An Enhanced Secure Cooperative Relay Systems with SADEA-Optimised Hybrid Decode-Amplify-Forward Protocols

J. A. Adeleke[1*], D. B. O. Konditi[2] , Z. K. Adeyemo[3]

[1]Department of Electrical Engineering (Telecommunication Option), Pan African University, Institute for Basic Sciences and Technology and Innovation, Nairobi, Kenya.
[2]School of Electrical and Electronics Engineering, Technical University of Kenya (TUK), Nairobi, Kenya.
[3]Department of Electrical and Electronics Engineering, Ladoke Akintola University of Technology, Oyo State, Nigeria.

ABSTRACT: One of the most crucial tasks in modern wireless communication systems is to ensure dependable transmission security. Unfortunately, traditional secure data transmission techniques are vulnerable to eavesdropping, while modern methods struggle with complexity, power consumption, and dynamic channels. Cooperative jamming is limited by power allocation and synchronization in decentralized networks. This paper proposes a Secure Space Diversity-Based Hybrid Decode Amplify and Forward (HDAF) Cooperative Relay Protocol to address these issues. It utilizes Space Diversity (SD), HDAF, and Information-theoretic security (IS) for secure communication. Relay selection is optimized based on SNR, while exclusive OR (XOR) processing at relays ensures data confidentiality. The Surrogate Model-Assisted Differential Evolution for Antenna Synthesis (SADEA) algorithm is used to optimize antenna configurations at the transmitter. Using machine learning-driven Gaussian process models with Differential Evolution (DE), SADEA can enhance efficiency and reduce computational costs. The proposed HDAF protocol outperforms conventional methods, achieving a 96.86%, 36.36%, 19.94% reduction in Bit Error Rate (BER), Outage Probability (OP) and Secrecy Outage (SO) respectively via MATLAB simulations at an SNR of 0 dB and L = 2 for 64-PSK modulation. The HDAF protocol is therefore proposed as one of the best candidates for enhancing physical layer security in wireless networks.

KEYWORDS: Cooperative Relay Protocol, Space Diversity, Secure Communication, SADEA, Information-Theoretic Security

[Received Mar. 7, 2025; Revised Apr. 2, 2025; Accepted Apr 8, 2025] Print ISSN: 0189-9546 | Online ISSN: 2437-2110

I. INTRODUCTION

Wireless communication has significantly advanced data transmission, enabling flexible and reliable connectivity, as Ojo et al. (2022) emphasised. However, the increasing demand for high data rates has introduced challenges such as multipath-induced fading, signal outages, and security vulnerabilities in Yatnalli et al. (2020). Addressing these challenges requires innovative solutions that enhance signal reliability and security.

Cooperative communication (CC) has emerged as a promising technique for mitigating fading by employing relay nodes to forward signals, improving resilience against channel distortions, as emphasised in Bayrakdar (2019). Traditional cooperative relay strategies include Amplify-and-Forward (AF) and Decode-and-Forward (DF). While AF amplifies signals before forwarding them, it also propagates noise, reducing signal clarity. On the other hand, DF decodes and re-encodes the signal but may introduce errors, especially in poor channel conditions presented in Qin et al. (2022) and Yany et al. (2019). In order to overcome these limitations, the Hybrid Decode-Amplify-Forward (HDAF) protocol was introduced, combining the advantages of both AF and DF. However, HDAF still degrades the signal when the source-to-relay link is weak due to deep fading, as stated by Akande et al. (2023) and Liu et al. (2022).

Space Diversity (SD), which incorporates multiple antennas at the transmitter to provide independent fading paths to mitigate the deep fades and help the recovery of a signal, was introduced in the transmitter to enhance the performance of HDAF based on Homavazir (2020). The antenna configurations were also optimised in order to further optimise SD effectiveness. As emphasised in Cordero-Samortin et al (2021) and Akinsolu et al (2022), machine learning driven algorithm called SADEA was used in this research to optimise antenna settings to enhance signal reception and minimize interference. Even though SD together with SADEA still enhance the performance, as transmissions are open to eavesdropping wireless channels also present security threats (Shukla et al., 2018). Therefore, an Information-theoretic Security (IS), based on the cooperative relay framework was considered to mitigate security. IS implements physical layer security techniques such as XOR-based encoding to avoid interception by the third-party Bloch et al, (2021).

Recent studies have explored cooperative relay methods for improving wireless communication. Fitri et al. (2023) analyzed

*Corresponding author: job.adeleke@students.jkuat.ac.ke
doi: http://dx.doi.org/10.63746/njtd.v22i3.3472

secrecy outage (SO) in AF, DF, and Quantize-and-Forward (QF) protocols, highlighting that max-min relay selection improves secrecy capacity but lacks spatial diversity enhancements. Unlike their study, this work integrates SD and IS to strengthen security. Xiao and Ouyang (2015) developed a multiuser diversity framework for HDAF but did not address security aspects or spatial diversity optimization. The research fills these gaps by implementing SD through IS combined with SADEA to optimize system performance and security. Ahiadormey et al. (2019) analyzed outage probability (OP) in combined Power Line Communication (PLC) and wireless systems yet failed to discuss security threats. The research develops IS-secured transmissions along with SD efficiency improvements to enhance reliability. The research by Shukla et al. (2018) explored secure AF antenna selection yet suggested new investigations involving eavesdropper placement strategies. The SSD-HDAF protocol establishes secure XOR encoding and SD as a security solution.

Despite advances in Cooperative Communication, prior research has not adequately explored the joint integration of SD, SADEA, and IS within HDAF systems. The system with SADEA-based optimal antenna configuration and Equal Gain Combining (EGC) at the receiver accomplishes better performance than standard HDAF models while protecting against eavesdroppers. The combined usage of IS with the SD and SADEA protocol enables secure wireless communications between relay nodes while protecting against fading and eavesdropping threats. This signifies the added resilience of this protocol solution for cooperative networks.

Despite these advancements, some challenges remain. First, the computational complexity of SADEA, while reduced compared to exhaustive search techniques, still presents a trade-off between optimization accuracy and processing time, particularly for large-scale networks. Second, the proposed SSD-HDAF protocol, though optimized for security and reliability, does not explicitly account for power consumption constraints, which could be a critical factor in energy-limited wireless systems.

II. METHODOLOGY

This research proposes an SSD-HDAF Cooperative Relay Protocol with SADEA for antenna optimisation at the transmitter for wireless communication over Rayleigh fading channels. The system combines optimised SD with Information-theoretic Security (IS), employing SNR-based relay selection, XOR encoding for security, and Equal Gain Combining (EGC) for decoding. A Probability Density Function (PDF) was used to evaluate and compare the performance of the proposed method against conventional HDAF methods.

A. Antenna Optimization using Surrogate Model-Assisted Differential Evolution (SADEA)

SADEA was employed to optimise the transmitting antenna at the onset of the simulation in this research, while the antenna simulated in this study is the 60GHz Inter-chip wireless antenna with 10 design parameters. This type of antenna was chosen due to its suitability for high-speed, short-range communication, which aligns with the requirements of modern inter-chip communication systems. Operating in the unlicensed 60GHz millimetre-wave band, this antenna offers a high data transfer rate, reduced interference, and compact size. It is ideal for integration into wireless chip-to-chip communication setups.

Although this type of antenna has a problem with short-range communication, it is well-suited for secure and efficient data transmission between closely positioned components, as illustrated in Figure 1.

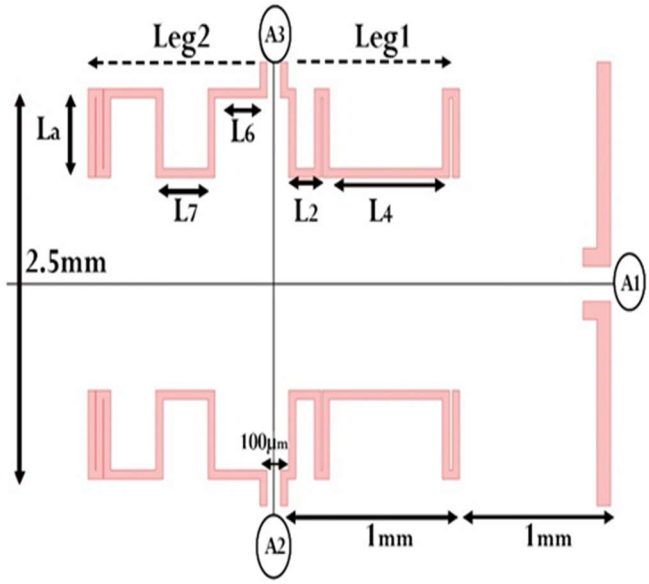

Figure 1. Antenna Proximity coupling scheme.

In the inter-chip communication scheme, Antenna A2 communicates with Antenna A3, while both experience interferences from Antenna A1, a broadband dipole used as a biasing element, against a 90nm CMOS silicon technology for the substrate. Antennas A2 and A3 are both chosen as meander-line dipoles. The optimisation aims to maximise the coupling from antennas A2 to A3 while minimising the crosstalk from antenna A1. Therefore, the optimisation problem is defined as shown in Eqn. 1:

$$f(x) = \begin{cases} maximize & coupling(A2, A3) \\ s.t. & crosstalk(A1, A2) \leq 30dB \end{cases} \quad (1)$$

The goal of the optimization is to maximize the coupling between Antenna A2 and A3 while ensuring that the crosstalk between A1 and A2 remains below a specified threshold. The gain function that SADEA maximizes is defined as:

$$\max_x f(x) = |S_{21}(A2, A3)|$$

where:

- $f(x)$ is the gain function that needs to be maximized.
- $S_{21}(A2, A3)$ represents the transmission coefficient between antennas A2 and A3.
- $x = \{L_1, L_2, \ldots, L_n\}$ is the set of design parameters being optimized.

Since SADEA is an optimization algorithm, it finds the optimal values of x that maximize $|S_{21}(A2, A3)|$ while satisfying the optimization constraints, which are subject to the following;

i. Crosstalk Constraint: $|S_{21}(A2, A3)| \leq S_{max}$

where $S_{max} = -30$ dB, ensures that crosstalk does not exceed the threshold.

ii. Frequency Constraint: $f_{target} = 60\,GHz$. The optimized antenna parameters must ensure operation at 60 GHz.

iii. Antenna Design Constraints: $L_{min,i} \leq L_i \leq L_{max,i}, \quad i = 1,2,\ldots,n$
where each design parameter L_i must lie within predefined practical limits to ensure manufacturability and compliance with system requirements.

Thus, SADEA stores a database with all the precisely evaluated solutions and their corresponding function values from the objective function to simplify the optimisation problem. When the new x function was evaluated, the database was updated with the exact function value pair. Latin Hypercube sampling (LHS) was then used to initialise the database in Peng et al. (2024).

The LHS sampling method samples the design space more homogenously and consequently requires fewer samples for better sampling. The flowchart of the SADEA implementation is illustrated in Figure 2. The SADEA algorithm was implemented using the following steps:

Step 1: The first database was generated via Latin Hypercube sampling solutions from the objective function and exact function evaluations of all individuals.

Step 2: The best solution from the database was outputted when the preset stopping criterion was achieved, i.e., when a maximum number of exact function evaluations was met; otherwise, continue to step 3.

Step 3: A population P was formed with the best solutions (i.e., minimum function values) from the database, and the best solution obtained was updated.

$$V_i(t+1) = x_{best}(t) + F\left(x_{r_1}(t) - x_{r_2}(t)\right) \quad r_1, r_2 \in \{1,\ldots,NP\}, r_1 \neq r_2 \neq i \tag{2}$$

where NP is the population size, $V_i(t+1)$ is a mutant version of $(t+1)$ generation. Indices r_1 and r_2 are selected at random, different from the current index i, and $x_{best}(t)$ is the current population's best individual. F is the scaling factor that is considered a constant for this research.

$$U_{i,j}(t+1) = \begin{cases} V_i(t) & if(rand(i,j) \leq CR) \mid j = randn(i) \\ V_{i-1}(t) & otherwise \end{cases} \tag{3}$$

where $randn(i)$ is a randomly chosen index from the set $\{1,\ldots,d\}$, $CR \in [0,1]$ is a parameter known as the crossover rate, $rand(i,j)$ is an independent random number uniformly distributed in the range $[0,1]$.

Step 4: Now, apply the DE mutation according to Eqn. 2 and crossover using Eqn 3 operators on P to generate λ child solutions.

Step 5: The last τ solution from the database (i.e., the newest τ solutions), along with their function values, was collected as training data to build a GP surrogate model.

Step 6: The λ child solutions in step 4 were pre-screened using the GP model from step 5 with LCB pre-screening.

Step 7: The pre-screened best child solution from Step 6 was evaluated, and the evaluated solution and its function value were added to the database. Then, the algorithm goes back to Step 2.

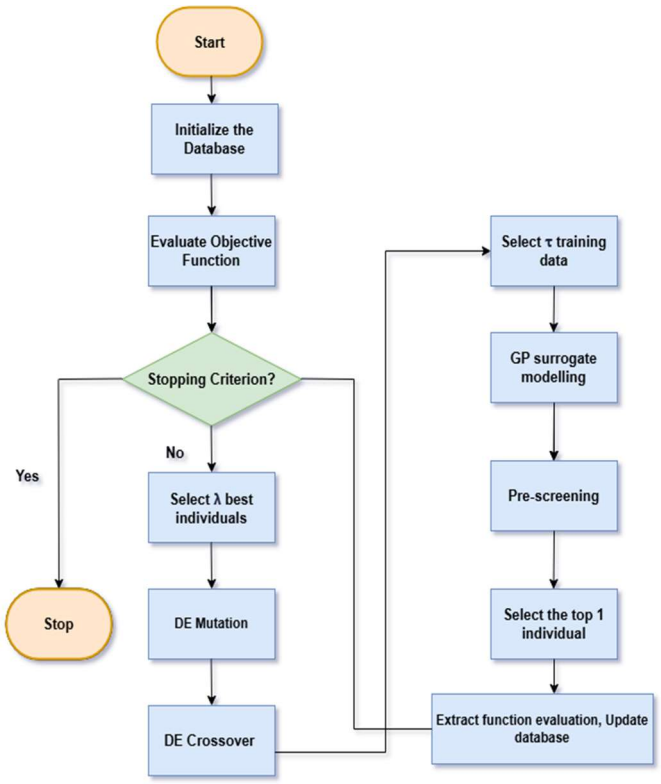

Figure 2. Flowchart of the SADEA Antenna Optimization Algorithm.

The inter-distance between antenna A2 and A3 is 2.5mm, as shown in Figure 1. In order to ensure that the crosstalk between antenna A1 to A2 and antenna A1 to A3 are equal, Antennas A2 and A3 were mirrored. Also, for each meander line antenna, both arms consist of five horizontal sections (L1 to L5 in one arm and L6 to L10 in the other arm). The total length of each arm is constrained to 1 mm, as shown in Eqn. 4, which is controlled as part of the data generation for the algorithm.

$$\sum_{m=1}^{5} L_m = \sum_{m=6}^{10} L_m = 1mm \tag{4}$$

The antenna width L_a is 500m, antenna A1's dipole length is 2.6 mm, and the dipole is 1mm from the other antennas. In the optimisation using SADEA, the base number of samples is fixed to 40 for the setting of 10 design variables, and other parameters are shown in Table 1. The scaling factor and crossover rate were set to 0.8 among these parameters. This choice was informed by prior optimization experiments reported by Zhang (2023) and Price et al. (2006), where extensive studies demonstrated that a scaling factor and crossover rate of 0.8 consistently yielded optimal performance in similar optimization scenarios. Antenna A2 and A3 coupling are optimised to -18.25 dB, while the constraint is satisfied with -29.18 dB crosstalk, and the obtained values of the 10 design parameters are shown in Table 2. One evaluation of potential solutions takes about 4 minutes for this optimisation process. Optimised antenna characteristics enable improved output in terms of bandwidth, efficiency, gain, and sidelobe levels. The antenna guarantees effective 60GHz operation and system security compliance through specific optimal values of

L1 to L10 coupled with defined coupling and crosstalk constraints.

Table 1. SADEA Simulation Parameters

Parameters	Values
Scaling factor (F)	0.8
Crossover rate (CR)	0.8
Number of training data (τ)	100
Population size (λ)	50
Initial samples (α)	3*d

The SADEA optimization model significantly enhances system performance by optimizing antenna configurations, which traditional techniques often overlook or handle less effectively. By employing Latin Hypercube Sampling (LHS) for initialization and Gaussian Process (GP) surrogate

Table 2. Optimal values for L1 – L10

Parameter	Optimal Value (µm)
L1	8.34
L2	136.8
L3	8.34
L4	823.33
L5	23.19
L6	328.85
L7	328.85
L8	328.85
L9	6.76
L10	6.69

modelling for pre-screening, SADEA efficiently explores the design space while minimizing computational overhead. The experimental results demonstrate that this method achieves optimal inter-chip wireless antenna coupling performance between A2 and A3 (-18.25 dB) with low crosstalk from A1 at -29.18 dB. The typical methods apply set designs or general algorithms to antenna optimization without achieving an optimal balance between coupling and crosstalk constraints, thus resulting in below-par performance outcomes. SADEA implements adaptive mutation and crossover operators for antenna parameter refinement (such as L1 to L10) that directly modify essential performance metrics like bandwidth, efficiency, gain and sidelobe levels. The optimized design achieves better signal reception quality and reduced interference, which helps lower the Bit Error Rate (BER) and Outage Probability (OP) measurements in SSD-HDAF protocol.

Experimental validation shows that the SADEA-optimized system achieves BER results twice as low as standard implementations at elevated path diversity conditions. The theoretical optimization through SADEA creates an explicit connection, demonstrating its superior reliability and spectral performance over traditional approaches.

B. SSD-HDAF Cooperative Relaying network using Space Diversity at the source and IS at the relay node

In this cooperative relaying network, the relay node receives multiple transmitted signal copies from the optimised antenna source, enhancing signal reliability through spatial diversity. The relay with the highest signal-to-noise ratio (SNR) is dynamically chosen for the next transmission hop. Once selected, this relay amplifies the decoded signal by a specific relay gain, as represented in Eqn. 5. The SNR γ_{Ri} of the signal selected at the relay node, is defined as shown in Eqn. 6. By multiplying the selected signal by the relay gain, Eqn. 7 will be obtained, representing the relay-transmitted signal after the gain application.

$$\beta = \left(\frac{P_r}{P_r {h_{sr}}^2 + N_r}\right)^{\frac{1}{2}} \tag{5}$$

where P_r is the relay power, ${h_{sr}}^2$ is the source of the relay channel coefficient, and N_r is the noise present at the relay node.

$$\gamma_{Ri} = \frac{P_t H_i}{N_i} \tag{6}$$

where; P_t is the power of transmitting signal, H_i is the channel gain between the source and relay and N_i is the noise present.

$$x_{Ri}(t) = \frac{P_t H_i}{N_i} \times \left(\frac{P_r}{P_r h^2{}_{sr} + N_r}\right)^{\frac{1}{2}} \tag{7}$$

This relayed signal then undergoes HDAF processing, followed by XOR encoding with a common message to secure the signal, leveraging (IS) before transmission to the destination. This step ensures protection against eavesdropping, as presented in Rong et al. (2023) and Han et al. (2014), as expressed in Eqn. 8.

Upon reaching the destination, the received signal is decoded by XOR with the common signal message as shown in Eqn. 9, thereby recovering the confidential message, as shown in Eqn. 10:

$$[x_{Ri}(t) \oplus x_n(t)] = [\gamma_{Ri} \times \beta \oplus X_n(t)] \tag{8}$$

$$[x_{Ri}(t) \oplus x_n(t)] \oplus x_n(t) = [\gamma_{Ri} \times \beta \oplus X_n(t)] \oplus x_n(t) \tag{9}$$

$$x_{Ri}(t) = \frac{P_t H_i}{N_i} \times \left(\frac{P_r}{P_r h^2{}_{sr} + N_r}\right)^{1/2} \tag{10}$$

C. Adaptive HDAF Cooperative Relaying with Space Diversity and Security Integration

Multiple antennas positioned at the relay node receive multiple copies of the transmitted signal, which are configured using the SADEA algorithm. Each incoming signal undergoes decoding through the standard HDAF approach. After decoding, the HDAF output is XOR, with a common message created by HDAF before relaying to the destination. This XOR process provides additional security, helping prevent eavesdroppers from interpreting the confidential information intended for the legitimate receiver, as presented in Ananda Krishna et al. (2018) and Urooj et al. (2023). Figure 3 shows the block diagram of a system, while Figure 4 shows the flow chart of the developed model; at the destination, these signal copies are combined through an Equal Gain Combiner (EGC) and then decoded using the common message.

The signal generated randomly at the source undergoes modulation and is sent over a Rayleigh fading channel. The multiple received signal copies are processed at the relay node through conventional HDAF; each signal is modulated using M-PSK in various attempts with the instantaneous signal strength γ for each path defined by Eqn. 11. Based on this, the channel gain H is computed as shown in Eqn. 12:

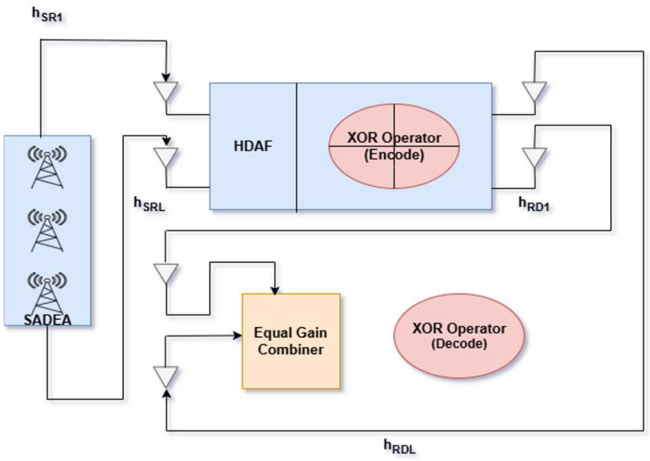

Figure 3. Block Diagram of the SSD-HDAF Relay Technique.

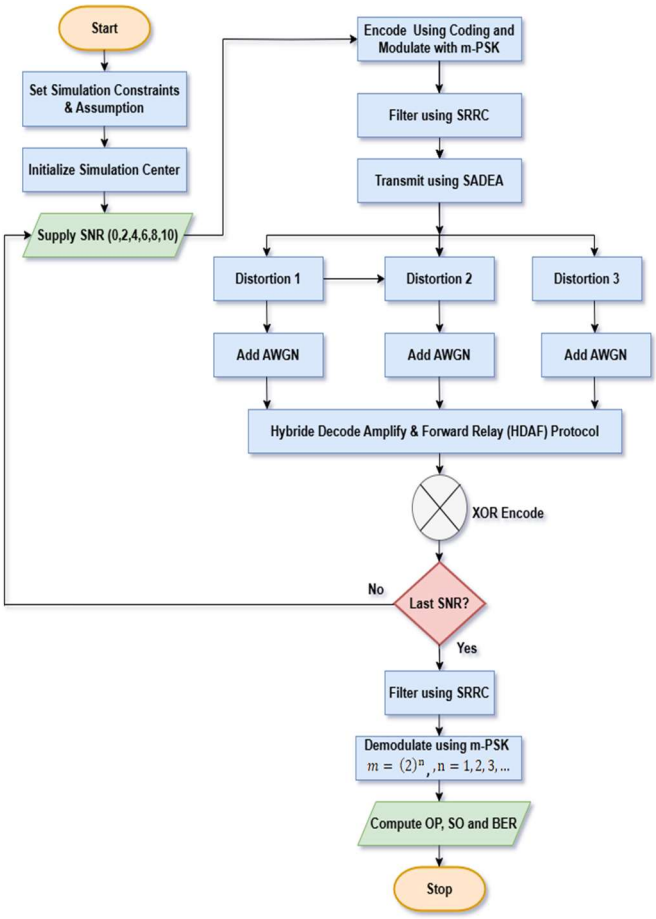

Figure 4. Flowchart of the SSD-HDAF Technique.

$$\gamma = \frac{P_t H}{w} \tag{11}$$

$$H = \frac{\gamma w}{P_t} \tag{12}$$

The signal-to-noise ratio (SNR) for the EGC output is expressed in (13), with the combined signal's SNR for this technique derived by substituting (11) into (13).

$$SNR_{mEGC} = \frac{1}{wL}\left(\sum_{i=1}^{L} r(i)\right)^2 \tag{13}$$

where $r(i)$ is the signal power on each branch, $\bar{L}$ is the number of branches, w is the noise on each branch.

The resulting channel gain of the combined signal is calculated as shown in Eqn. 14

$$H = \frac{\frac{1}{L}\left(\sum_{i=1}^{L} S(i)\right)^2}{P_t} \tag{14}$$

The Signal-to-Noise Ratio (SNR) for the EGC output is expressed in (15)

$$SNR_{EGC} = \frac{1}{wL}\left(\sum_{i=1}^{L}\left(\frac{P_t H_i}{N_i} \times \left(\frac{P_r}{P_r h^2{}_{sr} + N_r}\right)^{1/2}\right)\right)^2 \tag{15}$$

where $r(i)$ is the signal power on each branch, $\bar{L}$ is the number of branches, w is the noise on each branch.

The Probability Density Function (PDF) of the received signal over the Rayleigh fading channel is shown in Eqn. 16 and substituting Eqn. 15 into Eqn. 16 will result in Eqn. 17

$$P_R(r) = \frac{r}{\sigma^2}\exp - \left(\frac{r^2}{2\sigma^2}\right) \qquad 0 \le r \le \infty \tag{16}$$

$$P_R(r) = \frac{SNR_{EGC}}{\sigma^2} exp - \left(\frac{(SNR_{EGC})^2}{2\sigma^2}\right) \tag{17}$$

where r is the amplitude of the received signal, σ^2 is the time-averaged power of the received signal, $2\sigma^2$is the pre-detection mean power of the received signal. Table 3 depicts the system simulation parameters for the developed technique.

Table 3. System simulation parameters for the developed model

Parameters	Specifications
Modulation schemes	M-PSK
Fading	Rayleigh Fading channel
Number of paths	2,3,4
Carrier Frequency	1800MHz (The 1800MHz frequency band offers a good balance between coverage and capacity)
Noise	AWGN
Transmit Filter	Square Root Raised Cosine
Receiver Filter	Square Root Raised Cosine
Signal Bandwidth	2MHz
SNR	0,2,4.....,10
Number of symbols	10,000
Bit rate	10Mbps

III. PERFORMANCE METRICS

The performance of the proposed technique was evaluated using three key metrics.: Bit Error Rate (BER), Outage Probability (OP), and Secrecy Outage (SO). According to Derakhshani et al. (2020), OP evaluates how likely the SNR

will drop under a designated threshold, which causes communication reliability issues. SO provides Security Outage predictions that determine an attacker's ability to intercept confidential data, thus evaluating system security performance, according to Besser and Jorswieck (2020).

A. Bit Error Rate (BER)

BER is a critical performance metric in communication systems, measuring the rate of errors in a transmitted data stream. In wireless channels, factors like noise, interference, and fading affect BER, making it essential to evaluate how well a system minimizes errors and maintains signal integrity. The expression for BER ($P_b(E)$) is given in Eqn. 18, substituting Eqn. 15 into Eqn. 18 will result in Eqn. 19 and 20, Integrating Eqn. 20 gives Eqn. 21 which is the expression for BER ($P_b(E)$) used in this research work;

$$P_b(E) = \int_o^{\infty} \frac{1}{2}\exp(-0.5\gamma)\, P_\gamma(\gamma) d\gamma \quad (18)$$

$$P_b(E) = \int_0^{\infty} P_b\left(E/\gamma\right) \frac{SNR_{EGC}}{wL\sigma^2} exp - \left(\frac{(SNR_{EGC})^2}{2wL\sigma^2}\right) d\gamma \quad (19)$$

$$P_b(E) = \frac{SNR_{EGC}}{\sigma^2} exp - \left(\frac{(SNR_{EGC})^2}{2\sigma^2}\right) \times \int_0^{\infty} \frac{1}{2}\exp\left(-\frac{1}{2}\gamma\right) d\gamma \quad (20)$$

$$P_b(E) = \frac{SNR_{EGC}}{wL\sigma^2} exp - \left(\frac{(SNR_{EGC})^2}{2wL\sigma^2}\right) \times \frac{1}{2}\left[-\frac{1}{0.5} exp\left(\frac{1}{2}\right)\right]_0^{\infty} \quad (21)$$

where P_t is the transmit power at the source node, H_i is the channel gain of the i^{th} transmission path in SD, N_i is the noise power at the i^{th} receiver input, P_r relay transmission power, $h^2{}_{sr}$ is the channel gain between the source and relay in the cooperative relaying network, N_r is the noise power at the relay, L is the number of diverse branches in SD, w is the weighting coefficient of the system, σ^2 is the variance of the noise power (representing AWGN noise).

B. Secrecy Outage (SO)

SO is an essential metric in secure wireless communication since it defines the likelihood that the security capacity drops below a predefined threshold, making the system vulnerable to eavesdropping. In cooperative relay systems, an eavesdropper can exploit the broadcast nature of radio transmission to intercept signals, leading to potential security breaches. The effectiveness of secrecy outage analysis lies in evaluating the received signal-to-noise ratio (SNR) at both the legitimate destination and the eavesdropper's end. The research methodology adopted from this work follows the approach used by Agarwal et al. (2020) and Azhar et al. (2018) because they analyze outage probability (OP) in cooperative wireless systems. The proposed research develops a distinctive SO framework by integrating relay selection with space diversity approaches into its formulation.

The secrecy capacity analysis determining SO demonstrates that the outcome depends on the fluctuation between the SNR observed by the primary receiver and the eavesdropper. The calculation of secrecy outage probability depends on the likelihood that the secrecy capacity becomes lesser than C_{th}. An optimized security system results from adopting the proposed model that combines relay-aided transmission elements with space diversity techniques. The implementation of SO requires the description of channel capacity C and the eavesdropper's capacity C_e through Eqn. 22 and Eqn. 23. During the simulation process, the researchers established the secrecy threshold C_{th} , which serves as the definition of the outage condition.

$$C = B \times log_2(1 - SNR_{EGC}) \quad (22)$$

$$C_e = B \times log_2(1 - SNR_{EV}) \quad (23)$$

where B is the channel bandwidth, SNR_{EGC} and SNR_{EV} are the signal-to-noise ratio of the received signal at the destination and eavesdropper end, respectively.

The amplitude shifts keying signal '$V(t)$' can be defined as;

$$V(t) = \left(1 + V_m(t)\right)\left(\frac{A}{2} cos\left(2\pi f_c(t)\right)\right) \quad (24)$$

where V_m is a digital modulation signal, A is unmodulated carrier amplitude, f_c is the analogue carrier frequency, whereas according to Tran et al. (2022), OP is given as

$$P_{out} = 1 - Pr(\gamma_{SU} > \gamma_{th}) \quad (25)$$

Thus, by substituting (25) into (24), the resulting equation can be simplified to

$$C_s = B \times log_2(SNR_{EGC} - SNR_{EV}) \quad (26)$$

Since the general equation for SO in secure communication systems can be expressed as:

$$SO = P(C_s < C_{th}) \quad (27)$$

where C_s is the Secrecy Capacity, C_{th} is the threshold

Also, the eavesdropper can wiretap the primary signal due to the radio transmission's broadcast nature, resulting in the eavesdropper's received Signal-to-Noise Ratio (SNR) given by:

$$\gamma_{se} = \frac{p_s|h_{se}|^2}{\sigma^2} \quad (28)$$

where p_s is the source's transmit power, h_{se} is the source-to-eavesdropper channel, σ^2 is the noise variance.

Using Eqn. 27 and then substituting for Eqn. 28 and Eqn. 15, which are the received SNR for both eavesdropper and legitimate destination, the SO can be calculated as shown in Eqn. 29, which is the equation used to determine the secrecy outage in this study;

$$SO = P\left(B \times log_2\left(SNR_{EGC} - \frac{p_s|h_{se}|^2}{\sigma^2}\right) < C_{th}\right) \quad (29)$$

where B is the channel bandwidth, P_t is the transmit power at the source node, H_i is the channel gain of the i^{th} transmission path from the source to the i^{th} relay, N_r is the noise power at the relay node, p_s is the transmit power of the source in the presence of an eavesdropper, $h^2{}_{sr}$ is the channel gain between the source and relay in the cooperative relaying network, h_{se} channel coefficient between the source and the eavesdropper, N_r is the noise power at the relay, L is the number of diverse branches in SD, w is the weighting coefficient of the system, P_r is the transmit power at the relay node, σ^2 is the variance of the noise power.

C. Outage Probability (OP)

In wireless communications systems, OP is the key performance metric, which signifies the probability that the received signal-to-noise ratio (SNR) is less than the predefined threshold γ; thus, communication failure occurs. OP provides insight into system reliability in cooperative relay networks, particularly in fading environments where signal degradation occurs due to interference, noise, and multipath propagation.

Prior research from Tran et al. (2022) has extensively analysed OP in various cooperative communication schemes. However, this study presents an enhanced approach integrating SD, SADEA, and HDAF relaying to improve outage performance. The proposed model considers multiple relay paths with optimised antenna selection to enhance system performance. OP is the probability that the signal-to-noise ratio (SNR) of the received signal falls below a given threshold Tran et al. (2022). From Eqn. 30, OP is given as;

$$OP = P(\gamma < \gamma_0) = \int_0^{\gamma_0} P_r(\gamma) d\gamma \tag{30}$$

Substituting (15) into (30) gives;

$$P_{out} = \int_0^{\gamma_0} \frac{SNR_{EGC}}{\sigma^2} exp - \left(\frac{(SNR_{EGC})^2}{2\sigma^2}\right) d\gamma \tag{31}$$

$$P_{out} = \frac{SNR_{EGC}}{\sigma^2} \times \left(exp - \left(\frac{(SNR_{EGC})^2}{2\sigma^2}\right) * \int_0^{\gamma_0} \gamma(i) d\gamma \right) \tag{32}$$

Thus, integrating Eqn. 32 gives the closed-form expression for the outage probability given as Eqn. 33:

$$P_{out} = \frac{SNR_{EGC}}{\sigma^2} \times \left(exp - \left(\frac{(SNR_{EGC})^2}{2\sigma^2}\right) * (\gamma_0) \right) \tag{33}$$

where B is the channel bandwidth, P_t is the transmit power at the source node, H_i is the channel gain of the i^{th} transmission path from the source to the i^{th} relay, N_r is the noise power at the relay node, $h^2{}_{sr}$ is the channel gain between the source and relay in the cooperative relaying network, N_r is the noise power at the relay, L is the number of diverse branches in SD, w is the weighting coefficient of the system, P_r is the transmit power at the relay node, σ^2 is the variance of the noise power, γ is the SNR threshold defining the outage condition.

IV. RESULT AND DISCUSSION

This section presents the analysis of BER, OP, and SO for the developed enhanced cooperative relay system compared to the conventional system. The performance metrics are evaluated across various SNR levels, modulation schemes, and path numbers. Line graphs illustrate and compare system performance, highlighting the impact of the developed enhancements on system reliability and security. Key trends are examined to determine how the enhanced system improves data integrity and confidentiality, especially under challenging SNR conditions.

A. Bit Error Rate (BER)

The BER performance for different numbers of paths (L) and modulation schemes (64-PSK and 32-PSK) across varying signal-to-noise ratios (SNR) illustrates a significant reduction in error rates as both path diversity and SNR increase. Table 4 shows that at an SNR of 0 dB, the BER for 64-PSK with L=2 is 2.29×10^{-5}, which decreases progressively with higher path diversity, reaching 1.15×10^{-6} for L=4. Similarly, the 32-PSK scheme performs better, decreasing BER values from 4.57×10^{-6} at L=2 to 2.29×10^{-7} at L=4 for the same SNR.

The BER values demonstrate even lower error rates at higher SNR levels, such as 10 dB. For instance, at L=2 and 64-PSK, the BER is reduced to 8.59×10^{-9}, with 32-PSK showing a comparable reduction to 1.71×10^{-9}. This trend reflects the advantage of higher path diversity (L) and lower modulation order (32-PSK) in achieving better error performance, particularly at higher SNRs.

B. Secrecy Outage

The SO results for different path counts (L) and modulation schemes (64-PSK and 32-PSK) show a clear trend of decreasing SO with increased SNR and path diversity. Table 5 shows that at 0 dB SNR, the SO for 64-PSK with L=2 is 0.014227, whereas for 32-PSK, it is slightly higher at 0.015495. Increasing the number of paths to L=4 at this same SNR reduces the SO further, reaching 0.028459 for 64-PSK and 0.031005 for 32-PSK, highlighting the enhanced secrecy performance with path diversity.

The SO values decrease substantially at higher SNR levels, such as 8 and 10 dB. For example, at 10 dB with L=2, the SO for 64-PSK is 1.48×10^{-5}, and for 32-PSK, it is 1.61×10^{-5}. With L=4, these values reduce even further, achieving SO values of 2.96×10^{-5} for 64-PSK and 3.22×10^{-5} for 32-PSK. This data demonstrates that increasing path diversity and SNR can lower the SO, improving system security across both modulation schemes.

The SO values decrease substantially at higher SNR levels, such as 8 and 10 dB. For example, at 10 dB with L=2, the SO for 64-PSK is 1.48×10^{-5}, and for 32-PSK, it is 1.61×10^{-5}. With L=4, these values reduce even further, achieving SO values of 2.96×10^{-5} for 64-PSK and 3.22×10^{-5} for 32-PSK. This data demonstrates that increasing path diversity and SNR can lower the SO, improving system security across both modulation schemes.

C. Outage Probability

The OP results for various path counts (L) and modulation schemes (64-PSK and 32-PSK) exhibit a consistent decrease in OP with increasing SNR and path diversity. As shown in Table 6, at 0 dB SNR, the OP for 64-PSK with L=2 is 0.21629, while for 32-PSK, it is slightly lower at 0.202163. Increasing the number of paths to L=4 at the same SNR reduces the OP significantly to 0.10813 for 64-PSK and 0.101099 for 32-PSK, emphasising the improved performance due to path diversity. At higher SNR levels, the OP values decline even further. For instance, at 10 dB with L=2, the OP for 64-PSK is 0.058568, and for 32-PSK, it is 0.054743. With L=4, these values decrease to 0.02928 for 64-PSK and 0.027376 for 32-PSK. This indicates that higher path diversity and SNR levels significantly lower the OP, enhancing system reliability for both modulation schemes. These results highlight the effectiveness of leveraging path diversity and higher SNR levels to minimise OP in wireless communication systems.

Table 4. BER result for 32-PSK and 64-PSK

SNR	L=2		L=3		L=4	
	64-PSK	*32-PSK*	*64-PSK*	*32-PSK*	*64-PSK*	*32-PSK*
0	2.29E-05	4.57E-06	5.12E-06	1.02E-06	1.15E-06	2.29E-07
2	1.7E-05	3.38E-06	3.8E-06	7.57E-07	8.5E-07	1.7E-07
4	7.13E-06	1.42E-06	1.6E-06	3.18E-07	3.57E-07	7.13E-08
6	2.65E-06	5.28E-07	5.92E-07	1.18E-07	1.33E-07	2.65E-08
8	3E-07	5.98E-08	6.71E-08	1.34E-08	1.5E-08	3E-09
10	8.59E-09	1.71E-09	1.92E-09	3.84E-10	4.31E-10	8.59E-11

Table 5. SO result for 32psk and 64psk

SNR	L=2		L=3		L=4	
	64-PSK	*32-PSK*	*64-PSK*	*32-PSK*	*64-PSK*	*32-PSK*
0	1.42E-2	1.54E-2	1.89E-2	2.07E-2	2.85E-2	3.10E-2
2	1.08E-2	1.18E-2	1.44E-2	1.57E-2	2.17E-2	2.36E-2
4	4.47E-3	4.86E-3	5.95E-3	6.48E-3	8.93E-3	9.73E-3
6	5.93E-4	6.46E-4	7.91E-4	8.62E-4	1.19E-3	1.29E-3
8	2.84E-05	3.14E-05	3.79E-05	4.13E-05	5.69E-05	6.2E-05
10	1.48E-05	1.61E-05	1.97E-05	2.15E-05	2.96E-05	3.22E-05

Table 6. OP result for 32psk and 64psk

SNR	L=2		L=3		L=4	
	64-PSK	*32-PSK*	*64-PSK*	*32-PSK*	*64-PSK*	*32-PSK*
0	2.16E-1	2.02E-1	1.44E-1	1.35E-1	1.08E-1	1.01E-1
2	1.31E-1	1.22E-1	8.69E-2	8.14E-2	6.53E-2	6.10E-2
4	9.48E-2	8.86E-2	6.31E-2	5.91E-2	4.74E-2	4.43E-2
6	7.29E-2	6.81E-2	4.86E-2	4.54E-2	3.64E-2	3.41E-2
8	6.37E-2	5.95E-2	4.24E-2	3.97E-2	3.18E-2	2.98E-2
10	5.86E-2	5.47E-2	3.9E-2	3.65E-2	2.93E-2	2.74E-2

D. Result Discussion

The BER, SO and OP values were calculated to determine the performance of the developed approach among different pathways (L) and modulations (64-PSK and 32-PSK). The data shows that enhanced SNR values and increased path diversity (L) result in lower BER and improved SO and OP. The presented system demonstrates superior signal strength and enhanced error correction because of a higher signal-to-noise ratio and path diversity, according to the results obtained. During increased SNR and additional paths, the signal Source of Oscillation decreases, thus resulting in enhanced privacy for unauthorized users who cannot detect the signal. The system reliability increases when the signal-to-noise ratio elevates, and additional paths are added because this combination decreases the occurrence of signal dropping below-accepted thresholds. The system performance increases through better communication conditions, providing reliable and steady signal delivery even in challenging channels.

Increasing path count (L) improves performance since a large path count increases diversity, which implies low fading and interference on the diverse paths, resulting in more reliable signal transmission. For instance, when operating at high values of L, it is observed that the received signal experiences lesser error and offers better secrecy since the combined activity seems to provide enhanced results; also, at higher values of L, the system achieves lower OP, indicating improved communication stability. The modulation choice is also essential; 32-PSK is less noise-sensitive and has better BERs, SOs and OPs than 64-PSK under similar conditions, further improving system reliability. These outcomes imply that a plurality of path systems with intermediate index modulation are attainable at high security and low error rates and are indispensable for reliable wireless communication.

E. Result Benchmarking

The SO is presented in Figure 5, while Figure 6 shows the enhanced and the conventional system at varying path counts and under both 64-PSK and 32-PSK modulation, where the enhanced system has the higher advantage. The figures show that for every modulation scheme and at all values of SNR, the improved or enhanced system achieves lower SO than the conventional system and provides improved security. For example, at L=2 and SNR = 0 dB, the enhanced system achieves filter output probabilities SO at 0.0007 (for 64-PSK) and 0.0011 (for 32-PSK), considerably smaller than those of the conventional system of 0.0142 and 0.0155 for 64-PSK and 32-PSK, respectively.

This trend remains the same when the path count increases; the enhanced system has lower SO values. However, even where SO values for both systems decrease at higher SNRs due to stronger signal conditions, the SO of the enhanced system stays below the conventional system's values. This improved SO with the enhanced system has been achieved because of the efficient relay protocols and diversity techniques that can handle eavesdropping threats better than conventional systems. The results shed more light on the improved system where the proposed method provides a significant security advantage over the conventional approach for higher SNR and path diversity.

Figures 7 and 8 illustrate BER graphs under various modulation schemes (64-PSK and 32-PSK) across SNR levels, and path numbers provide a clear performance comparison between the improved and conventional systems.

The enhanced system demonstrates a significant reduction in BER across all SNR levels and path configurations, which is especially noticeable in higher SNR ranges. For instance, with L=2 at an SNR of 0 dB, the BER for the enhanced system with 64-PSK is approximately 2.29×10^{-5}, substantially lower than the conventional system's BER of 7.30×10^{-4}. This trend is

consistent for other SNR levels, with the enhanced system showing progressively lower BERs as SNR increases, underscoring its superior reliability.

The improved system attains an additional degree of improvement in BER for L=4, where more spatial diversity is used, as depicted by BER values reaching 4.30×10^ (-10) at 64-PSK with an SNR of 10dB. It is clear, therefore, that the improvement shown over the conventional system performance is due to the newly enhanced system's better relay and diversity control against noise and interference. Benchmarks made with these outcomes reveal that incorporating the proposed system as the improved relay selection and realising the aspect of diversity yields better data protection and better signal quality in the low SNR and high-path scenarios, which are not otherwise viable for the basic systems.

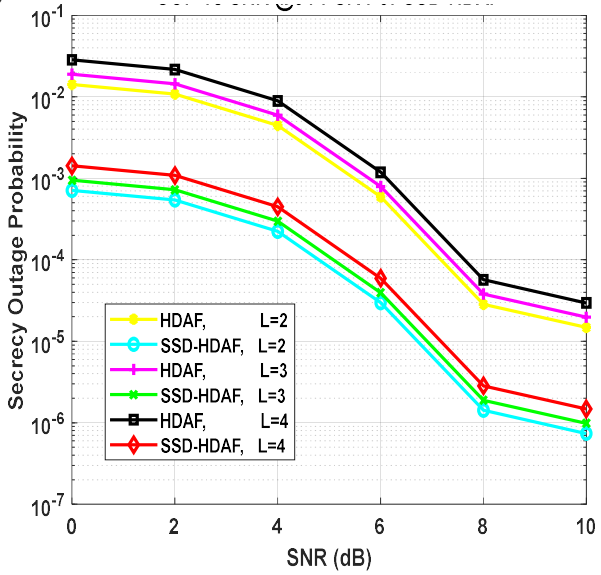

Figure 5. Secrecy Outage vs SNR for 64-PSK.

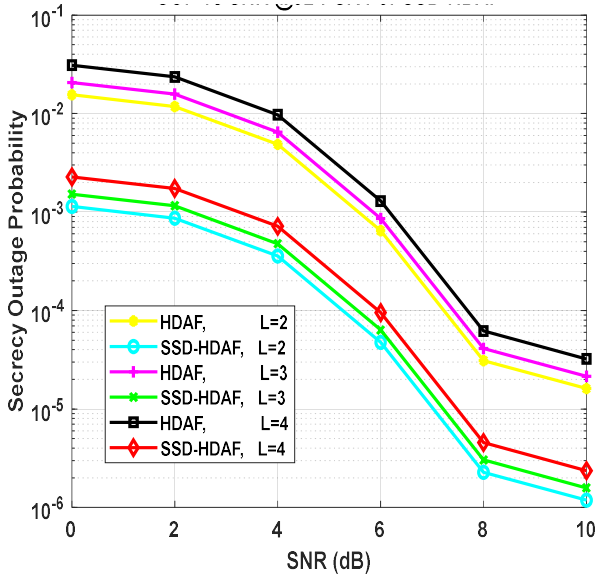

Figure 6. Secrecy Outage vs SNR for 32-PSK.

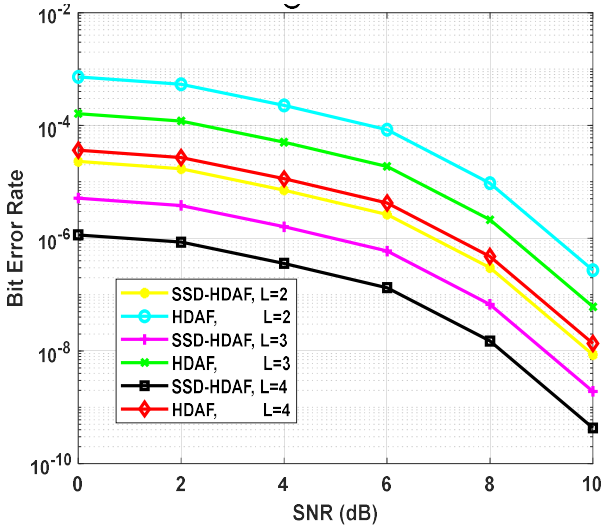

Figure 7. Bit Error Rate vs SNR Graph for 64-PSK

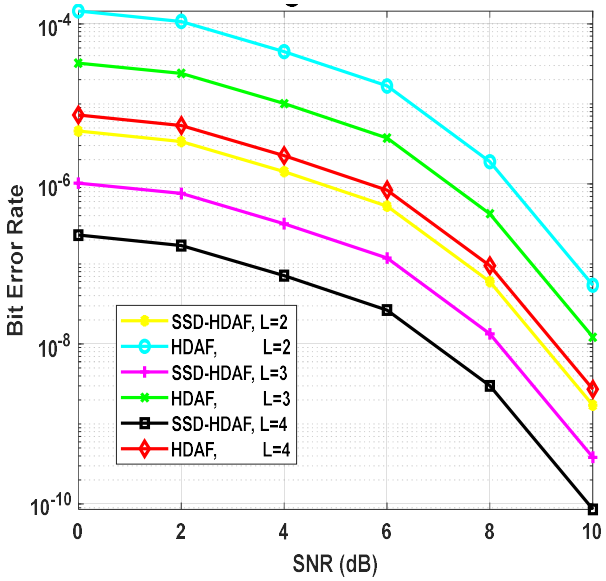

Figure 8. Bit Error Rate vs SNR Graph for 32-PSK.

The OP results are presented for the enhanced and conventional systems at varying path counts and under both 64-PSK and 32-PSK modulation schemes in Figures 9 and 10. The results show that the enhanced system consistently outperforms the conventional system across all SNR values, path counts (L), and modulation schemes, achieving lower OP and improving communication reliability. For example, at L=2 and SNR=0 dB, the enhanced system achieves an OP of 0.21629 for 64-PSK and 0.202163 for 32-PSK, while the conventional system shows higher OP values of 0.270177 and 0.252755, respectively. This substantial reduction in OP with the enhanced system highlights its superior ability to mitigate outages.

The enhanced system delivers better performance as the path count increases to L=4. At SNR=0 dB, the enhanced system's OP is reduced to 0.10813 for 64-PSK and 0.101099 for 32-PSK, whereas the conventional system yields higher values of 0.135158 and 0.126305, respectively.

This trend persists at higher SNR levels; for instance, at SNR=10 dB and L=4, the enhanced system achieves OP values of 0.02928 (64-PSK) and 0.027376 (32-PSK) compared to the conventional system's 0.036599 (64-PSK) and 0.034202 (32-PSK).

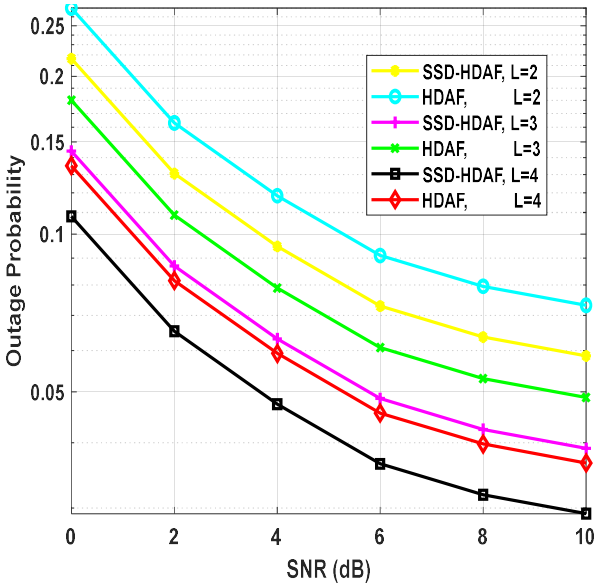

Figure 9. Outage Probability vs SNR for 64-PSK.

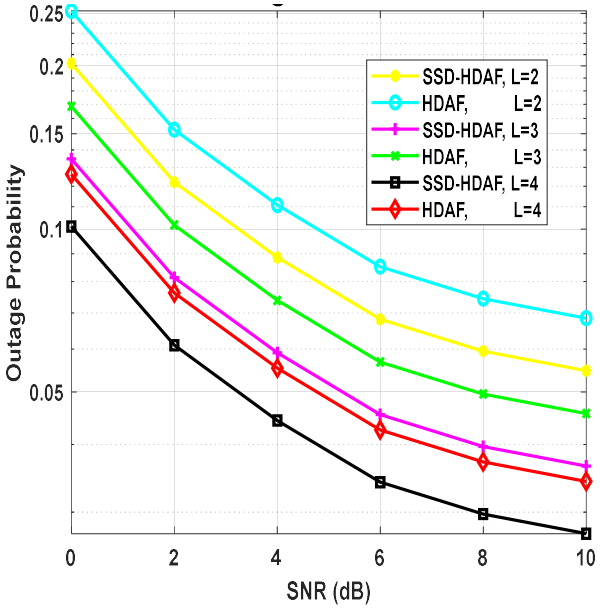

Figure 10. Outage Probability vs SNR for 32-PSK.

The findings from this study have significant implications for practical wireless communication systems, particularly in enhancing system reliability, security, and efficiency. Maintaining a low BER ensures accurate data transmission in practical applications such as 5G networks, Internet of Things (IoT) systems, and mission-critical communications (e.g., military and emergency response networks). The results indicate that the proposed model significantly reduces BER, even at lower SNR levels, which means that wireless networks can maintain data integrity in environments with high interference and fading.

Furthermore, the reduction in SO highlights the proposed model's improved security performance, effectively reducing the probability that an eavesdropper will successfully decode confidential information. This is particularly beneficial in applications requiring secure communications, such as financial transactions, military communications, and healthcare data transmission, where security breaches can have severe consequences.

The improved OP results demonstrate the model's practical effectiveness in maintaining stable connections under varying channel conditions. In traditional cooperative relay systems, reliability degrades significantly in low-SNR environments. However, the proposed model leverages path diversity (L), which has direct applications in vehicular communication systems, satellite-based networks, and industrial automation, where maintaining a reliable connection is crucial for real-time operations.

Compared to traditional relay techniques such as AF, DF, and even conventional HDAF protocols, the experimental results validate the theoretical expectations that higher path diversity, advanced modulation schemes, and security enhancements contribute to a more resilient and efficient system. The SSD-HDAF model presents a practical, scalable, high-performance solution for modern wireless communication systems.

F. Result Comparison with Previous Research

The comparison of BER performance between SSD-HDAF and Nayak & Gurrala's (2021) system, as shown in Figure 11, demonstrates that SSD-HDAF achieves significantly lower BER across all SNR values and path numbers (L) for 4-PSK modulation. At L = 4, SSD-HDAF records a BER of 3.56E-08 at SNR = 0 dB, compared to 3.39E-07 in Nayak & Gurrala's system, reflecting nearly a tenfold improvement. Similarly, at L = 3, SSD-HDAF attains a BER of 1.59E-07 at SNR = 0 dB, whereas Nayak and Gurrala's system records 1.83E-06, highlighting a significant reduction in error rates. This performance advantage is also evident at L = 2, where SSD-HDAF achieves a BER of 7.11E-07 at SNR = 0 dB, compared to 9.60E-06 in Nayak & Gurrala, further confirming its superior error resilience. The SSD-HDAF performs better than the system presented by Nayak & Gurrala because it incorporates space diversity through SADEA with optimal relay selection and equal gain combined for improved channel impairment reduction. The SSD-HDAF protocol performs better than Nayak & Gurrala's system because it implements a complete solution that includes SD with SADEA optimization and standard HDAF processing. The design enhancements lead to superior error-handling capabilities, especially during unfavourable fading environments.

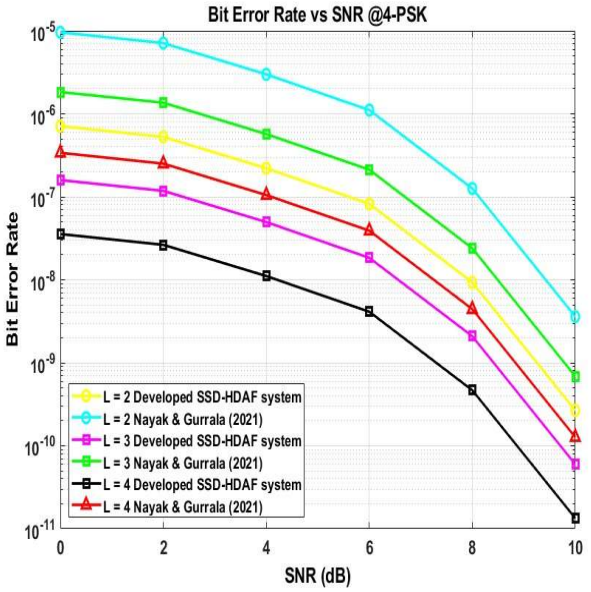

Figure 11. Developed SSD-HDAF against Nayak & Gurrala, (2021) BER for 4-PSK

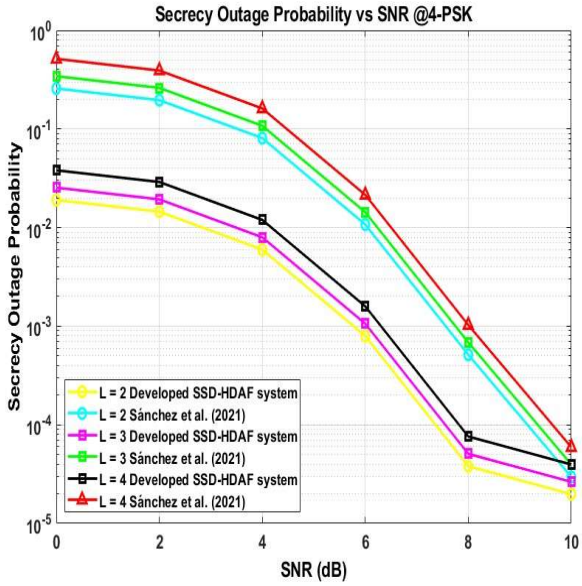

Figure 12. Developed SSD-HDAF against Sánchez et al. (2021) BER for 4-PSK

Also, the comparison of SOP between the SSD-HDAF protocol and Sánchez et al. (2021) for 4-PSK modulation, as shown in Figure 12, highlights the superior performance of the proposed system. The SSD-HDAF protocol operates with an SOP value of 0.038114 at L=4 and SNR=0 dB, which exceeds the 0.514534842 performance reported by Sánchez et al. (2021). Every path parameter plus SNR condition demonstrates that the SSD-HDAF protocol delivers SOPs that remain lower when compared to other protocols. At L=2, when SNR reaches 10 dB, the SSD-HDAF SOP amounts to 0.01907, while Sánchez et al.'s work reports an SOP value of 0.257449.

Multiple features of SD and SADEA with XOR-based encoding in the SSD-HDAF protocol serve to produce these performance enhancements. Signal reliability increases through SD's ability to develop parallel fading paths in addition to SADEA's antenna optimization feature, which minimizes interference and provides enhanced coupling. The XOR encoding technology protects data transfer by creating data obfuscation layers that exploit communication channels between authorized parties and potential intruders. Sánchez et al.'s methodology deals with physical layer security theory yet fails to include SD or advanced relay processing strategies, including SADEA.

The SSD-HDAF protocol performs better than Sánchez et al.'s method because it structures its solutions through integrated SD and optimized SADEA and IS developments to defeat fading and security threats. These experimental results validate the theoretical improvements introduced by the proposed technique, demonstrating its ability to achieve better secrecy performance under realistic channel conditions.

V. CONCLUSION

The research introduces an innovative SSD-HDAF cooperative relay protocol which integrates IS and SADEA optimisation to improve wireless communication security while ensuring reliability. The research investigates security and reliability issues that impact cooperative relay systems operating in areas where signals are prone to eavesdropping and fading effects. SD, when integrated with SADEA for antenna optimisation along with XOR-based encoding HDAF Relay protocol and EGC at the receiver, provides superior protection against eavesdropping and fading compared to traditional HDAF protocols. According to analysis, the proposed system achieves superior security performance and data accuracy across multiple paths when using high-order modulation compared to conventional systems.

SADEA antenna optimisation integrated into the system enhances performance through better antenna coupling and minimises high-frequency wireless interference during operations at 60 GHz. The simulation-based results show the SSD-HDAF protocol generates much better BER performance with lower OP and SOP across different SNR profiles using multiple modulation schemes than traditional HDAF mechanisms. Based on L=4 paths and 10 dB SNR, SSD-HDAF demonstrates 96.83% better BER in 64-PSK modulation than HDAF alone. The protocol's dual advantages of security enhancement become evident through an 19% reduction in OP combined with a 20% cut in SOP while operating at the same conditions. Unlike traditional cooperative relay approaches that suffer from degraded security in multipath fading environments, the developed method maintains data integrity while effectively suppressing crosstalk and interference. This highlights the suitability of the developed model for secure high-speed, short-range communication, such as inter-chip wireless networks and next-generation IoT applications.

Future research can explore adaptive surrogate modelling techniques to reduce computational overhead further while maintaining optimisation precision. Additionally, future work can integrate energy-efficient relay selection and power-aware optimisation frameworks to enhance the system's practicality in low-power applications.

AUTHOR CONTRIBUTIONS

J. A. Adeleke: Conceptualization, Software, Validation, Writing – original draft., Conceptualisation, Methodology, Writing – review & editing **D. B. O. Konditi:** Supervision. **Z. K. Adeyemo:** Supervision

ACKNOWLEDGMENT

The authors gratefully acknowledge financial support from members of the Pan African University Institute for Basic Sciences, Technology and Innovation in Nairobi, Kenya, and the African Union Commission.

REFERENCES

Bloch, M., Günlü, O., Yener, A., Oggier, F., Poor, H. V., Sankar, L., & Schaefer, R. F. (2021). An overview of information-theoretic security and privacy: Metrics, limits and applications. *IEEE Journal on Selected Areas in Information Theory*, *2*(1), 5-22.

Ojo, S. I., Adeyemo, Z. K., & Ojo, F. K. (2022). Energy-efficient cooperative spectrum sensing for detection of licensed users in a cognitive radio network using an eigenvalue detector. International Journal of Wireless and Mobile Computing, 23(2), 123-131.

Yatnalli, V., Shivaleelavathi, B. G., & Sudha, K. L. (2020). Review of inpainting algorithms for wireless communication application. Engineering, Technology & Applied Science Research, 10(3), 5790–5795

Bayrakdar, M. E. (2020). Cooperative communication-based access technique for sensor networks. International Journal of Electronics, 107(2), 212-225.

Qin, D., & Zhou, T. (2022). Energy efficiency in cognitive cooperatives amplifies and forwards networks—Sustainable Energy, Grids and Networks, 32, p.100923.

Li, B., Yang, J., Yang, H., Liu, G., Ma, R., & Peng, X. (2019). Decode-and-forward cooperative transmission in wireless sensor networks based on physical-layer network coding. *Wireless Networks*, 30(1), 1-7.

Akande, A. O., Agubor, C. K., Ahmed, W. A., Ogunbiyi, O., & Akinde, O. K. (2023). Performance of cooperative relay protocol in 5G mobile communication network over Rayleigh fading channel. International Journal of Mobile Communications, 21(4), 494-517.

Liu, Y., Wang, Z., Liu, C., Coombes, M., & Chen, W. H. (2022). Auxiliary particle filtering over sensor networks under protocols of amplify-and-forward and decode-and-forward relays. *IEEE Transactions on Signal and Information Processing over Networks*, *8*, 883–893.

Homavazir, Z. (2023, August). Improvement of Reliable Data Transmission Signal by Space Diversity Technique in Wireless Communication. In *2023 IEEE 4th Annual Flagship India Council International Subsections Conference (INDISCON)* (pp. 1-7). IEEE.

Akinsolu, M. O., Excell, P., & Liu, B. (2022). Surrogate Model-Assisted Global Optimization for Antenna Design. In *Surrogate Modeling For High-frequency Design: Recent Advances* (pp. 123–152).

Cordero-Samortin, A., Cruz, J. D., & Mabunga, Z. (2021). The optimisation of a 5g inset-fed patch antenna using the machine learning algorithm surrogate model assisted differential evolution for antenna synthesis. In 2021 IEEE 4th International Conference on Computer and Communication Engineering Technology (CCET) (pp. 371-375). IEEE.

Shukla, A. K., & Yadav, S. (2018). Performance analysis of incremental hybrid decode-amplify-forward cooperative relaying with relay selection in Nakagami-m fading channels. *Computers & Electrical Engineering*, *72*, 529-542.

Fitri, N. M., Yunida, Y., Melinda, M., & Nasaruddin, N. (2023). Secrecy capacity of cooperative D2D multi-relay communication system with multiple protocols based on max-min relay selection. *Jurnal Rekayasa Elektrika*, *19*(3).

Xiao, H., & Ouyang, S. (2014). Power allocation for a hybrid decode–amplify–forward cooperative communication system with two source–destination Pairs under outage probability constraint. *IEEE Systems Journal*, *9*(3), 797-804.

Ahiadormey, R. K., Anokye, P., Jo, H. S., & Lee, K. J. (2019). Performance analysis of two-way relaying in cooperative power line communications. *IEEE Access*, *7*, 97264-97280.

Shukla, M. K., Yadav, S., & Purohit, N. (2018). Secure transmission in cellular multiuser two-way amplify-and-forward relay networks. *IEEE Transactions on Vehicular Technology*, *67*(12), 11886-11899. Dec. 2018.

Peng, G., Ma, L., Hong, S., Ji, G., & Chang, H. (2024). Optimisation design and internal flow characteristics analysis based on the Latin hypercube sampling method. *Arabian Journal for Science and Engineering*, 1-40.

Zhang, X. (2023). Differential evolution without the scale factor and the crossover probability. *Journal of Mathematics*, *2023*(1), 8973912

Price, K., Storn, R. M., & Lampinen, J. A. (2006). *Differential evolution: a practical approach to global optimisation*. Springer Science & Business Media. 141(2)

Rong, B. (2023). Security in wireless communication networks. *IEEE Wireless Communications*, *30*(1), 10-11.

Han, L. C., & Mahyuddin, N. M. (2014). An implementation of Caesar cypher and XOR encryption technique in a secure wireless communication. In *2014 2nd International Conference on Electronic Design (ICED)* (pp. 111-116).

AnandaKrishna, B., Madhuri, N., Rao, M. K., & VijaySekar, B. (2018). Implementation of a novel cryptographic algorithm in Wireless Sensor Networks. In the *2018 conference on signal processing and communication engineering systems (SPACES)* (pp. 149-153).

Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023). Cryptographic data security for reliable wireless sensor network. *Alexandria Engineering Journal*, *72*, 37-50.

Li, S., Derakhshani, M., Lambotharan, S., & Hanzo, L. (2020). Outage probability analysis for the multi-carrier

NOMA downlink relying on statistical CSI. *IEEE Transactions on Communications*, *68*(6), 3572-3587.

Besser, K. L., & Jorswieck, E. A. (2020). Bounds on the secrecy outage probability for dependent fading channels. *IEEE Transactions on Communications*, *69*(1), 443-456.

Agarwal, A., Chaurasiya, R., Rai, S., & Jagannatham, A. K. (2020). Outage probability analysis for NOMA downlink and uplink communication systems with generalised fading channels. *IEEE Access*, *8*, 220461–220481.

Azhar, M., & Shabbir, A. (2018). 5G networks: challenges and techniques for energy efficiency. *Engineering, Technology & Applied Science Research*, *8*(2), 2864-2868.

Tran, H., Dang, V. H., Niyato, D., Cuong, D. N., Luong, N. C., & So-In, C. (2022). Outage probability minimisation in secure NOMA cognitive radio systems with UAV relay: A machine learning approach. *IEEE Transactions on Cognitive Communications and Networking*, *9*(2), 435-451. December 2022..