{\text{BB}}|^2]$ is the average gain of the channel.

3.4 | Secrecy capacity

The secrecy capacity is known to be the maximum transmission rate from the source to the specified receiver such that the sensitive user information is uncompromised. The average of the instantaneous secrecy capacity, C_s^+ , over the fading

coefficients h_{sd} and h_{se} , gives the ergodic secrecy capacity, where $C_s^+ = \max(C_s, 0)$ defined in Equation (16)

$$C_s = \begin{cases} 0, & C_R - C_E < 0, \\ 1, & C_R - C_E > 0. \end{cases} \quad (16)$$

The source transmission is only secure provided the secrecy capacity C_s is above zero to prevent the source signal from the eavesdropper's interception. If we define $x = |h_{sd}|^2$ and $y = |h_{se}|^2$, then the intercept probability of the direct transmission is given by Equation (17):

$$P_{\text{intercept}} = P_r(C_s < 0), \quad (17a)$$

$$P_{\text{intercept}} = P_r(|h_{sd}|^2 < |h_{se}|^2), \quad (17b)$$

$$\begin{aligned} C_s &= \int_0^{\gamma_B} (\log_2(1 + \gamma_B) - \log_2(1 + \gamma_E)) f(\gamma_B, \gamma_E) d\gamma_E \\ &= \log_2(1 + \gamma_B) \int_0^{\gamma_B} f(\gamma_B, \gamma_E) d\gamma_E - \int_0^{\gamma_B} \log_2(1 + \gamma_E) \frac{\partial f(\gamma_B, \gamma_E)}{\partial \gamma_B \partial \gamma_E} \\ &= \log_2(1 + \gamma_B) \int_0^{\gamma_B} f(\gamma_B, \gamma_E) d\gamma_E - \left[\log_2(1 + \gamma_E) \frac{\partial F}{\partial \gamma_B} \right]_0^{\gamma_B} \\ &\quad + \frac{1}{\log_2} \int_0^{\gamma_E} \frac{1}{1 + \gamma_E} \frac{\partial F}{\partial \gamma_E} d\gamma_E, \end{aligned} \quad (18)$$

$$\begin{aligned} C_s &= \frac{1}{\log_2} \int_0^\infty \int_\infty^{\gamma_B} \frac{1}{1 + \gamma_E} \frac{\partial F}{\partial \gamma_E} d\gamma_B d\gamma_E \\ &= \frac{1}{\log 2} \int_0^\infty \frac{1}{\gamma_E} [F(\gamma_B, \gamma_E)]_{\gamma_E}^\infty d\gamma_E \\ &= \frac{1}{\log 2} \int_0^\infty \frac{1}{1 + \gamma} F(\gamma_B, \gamma_E) - F(\gamma_E) d\gamma_E \\ &= \frac{1}{\log 2} \int_0^\infty E \left\{ \frac{e^{-\gamma I_{B,E}} - I_x(B, \gamma)}{1 + \gamma} \right\} d\gamma_E. \end{aligned} \quad (19)$$

Thus, Equation (19) is obtained by changing the order of integral $F(\infty, \gamma_e) = f_e(\gamma_e)$ as explained in Reference 38. Besides, C_R defines the capacity through the main link, and C_E denotes the capacity of the adversary link. The expression, $P_{\text{intercept}} = \frac{\sigma_{se}^2}{\sigma_{sd}^2 + \sigma_{se}^2}$ revealed that the random variables $|h_{sd}|^2$ and $|h_{se}|^2$ are independent, and exponentially distributed. Also, σ_{sd}^2 and σ_{se}^2 show the expected values of $|h_{sd}|^2$ and $|h_{se}|^2$, respectively. Following Equation (17), transmit power P is insignificant to the intercept probability of conventional direct transmission. Therefore, PLS is never improved with the increase of transmit power.

Now, let λ_{me} denote the ratio of the average main channel gain σ_{sd}^2 to the average channel gain σ_{se}^2 of the eavesdropper. The ratio implies that $\lambda_{me} = \sigma_{sd}^2 / \sigma_{se}^2$, and is known as the main-to-eavesdropper ratio (MER). Usually, the eavesdropper is passive, and the wiretap channel information is hard to get. That is why the best relay selection criterion of the boundary technique is better to deploy and is given as:

$$BR = \arg \max_{i \in \mathbb{R}} \frac{|h_{si}|^2 |h_{id}|^2}{|h_{si}|^2 + |h_{id}|^2}, \quad (20)$$

where R represents a set of N relays. And $|h_{si}|^2$ and $|h_{id}|^2$ denote fading coefficients of the channel from the transmitter to relay R_i , and then from relay R_i to destination, respectively.

The criterion for selecting the best relay is shown in Equation (20), which shows that the main channel information, $|h_{si}|^2$ and $|h_{id}|^2$ required for maximum channel capacity. In the configuration, the main and wiretap channels are designed to be independent of each other. The secrecy capacity of the best relay selection is described in Equation (16) as $C_s = C_R - C_E$, and the effect is depicted in Figure 8. The probability at which the secrecy capacity is < 0 gives the intercept probability of the best relay selection.

3.5 | Secure connectivity

Secure connectivity entails secure protection of the communication channel from the eavesdropper. In order to achieve secure connectivity, certain conditions must be satisfied, such as the determination of the tolerable acceptable error in the communication, referred to as bit error rate (BER). If the CSI of the main channel and that of the eavesdropper is not known to the source, then the rate of the transmitted codewords R_t , and that of the confidential messages R_s , likewise BER, need to be determined. In this study, Rayleigh fading is employed over the main channel and the eavesdropper channel to gain secure connectivity sc . Therefore, the probability of secure connectivity P_x^{sc} is given by Equation (21):

$$P_x^{sc}(u) = E \left\{ e^{-I_{x,r}} (1 - e^{-s_e I_{x,e}(u)}) \right\} = P_{x,r}^c - I_x(u), \quad (21)$$

where $I_x(u) = E \left\{ e^{-s_e I_{x,e}(u)} \right\}$ describes the joint connection probability of the receiver and the eavesdropper. Consequently, the proportionality of BER to SNR is as well depicted in Figure 10.

Here, θ is located at the angle to the transmitter to account for the correlation of interference and the fading states of the interfering channels at the receiver and the eavesdropper. Additionally, θ is placed over the locations of the interferers. By using the PGFL of the PPP and considering that the fading samples in the interfering channels at the receiver and the eavesdropper are i.i.d. unit-mean exponential RVs, Equation (15) is then expressed as follows:

$$\begin{aligned} I_x(u) &= \int_0^{\frac{\pi}{2}} \exp \left(-\lambda \int_{s_x} \left(1 - \frac{1}{1 + sg(r)} \frac{1}{1 + s_e g(d)} \right) dS \right) f_\theta d\theta, \\ I_x(u) &= \int_z \exp \left(-\lambda \int_{s_x} \left(1 - \frac{1}{1 + sg(r)} \frac{1}{1 + \sigma z^{-1} g(d)} \right) dS \right) f_z dz, \end{aligned} \quad (22)$$

where s_x gives the infinite plane when the receiver is out of the corner. At this instance, dS describes the integration element, and d shows the distance between the integration element and the eavesdropper. The letter z shows the distance-based pathloss over the eavesdropper channel. It is therefore important to mention that the placement of the receiver at the bulk does not affect the location distance, u . Hence, the probability for secure connectivity is given by Equation (23):

$$P_x^{sc}(u) \approx YE \left\{ Z^{-1} \right\} E \left\{ I_{x,e}(u) \right\} - \frac{Y^2}{2} E \left\{ Z^{-2} \right\} \text{Var} \left(\frac{I_{x,e}(u) + E \left\{ Z^{-1} \right\}^2 E \left\{ I_{x,e}(u) \right\}^2 + \dots}{\frac{4\rho x(u)}{g(d_0)} E \left\{ Z^{-1} \right\} \sqrt{\text{Var}(I_{x,r}) \text{Var}(I_{x,e}(u))}} \right). \quad (23)$$

3.6 | Simulation and performance evaluation

This section presents the validation of the proposed secrecy improvement technique. The simulation is carried out in MATLAB, using a two-dimensional plane. The transmitter, receiver, eavesdropper and interference are positioned at varying angles throughout the simulations. The simulated distance between the transmitter and receiver is maintained, d_o , and the distance between the receiver and eavesdropper is given by u . During the simulations, different values of angle are allotted to $\angle T_x R_x I$ and $\angle I R_x E$. Specifically, the transmit power is dispensed evenly between the transmitters. Finally, the Monte Carlo simulations were compared against analytical results.

4 | RESULTS, DISCUSSIONS, AND CONTRIBUTIONS

In this section, we compared the simulated results with the analytical results of the secrecy capacity of the main channel. It is observed that the analytical result justified Monte Carlo simulated result by the analysis shown in Figure 4. The communication network would be highly secure if the outage probability is less while the SNR is high. Our numerical analysis in Equation (10) also justified the results. For instance, at the outage probability value of 10^{-3} , the analytical result reveals 11 dB as the SNR, which is far lesser than the 19 dB SNR given by the simulation result. The results show that the complementary value propagates in the SNR value against the outage probability value.

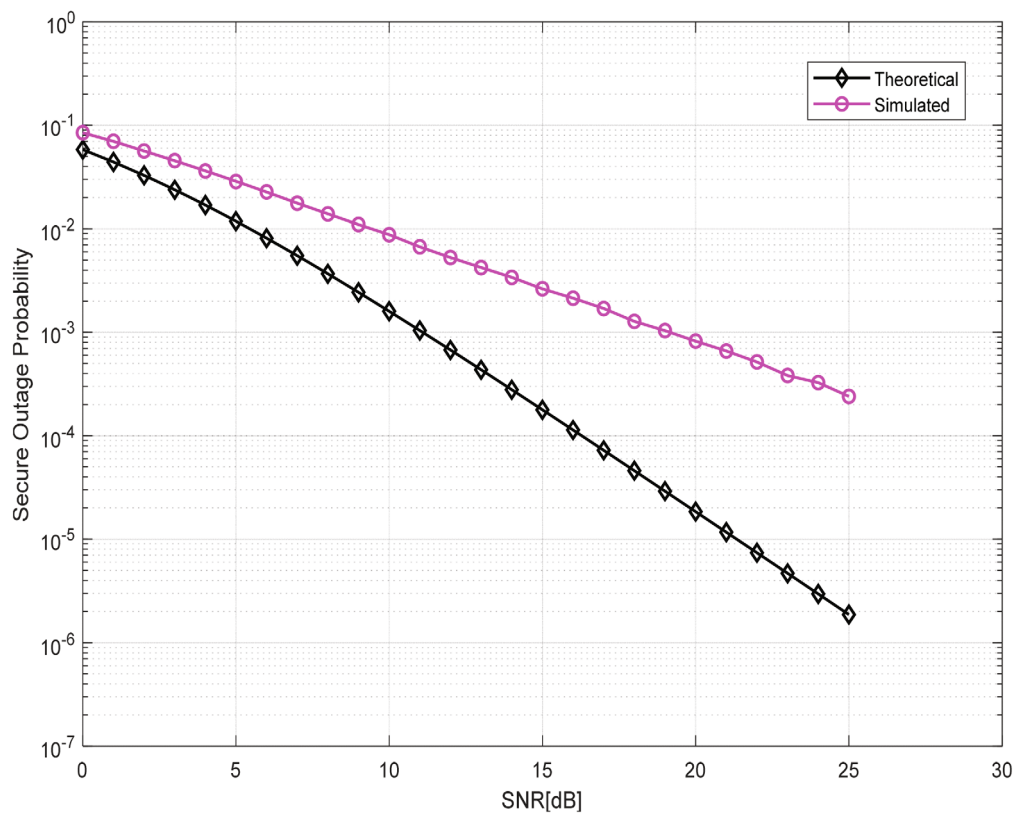


FIGURE 4 Comparison of simulated and analytical results

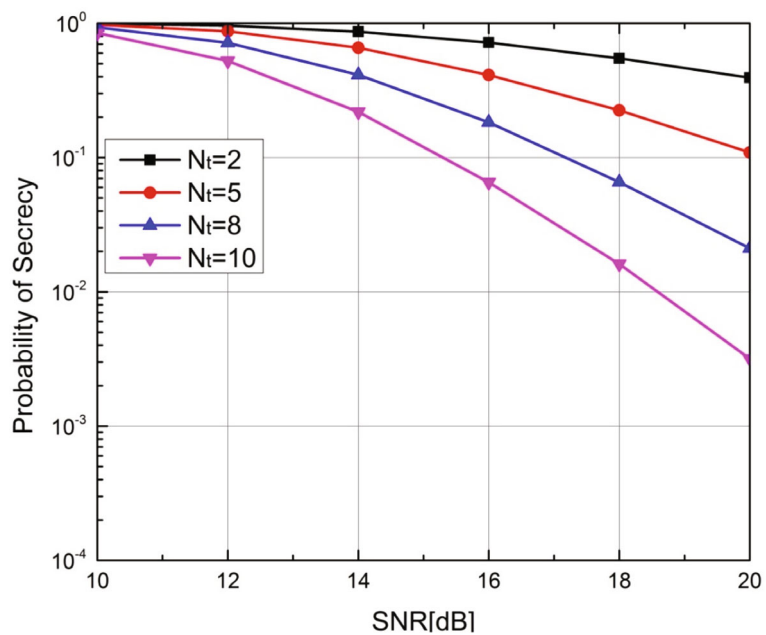


FIGURE 5 Plots showing the probability of secrecy against SNR

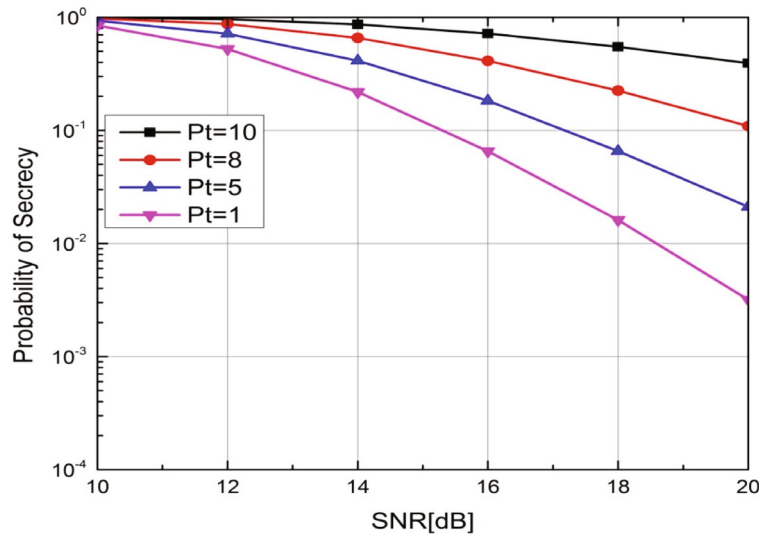


FIGURE 6 A graph of the probability of secrecy against SNR in power transmit deployment.

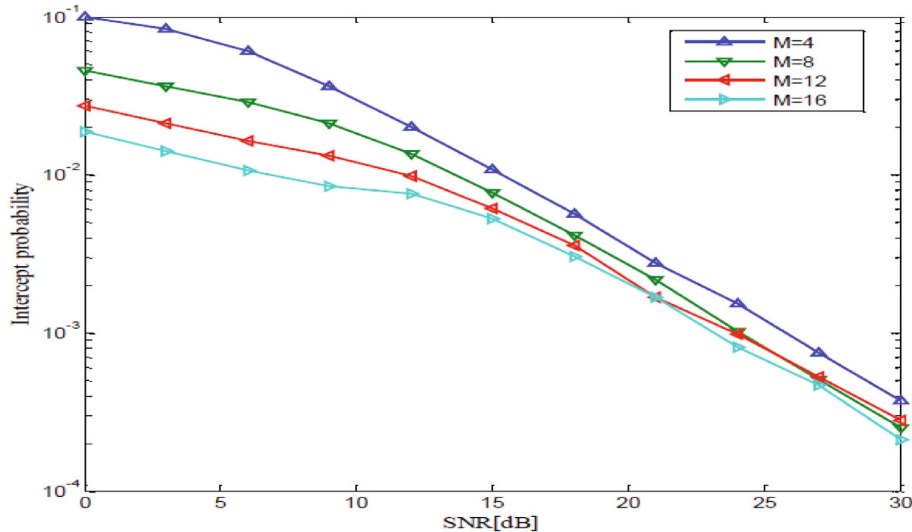


FIGURE 7 Simulation result showing intercept probability against main channel average SNR for various number of Interferers

Figure 5 shows the high efficiency of secrecy capacity at a lesser transmit noise (N_t). This technique is better than the Artificial Noise technique, which broadcasts noise to engage eavesdroppers against the interpretation of the primary signal intended for the legitimate receiver. Although the AN technique also achieves high secrecy capacity, it brings to the communication network vast consumption of power. The boundary technique shown in Figure 5 assures better secrecy capacity without noise. It is observed here that the result with a higher transmit noise value of 10 dB has the most negligible probability of secrecy. Unlike Figure 5, Figure 6 shows that the higher the transmit power (P_t), the more significant the chance of secrecy. It is observed from Figure 6 that when the transmit power, $P_t = 10$, there is a high value of both the probability of secrecy and SNR compared to when $P_t = 1$.

While analyzing the probability of intercept against its effect on SNR, Figure 7 depicts that even at varying starting points of the intercept probability, they still have like effects on SNR. This fact is also well buttressed in Figure 10 using BER, showing that the interferer is proportional to the signal attenuation. Besides, Figure 11 shows the comparison of simulated and analytical approaches based on the effect of BER on SNR. Still, it is discovered that as the intercept probability persists, irrespective of the number of interferers, their impact on the signal is (closely) the same. That is why at the intercept probability of $10^{-2.9}$, both the communication network with 12 and 16 interferers have the same effect of

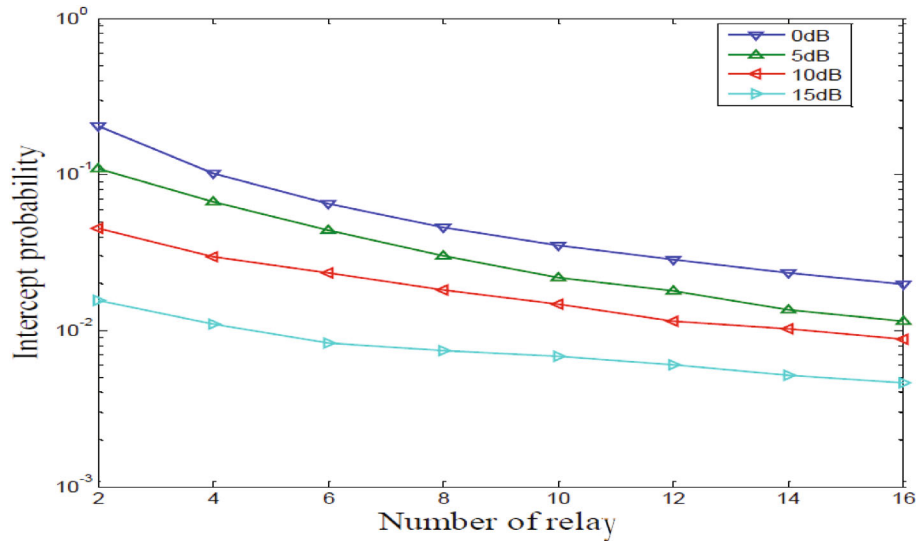


FIGURE 8 Simulation result showing the intercept probability in relation to the relay

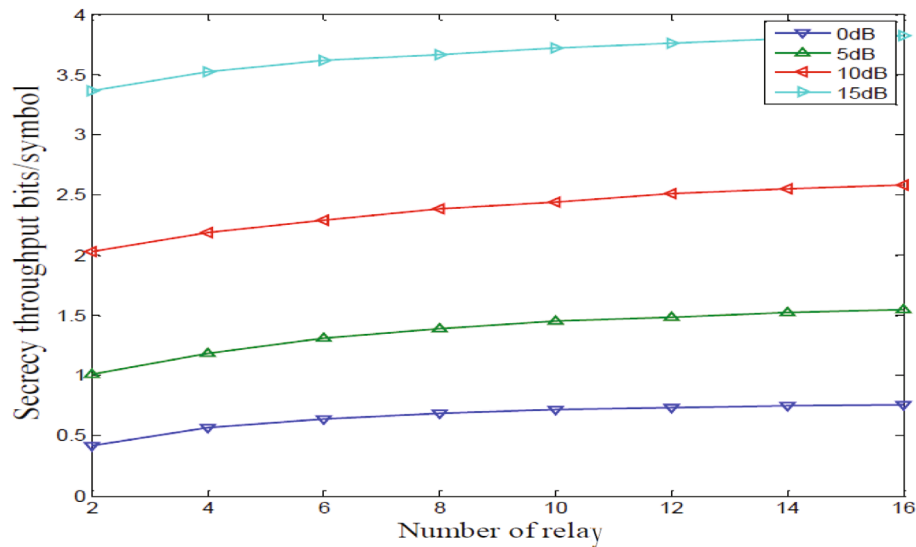


FIGURE 9 Secrecy capacity throughput of the main channel vs number of relays

21 dB on the signal reach at the receiver. The same scenario is recorded between eight and 12 interferers at 24 dB SNR. Even the wireless communication networks with 8, 12, and 16 experience the same signal effect of 28 dB at $10^{-3.3}$ intercept probability. From the analysis, it could be presumed that regardless of the difference in the number of interferers in the communication network, the intercept probability has an adverse effect on the SNR and has the same colluding effect on the system.

While examining the effect of a number of the relay on the intercept probability, it was discovered that as the number of relays deployed increases, there is a steady less signal power of intercept probability. The steady less signal power of intercept probability shows that the relay amplifies the signal reach to the legitimate receiver. This finding of ours, as depicted in Figure 8, is an improvement to the results of the work,³⁹ that the number of relays is proportional to both the secrecy capacity and intercept probability of cooperative relay transmission.

Figure 9 shows improved efficiency of capacity secrecy of the communication network between the legitimate transmitter and receiver, even amidst an eavesdropper. The improved efficiency of capacity secrecy of the communication network is because the eavesdropper has been degraded with the high power transmission of the transmitter coupled

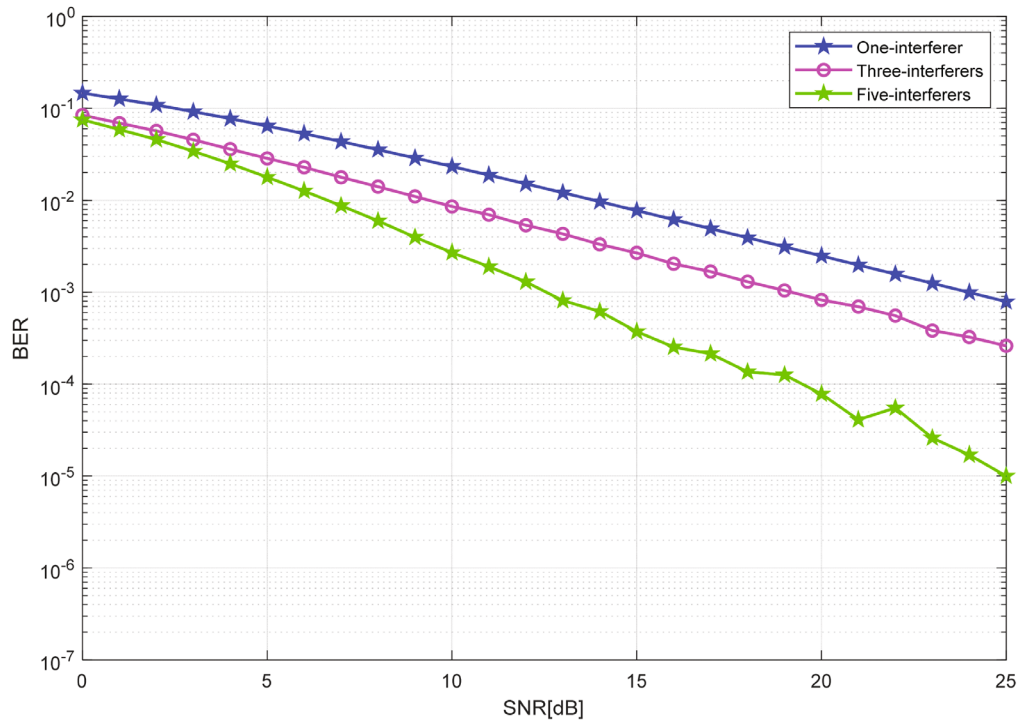


FIGURE 10 Effects of number of interferer on SNR

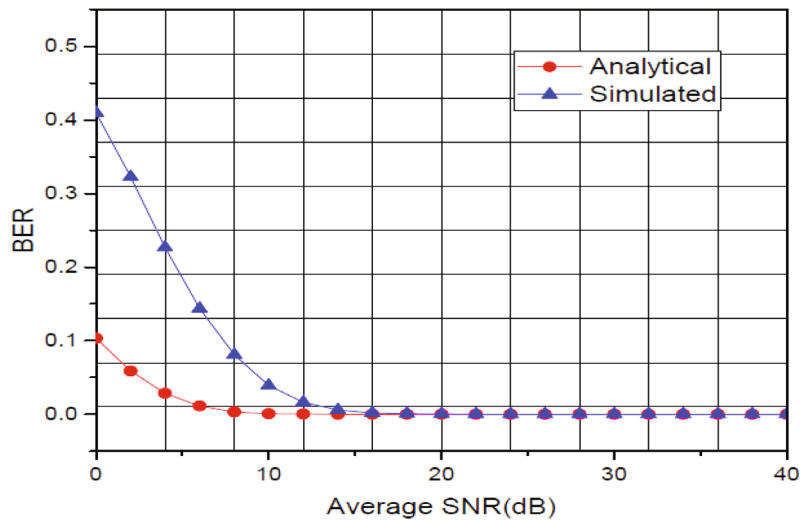


FIGURE 11 BER against average SNR

with the presence of the relay in the transmission. By analyzing the secrecy throughput bit/symbol from the range of 0–4, Figure 9 depicts that at 15 dB, the secrecy capacity is high compared to its secrecy capacity at 0 dB. Besides, secrecy capacity propagates as the number of relays advances. This trend confirms that the use of the boundary technique deployed has aided the secrecy capacity, secrecy connectivity and degraded eavesdropper effect. Again, the findings correspond with the results³⁹ that the number of relays is proportional to the secrecy capacity.

Figure 10 shows that as the bit error rate (BER) decreases, there is a steady increase in the signal-to-noise ratio (SNR). While analyzing the state of interferer on the system, it could be found, as depicted, that when the communication network is subjected to one and three interferers, respectively, both have no signal at their same starting point of BER. In contrast, as they propagate along the communication line, an interferer has a lesser effect (compared to three

interferers) on the secrecy capacity reach of the legitimate receiver. For example, at 10^{-2} value of BER, the effect of an interferer deploys SNR of 18 dB against 12 dB in the presence of three interferers. When the wireless communication network experiences an increase in the number of interferers to five, there is a drastic effect on the signal of the network, which earlier causes an attenuation effect. Figure 5 shows that at 10^{-3} BER, effects of one, three, and five interferers are 27, 17, and 10 dB, respectively. From the analysis, it could be affirmed that the number of interferers is inversely proportional to SNR. Therefore, it needs to be degraded to efficiently deploy secure wireless communication at the PHY layer.

In addition to the result explained in Figure 10, Figure 11 shows appreciable SNR achieved at the null value of BER for both the Monte Carlo simulated and analytical results. The result obtained in Figure 11, therefore, assures adequate secrecy capacity and secure connectivity but a degradable effect on the eavesdropper. It is noticeable that at higher BER, the communication network experiences its impact on the signal by having low SNR. For example, when BER stands at 0.5, the average SNR is 0 dB. A very low BER, ranging from 0.1 to 0, is recorded in the analytical result. This tallies with the comparison effect noticed in Figure 4.

5 | CONCLUSIONS

In this work, the use of boundary technique was employed to enhance the secure transmission in wireless systems at the physical layer. This approach was used based on its novelty against the deception characteristic of some eavesdroppers, through their varying angular hide-out, to actively or passively lay ambush on the legitimate transmitter–receiver path. This consideration is yet, to the best understanding of the authors, to be considered by the previous researchers. The MISOME model was used to experiment with the proposed method; the transmitter and eavesdropper have multiple antennas; the legitimate receiver has a single antenna, and it is placed at a random angle θ from the associated transmitter. Also, we evaluated the effectiveness of the novel approach using some performance metrics such as SOP, secrecy capacity, and secure connectivity. The findings show that the secure transmission can be enhanced by considering the angular location in WCSs. The validity of the proposed secrecy improvement scheme is simulated, and different angle values are assigned accordingly to justify the effectiveness of the proposed technique compared to others. The findings also depict that the communication network would be highly secure if and only if the outage probability is less while the SNR is high. In addition to that, the numerical results also prove that the boundary technique enhances secure wireless communication. Conclusively, our future work will explore optimal security techniques enhancement for PLS wireless communication in the angular domain.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ETHICS STATEMENT

This article does not contain any studies with human participants or animals performed by any of the authors.

ORCID

Ismaeel Abiodun Sikiru  <https://orcid.org/0000-0003-1225-7375>

Agbotiname Lucky Imoize  <https://orcid.org/0000-0001-8921-8353>

REFERENCES

1. Kadhim A N, Sadkhan SB. Security threats in wireless network communication – status, challenges, and future trends. In: International Conference on Advanced Computer Applications (ACA); 2021:176–181.
2. Nosrati E. Secrecy enhancement in cooperative relaying systems. Electronic Thesis and Dissertation Repository 2015:1–98. <https://ir.lib.uwo.ca/etd/3310>
3. Jamshed MA, Heliot F, Brown T. A survey on electromagnetic risk assessment and evaluation mechanism for future wireless communication systems. *IEEE J Electromagn., RF Microw Med Biol.* 2019;4(1):24–36.

4. Tse D, Viswanath P. *Fundamentals of Wireless Communication*. Cambridge: Cambridge University Press; 2005.
5. Fang W, Li F, Sun Y, et al. Information security of PHY layer in wireless networks. *Journal of Sensors*. 2016;2016:1-10.
6. Lu X. *Cost-Effective Signal Processing Algorithms for Physical-Layer Security in Wireless Networks*. Doctoral dissertation. United Kingdom: University of York/University Press; 2016.
7. Rahmanpour A, Vakili VT, Razavizadeh SM. Enhancement of physical layer security using destination artificial noise based on outage probability. *Wireless Personal Communications*. 2017;95(2):1553-1565.
8. Wyner AD. The wiretap channel. *Bell Syst Tech J*. 1975;54(8):1355-1387.
9. Leung-Yan-Cheong SK, Hellman M. The gaussian wiretap channel. *IEEE Trans Inf Theory*. 1978;24(4):451-456.
10. Khan MI, Riaz M. Comparison of different types of physical layer security techniques in wireless communication systems: a review. *Eur J Eng Technol*. 2017;5(1):51-61.
11. Darshini R, Sampooram KP. A survey: proactive eavesdropping via jamming to defend against suspicious communication link. *Int J Innov Res Sci, Eng Technol*. 2018;7(10):10437-10442.
12. Du R, Zhen L. Multiuser physical layer security mechanism in the wireless communication system of IIOT. *Comput Secur*. 2022;113(1):1-12. doi:10.1016/j.cose.2021.102559
13. Koufos K, and Dettmann CP. *Boundaries as an Enhancement Technique for Physical Layer Security*. IEEE Transactions on Information Forensics and Security. New Jersey: Institute of Electrical and Electronics Engineers (IEEE); 2018;14(1):61-74 .
14. Vaezi M, Amarasuriya G, Baduge A, et al. Interplay between NOMA and other emerging technologies: a survey. *IEEE Trans Cognit Commun Netw*. 2019;5(4):900-919.
15. Güvenkaya E, Hamamreh JM, Arslan H. On physical-layer concepts and metrics in secure signal transmission. *Phys Commun*. 2018;25(2):14-25.
16. Wang HM, Xia XG. Enhancing wireless secrecy via cooperation: signal design and optimization. *IEEE Communications Magazine*. 2015;53(12):47-53.
17. Zhi L, Min L, Benoit C, Wei-Ping Z, Naofal A. Secure and energy efficient transmission for RSMA-based cognitive satellite-terrestrial networks. *IEEE Wirel Commun Lett*. 2020;10:1-5. doi:10.1109/LWC.2020.3026700
18. Zou Y, Zhu J, Wang X, Leung VCM. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network*. 2015;29(1):42-48.
19. Shiu Y, Chang SY, Wu HC, Huang SC-H, Chen HH. Physical layer security in wireless networks: a tutorial. *IEEE. Wireless Communications*. 2011;18(2):66-74.
20. Li H. Physical-layer security enhancement in wireless communication systems. University of Western Ontario – Electronic Thesis and Dissertation Repository; paper 1583; 2013:1-115.
21. Zhang R, Song L, Han Z, and Jiao B. Improve physical layer security in cooperative wireless network using distributed auction games. In: IEEE Conference on Computer Communications Workshop 2011. doi:10.1109/infcomw.2011.5928805
22. Quyen NX, Duong TQ, Vo N-S, Xie Q, Shu L. Chaotic direct-sequence spread-spectrum with variable symbol period: a technique for enhancing physical layer security. *Comput Netw*. 2016;109(1):4-12.
23. Hu L, Wen H, Wu B, Pan F, Liao RF, Song H, Tang J, and Wang X. Cooperative jamming for physical layer security enhancement in internet of things. *IEEE Internet Things J* 2018;5(1):219-228.
24. Lee JH. Optimal power allocation for physical layer security in multi-hop DF relay networks. *IEEE Trans Wirel Commun*. 2015;15(1):28-38.
25. Wang Q, Chen Z, Mei W, Fang J. Improving physical layer security using UAV-enabled Mobile relaying. *IEEE Wirel Commun Lett*. 2017;6(3):1-4.
26. Feng Y, Yan S, Yang Z, Liu C, Yang Z, Yang N. Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access. *IEEE Trans Inf Foren Sec*. 2018;14(6):1670-1683.
27. Zhi L, Min L, Jun-Bo W, Tomaso dC, Jiangzhou W. Joint beamforming and power allocation for satellite-terrestrial integrated networks with non-orthogonal multiple access. *IEEE J Sel Top Signal Process*. 2019;13(3):657-670.
28. Zhi L, Hehao N, Kang A, et al. Refracting RIS aided hybrid satellite-terrestrial relay networks: joint beamforming design and optimization. *IEEE Trans Aerosp Electron Syst*. 2022;58(4):3717-3724. doi:10.1109/TAES.2022.3155711
29. Wang L, Cai Y, Zou Y, Yang W, Hanzo L. Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays. *IEEE Trans Vehic Dent Tech*. 2015;65(8):6259-6274.
30. Zhi L, Min L, Tomaso DC, Jun-Bo W, Wei-Ping Z, and Julian C. Supporting IoT with rate-splitting multiple access in satellite and aerial integrated networks. *IEEE Internet Things J*. 2021;8(14):11123-11134. doi :10.1109/JIOT.2021.3051603
31. Sheng Z, Tuan HD, Duong TQ, and Poor HV. *Beamforming Optimization for Physical Layer Security in MISO Wireless Networks*. IEEE Transactions on Signal Processing. 2018;66(14):3710-3723.
32. Zhang Y. *Wireless Security with Beamforming Technique*. Doctoral dissertation. United Kingdom: The Queen's University of Belfast; 2016.
33. Mukherjee A, Ali S, Fakoorian A, Huang J, and Swindlehurst AL. *Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey*. Vol. 16. IEEE Communications Surveys & Tutorials; 2014: 1550-1573.
34. Ekrem E, Uluks S. Secure broadcasting using multiple antennas. *J Commun Netw*. 2010;12(5):411-432.
35. Yingbin L, Poor HV, Shamai S. Secure communication over fading channels. *IEEE Trans Inf Theory*. 2008;54(6):2470-2492. doi:10.1109/TIT.2008.921678
36. Khisti A, Wornell GW. Secure transmission with multiple antennas. The MISOME Wiretap Channel. *IEEE Trans Inf Theory*. 2010a;56(7):3088-3104. doi:10.1109/TIT.2010.2048445

37. Yan S, Yang N, Malaney R, Yuan J. Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels. *IEEE Trans Wirel Commun*. 2014;13(3):1656-1667. doi:[10.1109/twc.2013.013014.131248](https://doi.org/10.1109/twc.2013.013014.131248)
38. Papoulis A. *Probability, Random Variables and Stochastic Processes*. 3rd ed., United States: McGraw-Hill; 1991.
39. Zou Y, Zhu J, Wang X, Leung VCM. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Netw*. 2015;29(1):42-48.
40. Zhu G, Liu D, Du Y, You C, Zhang J, Huang K. Towards an intelligent edge: wireless communication meets machine learning. *IEEE Commun Mag*. 2020;58(1):19-25.
41. Mukherjee A. Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints. *Proc IEEE*. 2015;103(10):1747-1761. doi:[10.1109/JPROC.2015.2466548](https://doi.org/10.1109/JPROC.2015.2466548).
42. Chen S, Wen H, Wu J, et al. Radio frequency fingerprint-based intelligent Mobile edge computing for IoT authentication. *Sensors*. 2019;19(16):36-46.
43. Baldi M, Bianchi M, Maturo N, Chiaraluce F. A physical layer secured key distribution technique for IEEE 802.11g wireless networks. *IEEE Wirel Commun Lett*. 2013;2(2):183-186.
44. Pan F, Jiang Y, Wen H, Liao R, and Xu A. *Physical Layer Security Assisted 5G Network Security*. 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall); 2017:1-5.
45. Mazin A, Davaslioglu K, and Gitlin RD. Secure key management for 5G physical layer security. In: IEEE 18th Wireless and Microwave Technology Conference (WAMICON); 2017:1-5. doi:[10.1109/WAMICON.2017.7930246](https://doi.org/10.1109/WAMICON.2017.7930246)
46. Mostafa A, Lampe L. Enhancing the security of VLC links: physical-layer approaches. *2015 IEEE Summer Topicals Meeting Series (SUM), Nassau, Bahamas*. SUM; 2015:39-40.
47. Zhang L, Wen H, Song H, Tang J, Jiang V, Dong W, and Zhu X. The performance of the MIMO physical layer security system with imperfect CSI. In: IEEE Conference on Communications and Network Security (CNS). IEEE; 2016:346-347. doi:[10.1109/CNS.2016.7860504](https://doi.org/10.1109/CNS.2016.7860504)
48. Yao J, Zhou X, Feng YLS. Secure transmission in linear multihop relaying networks. *IEEE Trans Wirel Commun*. 2017;17:822-834. doi:[10.1109/TWC.2017.2771774](https://doi.org/10.1109/TWC.2017.2771774)
49. Abdelgader AMS, Shu F. Exploiting the physical layer security for providing a simple user privacy security system for vehicular networks. *International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE)*. Khartoum, Sudan; 2017.
50. Wu Q, Mei W, Zhang R. Safeguarding wireless network with UAVs: a physical layer security perspective. *IEEE Wirel Commun*. 2019;26(5):12-18.
51. Qin Z, Liu Y, Ding Z, Gao Y, Elkashlan M. Physical layer security for 5G non-orthogonal multiple access in large-scale networks. In: *Proc. IEEE ICC 2017*. Kuala Lumpur, Malaysia: IEEE; 2016:1-6.

SUPPORTING INFORMATION

Additional supporting information can be found online in the Supporting Information section at the end of this article.

How to cite this article: Sikiru IA, Olawoyin LA, Faruk N, et al. Physical layer security using boundary technique for emerging wireless communication systems. *Security and Privacy*. 2022;e288. doi: [10.1002/spy2.288](https://doi.org/10.1002/spy2.288)