Bima Journal of Science and Technology, Vol. 8(3B) Oct, 2024 ISSN: 2536-6041

DOI: 10.56892/bima.v8i3B.849

Development of a Relay-Based Approach to Enhance Security of Voice Over Internet Protocol in Rayleigh Fading Distribution

Oseni Olasunkanmi Fatai[1], Abubakar Nuraddeen Yahya[1,2*] and Sani Saminu[3]

[1]Department of Electronic/Electrical Engineering, Ladoke Akintola University, Oyo state Nigeria
[2]Network Operations Centre, University of Ilorin, Ilorin, Nigeria
[3]Department of Biomedical Engineering, University of Ilorin, Ilorin, Nigeria

Corresponding Author: nuray5056@gmail.com, deenyahya@unilorin.edu.ng

ABSTRACT

There is a severe risk to VoIP communication's secrecy, privacy, and integrity when fading signal strength (Rayleigh fading) degrades the encryption techniques, leaving data open to interception and breaches by eavesdroppers. To address the security vulnerabilities brought in by the communication between the source and destination from interference or monitoring from an eavesdropper. This work proposed and developed the model based on the amplify and forward relay system with modifications in which jamming (noise) is used to shield communication between the source and destination from interference or monitoring from an eavesdropper, as relays are devices that can receive a signal and then retransmit it. The proposed developed model was evaluated using the Secrecy capacity (SC) and signal-to-noise ratio (SNR) for both proposed and existing models at the destination and eavesdropper.

The SC values obtained for the developed model after adjusting linearly amplified signal, G_0 (linearly amplified version) was set to 2 and SNRs to 2, 6, and 10 dB, for the destination and eavesdropper were 0.3471, 0.4904, and 0.6019, and 0.257, 0.3664, and 0.4545, respectively. On the other hand, at the same SNRs, the destination SC values for the traditional model were 0.298, 0.4355, and 0.5466, and the eavesdropper values were 0.257, 0.3644, and 0.4545. This study shows that using the relay strategy significantly improves system performance, VoIP security, and dependability Compared to previous approaches.

Keywords: VoIP, Eavesdropper, Relay, Rayleigh Fading.

INTRODUCTION

Voice over Internet Protocol with VoIP, people can communicate with each other without using a phone by making calls over fast internet [1]. The industry has come to love this technology because it is a dependable and affordable form of communication. Circuit switch networks were used for communication in the past, but VoIP has taken over as the preferred technique with the introduction of packet switched networks based on Internet Protocol (IP) [2]. VoIP communication is made up of endpoints, or telephones, control nodes, gateway nodes, and IP-based networks that communicate via a variety of media, including Ethernet, fiber, and wireless. VoIP has improved communication by offering features like file sharing, screen sharing, data sharing, and, most importantly, video chats [1,3].

VoIP is subject to comparable security issues because it is built on the same infrastructure as traditional data networks. Like any new technology, VoIP has significant security problems. One of the main ones is that it uses a lot of proprietary standards, making it difficult to install security safeguards. Because many businesses using VoIP services are ignorant of the possible security dangers, their network is open to misuse and exploitation.

DOI: 10.56892/bima.v8i3B.849

Advanced security threats including Denial of Service (DoS), Eavesdropping, and Caller ID spoofing have surfaced as VoIP continues to develop [4].

Sniffing, in other words eavesdropping, is an illegal attack in which a third party listens in on confidential conversations between two parties, such as a message, fax, video conference, or phone call. This is accomplished by intercepting the conversation without the participants' knowledge or consent, frequently by sniffing the victim's system. Since VoIP systems sometimes lack encryption, making it easy for hackers to listen in on calls, they are especially vulnerable to eavesdropping [5]. Even with their efficacy, current security protocols still contain serious vulnerabilities that are being used every day.

The influence of current cryptography algorithms on latency is one of the main problems. Voice packet processing can be slowed down by methods like encryption and decryption, which can raise latency and lower call quality. Furthermore, by introducing issues like packet loss and jitter into the network, firewalls and other security measures can adversely affect the Quality of Service (QoS) of VoIP calls [6]. The usefulness of some VoIP-specific security measures, like media encryption, to avoid eavesdropping may be limited if they are incompatible with other VoIP system types. This is especially true if hackers are able to take advantage of security flaws or exploit system vulnerabilities [7].

An injection approach known as artificial noise (AN) has been developed to secure wireless transmissions. It stops the eavesdropper from decoding the secret communication meant for the authorized recipient by concurrently conveying data symbols and artificial disturbance [8]. This method decreases the eavesdropper's signal reception by creating AN in the null space of the targeted receiver's channel and radiating it isotopically. Even in the absence of the eavesdropper's Channel State Information (CSI), the AN-aided security system ensures a non-negative secrecy rate for the authorized transmitter-receiver pair. In wireless transmissions, this method successfully preserves confidentiality [8,9].

In this work, the Amplify and Forward (AF) relay technique is used. Relays are devices that have the capacity to receive a signal and then retransmit it. They are based on the current amplify and forward relay system with modifications in which jamming (noise) is used to shield communication between the source and destination from interference or monitoring from an eavesdropper.

Related Works

In the related works, there have been a handful of methods for Rayleigh fading infrastructure-based communications. The authors in [10] created a framework for analysis to examine the likelihood of eavesdropping attacks in wireless networks with channel randomization. Specifically, the Rayleigh fading effect, the shadow fading effect, and the path loss effect. [11] addresses the security concerns of the Internet of Things (IoT) by presenting a novel analytical model specifically designed to investigate eavesdropping attacks in Wireless Network of Things (WNoT). The proposed model considers various channel conditions, including path loss, shadow fading, and Rayleigh fading effects. In [12] the study investigates Wyner's wiretap model's performance in vehicle communications networks' double Rayleigh fading channels' physical layer secrecy. It develops closed-form formulas, accounts for fading, path loss, and eavesdropper location uncertainty, and uses simulation for numerical evaluation [13].

The authors developed a model to optimize data packages for UAV 19 under power constraints, focusing on Weibull fading

DOI: 10.56892/bima.v8i3B.849

channels. They found that power consumption increases over time, regardless of distance. They recommend linear programming for jamming strength and consider the topology of a semicircle between approved and suspect UAVs. Four popular fading models were used to analyze performance. [14] studied improving physical layer security in wireless sensor networks using traditional key-based cryptographic techniques. They created a protective region to restrict active eavesdropper locations, using hybrid outage probability as a security metric. The study also examined the multiple-input single-output (MISO) system [15]. This research explores a new wireless security problem by proposing a proactive eavesdropping plan using a spoof relaying approach. The plan uses a legitimate monitor as a full-duplex relay, optimizing transmit precoding matrix and receive power splitting ratios. This approach significantly improves information surveillance performance.

MATERIALS AND METHODS

A new security model for VoIP channels is developed, incorporating Rayleigh fading channel PDF, artificial noise, and relays. A comprehensive simulation was conducted using MATLAB R 2020a, evaluating secrecy capacity and throughput. The model aims to provide a reliable and efficient method for safeguarding VoIP communications.

Development of Improved Security Model with Relaying Over Rayleigh Fading Channel.

The security model uses an existing amplify and forward relay system with modifications to protect communication between the source and destination from interference or monitoring from an eavesdropper. Relays receive and retransmit signals, increasing signal quality and extending communication range. The PDF of the Rayleigh fading channel is used to improve signal quality by increasing the signal-to-noise ratio, making it easier to detect and interpret at the receiving end. Artificial noise produced in the null space between the relay and eavesdropper is also analyzed to determine the appropriate noise level to disperse throughout the system. The complete developed improved security model with forward and amplify relaying scheme is shown in Figure 1.

Relay Selection Technique Based on SNR Threshold Approach

In cooperative relay network, the selection of the distributed relays is based on the number of relay nodes between the source and destination nodes. In this research, amplify and forward single relay threshold-based relay selection technique was adopted. This proposed relay selection technique is based on the received instantaneous SNR at each particular relay, this idea improves the quality of the received and transmitted signal as well as to decrease the power consumption of the relay. The selection of the relay based on the fixing the threshold of SNR and tested to select the relay with high SNR that met the threshold criteria. The steps for the proposed model are as follows [16]:

Step 1: the relay within the coverage area received the signal from the source

Step 2: signal to noise ratio is set at the relay (γ_{iT}) based on amplify and forward method

Step 3: the relay amplifies and forward the source signal if the threshold SNR (γ_{iT}) at the relay is less than the instantaneous SNR(γ_{sr}). Otherwise, it will be in sleep mode.

Step 4: if the condition in step 3 is not satisfied, the source signal is detected at the destination through direct link.

The improved relaying scheme with jamming block diagram shows that a source node sends

DOI: 10.56892/bima.v8i3B.849

a signal to a relay node, which amplifies it and injects fake noise to mask it. The relay node then sends the enhanced signal to the destination node, marking the possible eavesdropper zone that the jamming is intended to prevent.

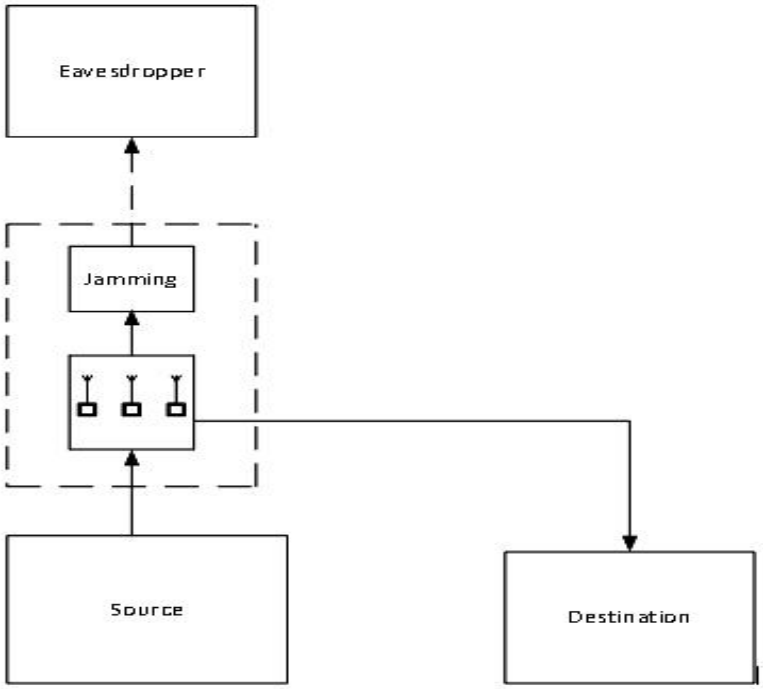

Figure 1: Diagram of the improved developed relaying scheme model with jamming.

The received signal from the source by the relay is given as:

$$y_{SRi} = \sqrt{P}h_{SRi}x + n_{SRi} \quad (1)$$

$$y_{SD} = \sqrt{P}h_{SD}x + n_{SD} \quad (2)$$

Where, h_{SRi} referred to as the path gain between the source and the relay, while and h_{SD} is denoted as the path gain between source to destination. The AWGN is denoted as n_{SRi} and n_{SD} for the relay and destination respectively. The transmitted symbol is denoted as x.

The source signal is amplified and forward by the relay with highest SNR (relay with SNR greater than the γ_{iT}) by scaling the power of the received signal with an inversely proportional factor to the power as in equation (3);

$$\beta_r = \frac{\sqrt{P}}{\sqrt{p|h_{SRi}|^2+N_0}} \quad (3)$$

At the destination, the total SNR is the sum of SNR from the relay and source links. Each of the SNR can be computed as [16]:

SNR at the relay

$$y_{Ri,D} = \frac{\sqrt{P}}{\sqrt{p|h_{S,Ri}|^2+N_0}} + h_{Ri,D}y_{s,ri} + n_{Ri,D} \quad (4)$$

DOI: 10.56892/bima.v8i3B.849

While, that of source is

$$\gamma_{s,D} = \frac{p}{N_0}\left|h_{S,Ri}\right|^2 \quad (5)$$

Where, $h_{Ri,D}$ donates the channel coefficient from the relay to the destination

Substituting (1) and (5)

$$y_{Ri,D} = \frac{\sqrt{P}}{\sqrt{p\left|h_{S,Ri}\right|^2+N_0}} + h_{Ri,D}y_{s,ri}(\sqrt{P}h_{SRi}x + n_{SRi}) + n_{Ri,D} \quad (6)$$

$$y_{Ri,D} = \frac{\sqrt{P}}{\sqrt{p\left|h_{S,Ri}\right|^2+N_0}} + h_{Ri,D}y_{s,ri}\sqrt{P}h_{SRi}x + \acute{n}_{Ri,D} \quad (7)$$

$$\acute{n}_{Ri,D} = \frac{\sqrt{P}}{\sqrt{p\left|h_{S,Ri}\right|^2+N_0}} + h_{Ri,D}n_{SRi} + n_{Ri,D} \quad (8)$$

The terms n_{SRi} and $n_{Ri,D}$ that are represented as noise terms are assume to be independent, the noise $\acute{n}_{Ri,D}$ is equivalent to complex Gaussian random variable with a zero mean and variance

$$\acute{N}_0 = N_0\left(\frac{p\left|h_{Ri,D}\right|^2}{p\left|h_{S,Ri}\right|^2+N_0} + 1\right) \quad (9)$$

N_0 is denoted as the power spectral density of AWGN in (W/Hz)

At the destination, the instantaneous SNR is given by

$$\gamma_D = \gamma_{S,D} + \sum_{i=1}^{N}\frac{\gamma_{S,Ri}\gamma_{Ri,D}}{\gamma_{S,Ri}\gamma_{Ri,D}+1} \quad (11)$$

The instantaneous SNR from source to destination is given as:

$$\gamma_{S,D} = \frac{p\left|h_{S,D}\right|^2}{N_0} \quad (12)$$

While, the instantaneous SNR of from source to with relay is given as:

$$\gamma_{S,Ri} = \frac{p\left|h_{S,Ri}\right|^2}{N_0} \text{ and} \quad (13)$$

$$\gamma_{Ri,D} = \frac{p\left|h_{Ri,D}\right|^2}{N_0} \quad (14)$$

is the instantaneous SNR of the relay to destination. [16].

Simulation of the Developed Model

The simulation model consists of two sections. The first section uses a random generator to generate input for a QPSK modulator, mapping input bits into complex symbols with four phase shifts. An AWGN channel introduces random noise to simulate real-world communication channel effects. A QPSK demodulator recovers original symbols from the noisy signal, and the demodulated symbols are used to calculate error rates. The second section connects to a 64-QAM modulator for higher data rates. A noise generator adds artificial noise to the modulated

DOI: 10.56892/bima.v8i3B.849

signal, which is transmitted through a Multipath Rayleigh Fading Channel. The simulation process is connected for comparison and analysis. The flowchart of the simulation process and the simulation parameters used are presented in Figure 2 and Tables 1 respectively.

Table 1: System simulation parameters for the developed model

Parameter	Specifications
Number of bits	256
Bandwidth	16bps
Frequency	4Hz
Number of subcarriers	64
Symbol interval (X^{-n})	3
SNR	10

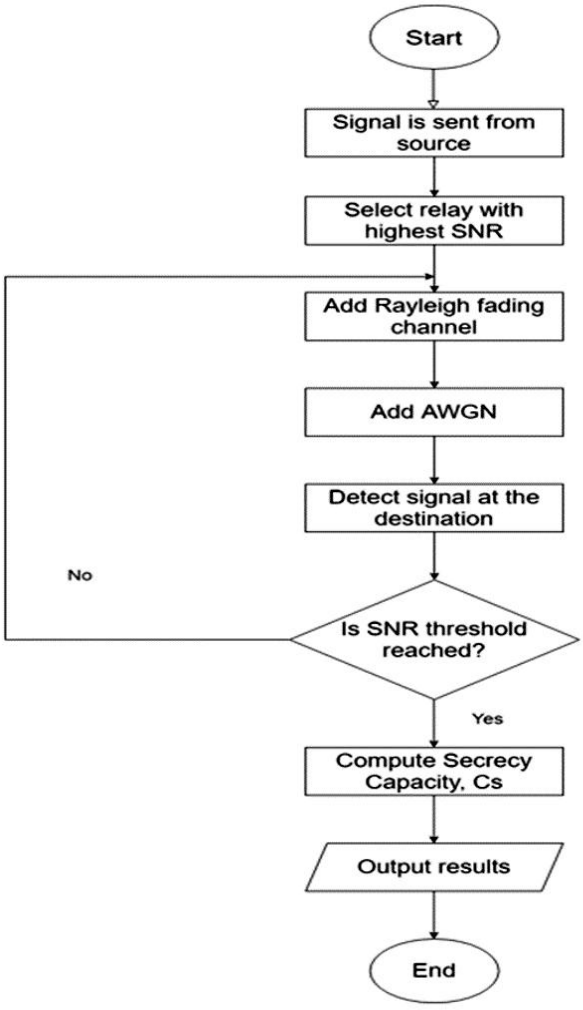

Figure 2: Flowchart of the simulation system model

Mathematical Expression for Received Signal and SNR at the Eavesdropper for the Developed Model

The signal at the destination of the developed model is a combination of the transmitted signals from the source to the relay, weighed by their respective fading coefficients, added with the AWGN in the channel between the relay and the destination.

DOI: 10.56892/bima.v8i3B.849

The signal received at the eavesdropper equation is modified and expressed as:

$$h_E = G_O\sqrt{P_S P_{Ri}}\left(\frac{h_{SRi}h_{RiE}}{{h_{SRi}}^2+{h_{RiE}}^2}\right)X_{Ri} + \frac{h_{RiE}}{{h_{SRi}}^2+{h_{RiE}}^2}\sqrt{P_{Ri}}\,N_E + G_O\sqrt{P_{Ri}}\,h_{RiD}\,N_{Ri} + \sqrt{P_{Ri}}\,h_{RiE}\,W_Z \quad (15)$$

where:

h_{SRi} is the fading coefficient from the source to the relay.

h_{RiE} is the fading coefficient from the relay to the eavesdropper.

X_{Ri} is the signal being relayed.

N_E is the AWGN at the eavesdropper.

N_{Ri} is the AWGN at the relay.

W_Z is the AN created in the null space between the relay and eavesdropper.

The modified SNR at the eavesdropper can be calculated by using the received signal at the eavesdropper and the total noise power.

$$\gamma_E = \frac{P_S\,P_{Ri}\,{G_O}^2\,{h_{SRi}}^2\,{h_{RiE}}^2}{\left({h_{RiD}}^2\,{h_{RiE}}^2\right)+\left({h_E}^2\,{h_{RiE}}^2\right)+\left(P_{Ri}{h_E}^2{G_O}^2\right)+\left({h_{RiE}}^2\,P_D\right)+\left(h_{RiD}\,P_D\right)} \quad (16)$$

where P_D is the power of the AWGN added to the signal in the channel between the source and the eavesdropper [17].

Performance Metrics

The metrics for evaluating the developed model are evaluated using SNR, secrecy capacity and throughput.

Mathematical expression for received signal and SNR at the destination for the developed model

If the fading coefficients follow a Rayleigh distribution, the probability density function (PDF) of h_{RiD} and h_{SD} can be expressed as:

$$f(h_{RiD}) = \left(\frac{h_{RiD}}{{\sigma_{RiD}}^2}\right)\exp\left(\frac{-h_{RiD}}{2{\sigma_{RiD}}^2}\right) \quad (17)$$

$$f(h_{SD}) = \left(\frac{h_{SD}}{{\sigma_{SD}}^2}\right)\exp\left(\frac{-h_{SD}}{2{\sigma_{SD}}^2}\right) \quad (18)$$

By incorporating these PDFs into the signal equation (19) and simplifying, we get the signal received at the destination of the developed model as in (20):

$$h_D = G_O\sqrt{P_S P_{Ri}}\,h_{RiD}X + \sqrt{P_{Ri}}h_{SD}X_{Ri} + N_D \quad (19)$$

$$h_D = G_O\sqrt{P_S\,P_{Ri}}\,\frac{h_{SD}\,h_{RiD}}{\left({h_{SD}}^2+{h_{RiD}}^2\right)^2} + \frac{h_{RiD}}{{h_{SD}}^2+{h_{RiD}}^2}\sqrt{P_{Ri}}\,N_D\,X \quad (20)$$

Where:

G_O is the linear amplified version of the received signal.

h_{SD} is the fading coefficient from source to destination.

h_{RiD} is the fading coefficient from the relay to the destination.

N_D is the AWGN added to the signal in the channel between the relay and destination.

The SNR at the destination in equation is modified and be expressed as:

$$= \frac{P_S\,P_{Ri}\,{G_O}^2\,(h_{SD}\,h_{RiD}\,)^2}{P_{Ri}\,{h_{RiD}}^2+{\sigma_{Ri}}^2+{\sigma_D}^2+P_S\,P_{Ri}\,{h_{SD}}^2} \quad (21)$$

DOI: 10.56892/bima.v8i3B.849

Mathematical expression for received signal and SNR at the eavesdropper for the developed model

The signal at the destination of the developed model is a combination of the transmitted signals from the source to the relay, weighed by their respective fading coefficients, added with the AWGN in the channel between the relay and the destination.

The signal received at the eavesdropper in equation is modified and expressed as $h_E = G_O\sqrt{P_S P_{Ri}}\left(\frac{h_{SRi}h_{RiE}}{{h_{SRi}}^2+{h_{RiE}}^2}\right)X_{Ri} + \frac{h_{RiE}}{{h_{SRi}}^2+{h_{RiE}}^2}\sqrt{P_{Ri}}\,N_E + G_O\sqrt{P_{Ri}}\,h_{RiD}\,N_{Ri} + \sqrt{P_{Ri}}\,h_{RiE}\,W_Z$ (22)

where:

h_{SRi} is the fading coefficient from the source to the relay.

h_{RiE} is the fading coefficient from the relay to the eavesdropper.

X_{Ri} is the signal being relayed.

N_E is the AWGN at the eavesdropper.

N_{Ri} is the AWGN at the relay.

W_Z is the AN created in the null space between the relay and eavesdropper.

The modified SNR at the eavesdropper can be calculated by using the received signal at the eavesdropper and the total noise power as [19]:

$$\gamma_E = \frac{P_S\,P_{Ri}\,{G_O}^2\,{h_{SRi}}^2\,{h_{RiE}}^2}{\left({h_{RiD}}^2\,{h_{RiE}}^2\right)+\left({h_E}^2\,{h_{RiE}}^2\right)+\left({P_{Ri}}{h_E}^2{G_O}^2\right)+\left({h_{RiE}}^2\,P_D\right)+\left(h_{RiD}\,P_D\right)} \quad (23)$$

where $\boldsymbol{P_D}$ is the power of the AWGN added to the signal in the channel between the source and the eavesdropper [18].

Secrecy Capacity for the developed model

The mathematical expression for secrecy capacity for the developed model is modified by substituting the values of γ_D and γ_E into some equations, the secrecy capacity of the system can be written as:

$$C_S = \frac{1+\frac{P_S\,P_{Ri}\,{G_O}^2\,\left(h_{SD}\,h_{RiD}\right)^2}{P_{Ri}\,{h_{RiD}}^2+{\sigma_{Ri}}^2+{\sigma_D}^2+P_S\,P_{Ri}\,{h_{SD}}^2}}{1+\frac{P_S\,P_{Ri}\,{G_O}^2\,{h_{SRi}}^2\,{h_{RiE}}^2}{\left({h_{RiD}}^2\,{h_{RiE}}^2\right)+\left({h_E}^2\,{h_{RiE}}^2\right)+\left({P_{Ri}}{h_E}^2{G_O}^2\right)+\left({h_{RiE}}^2\,P_D\right)+\left(h_{RiD}\,P_D\right)}} \quad (23)$$

RESULTS AND DISCUSSION

In this work, the performance of the developed system model was evaluated based on the secrecy capacity and the signal to noise ratio. A comprehensive simulation was conducted using MATLAB R 2020a version. The simulations were run on computing machine with a 64-bit operating system, an Intel(R) Core (TM) i3-8130U CPU running at 2.20GHz, and 12.0GB of RAM was used to run the simulations. This configuration guaranteed adequate processing power for the taxing simulations

Figure 3 displays the outcomes of the secrecy capacity (SC) versus signal-to-noise ratio (SNR) analysis conducted for the developed and existing models at the destination and eavesdropper, respectively. The SNR and linearly amplified signal were varied, with G_O set to 2 and SNR set to 20. The SC values obtained for the developed model at the destination are 0.3471, 0.4904, 0.6019, and eavesdropper 0.257, 0.3664, and 0.4545, at SNR of 2, 6, and 10 dB respectively as against the conventional model destination values, which are 0.298, 0.4355 and 0.5466, and eavesdropper values, which are 0 .257, 0.3644

DOI: 10.56892/bima.v8i3B.849

and 0.4545 at SNR 2, 6 and 10 dB respectively. The results reveal that as the SNR increases, the secrecy capacity at the destination also increases, indicating an enhancement over the conventional model. The developed model demonstrates superior performance in terms of secrecy capacity.

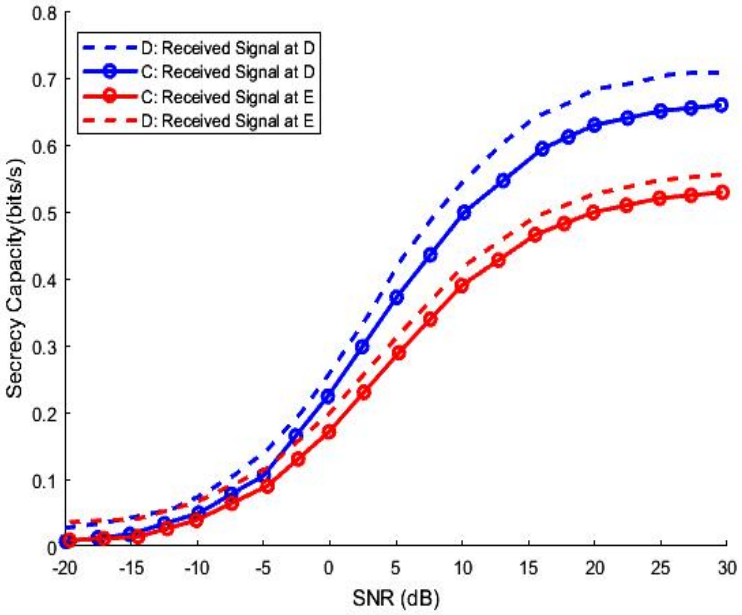

Figure 3: Secrecy versus signal to noise ratio graph

Figure 4 illustrates the SC versus SNR for the existing and developed models at the destination and eavesdropper, respectively. In this case, the values of G_0 and SNR were varied, with G_0 set to 4. The SC values obtained for the developed model at the destination are 0.4483, 0.5650, 0.6605, and eavesdropper 0.3359, 0.4364, and 0.5122, at SNR of 4, 8, and 12 dB respectively as against the existing model destination values, which are 0.3720, 0.4990 and 0.5942, and eavesdropper values, which are 0.2892, 0.3897 and 0.4655 at SNR 4, 8 and 12 dB respectively. The graph shows that the developed model improves communication quality by delivering a higher signal at the destination, resulting in a higher secrecy capacity, thereby facilitating more efficient transmission of confidential information compared to the existing model.

Figure 5 depicts the SC versus SNR graph for the developed and existing models at the destination and eavesdropper, respectively. The values of G_0 and SNR were varied, with G_0 set to 6 and SNR set to 20. The SC values obtained for the developed model at the destination are 0.7226, 0.7439, 0.7651, and eavesdropper 0.5698, 0.5865, and 0.6077, at SNR of 14, 16, and 20 dB respectively as against the existing model destination values, which are 0.6118, 0.6295 and 0.6506, and eavesdropper values, which are 0.4822, 0.4990 and 0.5202 at SNR 14, 16, and 20 dB respectively. Based on the observations, it can be deduced that an increase in the SNR leads to a corresponding increase in the SC at the destination, surpassing that of the existing model. In contrast, at the eavesdropper, an increase in SNR results in a greater presence of noise or absence of useful information, even more so than in the existing model. This boost in SNR contributes to a higher secrecy capacity at the destination, indicating that the

DOI: 10.56892/bima.v8i3B.849

developed model outperforms the existing model in terms of reliable and secure communication. The heightened secrecy capacity signifies an improved ability to transmit confidential information efficiently. Furthermore, the increase in the eavesdropper's reception with rising SNR signifies enhanced security. The developed model achieves a lower signal reception at the eavesdropper compared to the existing model. Consequently, the developed model effectively reduces the interception of information by unauthorized listeners, thereby bolstering the overall security of the system.

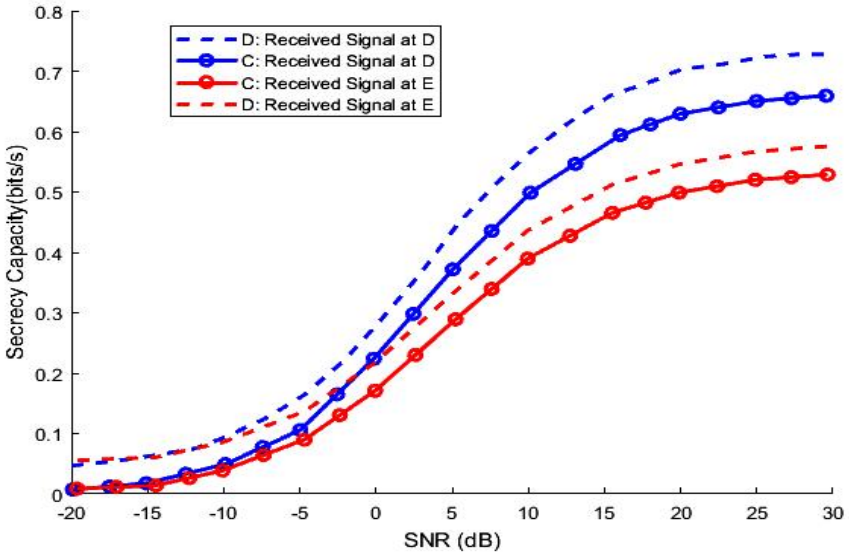

Figure 4: Secrecy versus signal to noise ratio graph

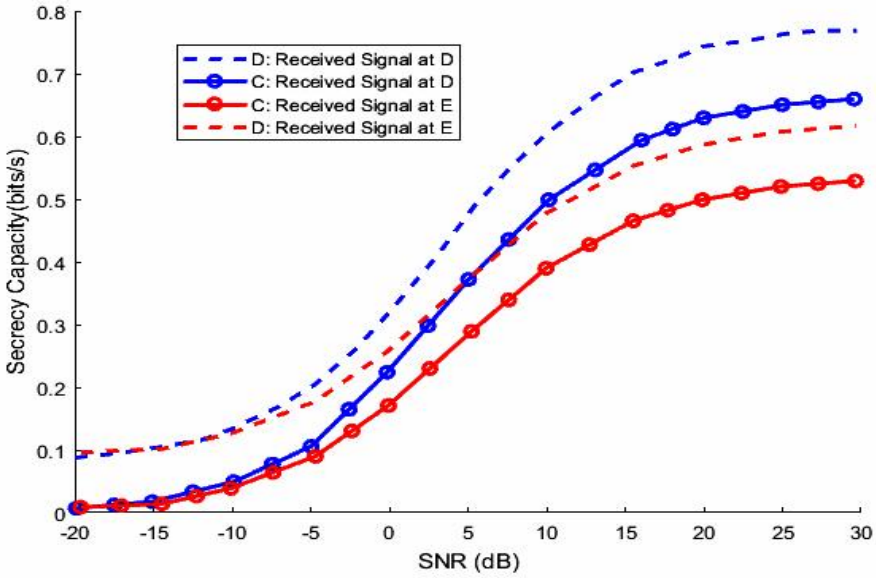

Figure 5: SC versus SNR graph when G_O= 6

DOI: 10.56892/bima.v8i3B.849

CONCLUSION

The developed security model has been implemented, and artificial noise has been added to calls as a form of precaution from eavesdropping. The system was developed by incorporating relays between the source and destination, to transmit VoIP calls, with AN produced in the null space between the relay and the destination, so as to prevent the AN from degrading the signal quality that will be received at the destination. Mathematical expressions for the received signal, eavesdropper signal, was derived using PDF. The PDF was employed to derive SNR at the destination and eavesdropper, which made up SC. These were used to evaluate the performance of the developed model by comparing it to the signal received at the destination and eavesdropper of the existing model.

REFERENCES

[1] Muhammad Zulkifl Hasan, M. Z. (2017). Collective Study on Security Threats In voip. International journal of scientific & technology research. 6(01), 20-23.

[2] Johanson Miserigodiasi Lyimo, (2023). Implementing a campus VoIP intercom VLAN: A technology review, system requirements and architecture. International Journal of Science and Research Archive, 09(02), 716–726.

[3] Saminu, S. Jabire, A.H. Ahmed, Y.K. Jajere, A.M. Ahmad, I.S. (2021). Performance Comparison of Transmit and Receive Diversity under Rayleigh Faded Channel Using Extended Alamouti's Scheme. Journal of Science Technology and Education. 9 (1); 257-269.

[4] Suthar, D. (2020). A Comprehensive Study of VoIP Security. International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). 812-817.

.[5] Peng and S. Tang, (2021). Covert communication over VoIP streaming media with dynamic key distribution and authentication, IEEE Trans. Ind. Electron., 68(4), 3619-3628.

[6] Lazzez, A. (2014). Securing VoIP Systems: A QoS- Securing VoIP Systems: A QoS-Oriented Oriented. IJCSI International Journal of Computer Science Issues, 11.

[7] Jabire, A. H. Salisu, S. Saminu, S. Jajere, M. A. Hussein, M. I. (2023). A crossed-polarized four port MIMO antenna for UWB communication. Heliyon. 9, (2023), e12710.

[8] Wu, F., Wang, W., Yao, B., & Yin, Q. (2013). Effective eavesdropping in the artificial noise aided security scheme. 2013 IEEE/CIC International Conference on Communications in China (ICCC). Xi'an, China, 2013, 214-218.

[9] Saminu, S. Jabire, A.H. Abdulkarim, A. Ahmed, Y.K. and Iliyasu, A.Y. Salisu, S. Karaye, I.A. Ahmad, I.S. (2021): Performance Analysis of Transmit Diversity Configurations Based on OSTBC Alamouti's Extension. Zaria Journal of Electrical Engineering Technology. 10 (1); 1-11.

[10] Xuran Li, Hao Wang, Hong-NingDai, Yuanyuan Wang, and Qinglin Zhao. (2016). An analytical Study on Eavesdropping Attacks in Wireless Nets of Things. Mobile Information Systems, 2016, Article ID 4313475, 10 pages.

[11] Xu, J., Duan, L., & Zhang, R. (2015). Proactive Eavesdropping via Jamming for Rate Maximization over Rayleigh Fading Channels. IEEE Wireless Communications Letters, 5(1), 80-83.

DOI: 10.56892/bima.v8i3B.849

[12] Yun, H., & Joung, J. (2021). Design of the power and dimension of artificial noise for secure communication systems. IEEE Transactions on Communications, 69(6), 4001–4010.

[13] Xiaoming Wang, Demin Li, Chang Guo, Xiaolu Zhang, Salil S. Kanhere, Kai Li, Eduardo Tovar. (2019). Eavesdropping and Jamming Selection Policy for Suspicious UAVs Based on Low Power Consumption over Fading Channels. Sensors. 19(5), 1126.

[14] Tao Li, Chaozheng Xue, Yongzhao Li and Octavia A. Dobre. (2020). Defending Against Randomly Located Eavesdroppers by Establishing a Protecting Region. Sensors. Sensors 2020, 20(2), 438.

[15] Zhou, N. R., Liang, X. R., Zhou, Z. H., & Farouk, A. (2016). Relay selection scheme for amplify-and-forward cooperative communication system with artificial noise: Relay selection scheme for amplify-and-forward cooperative communication system with artificial noise. Security and Communication Networks, 9(11), 1398–1404.

[16] Kumarapandian, Shamganth, (2021). Threshold-Based Relay Selection for Cooperative Wireless Network. Doctoral thesis, University of Huddersfield. http://eprints.hud.ac.uk/id/eprint/35519/

[17] Brian Dunn and J. Nicholas Laneman. (2005). Characterizing Source-Channel Diversity Approaches Beyond the Distortion Exponent University of Notre Dame Dept. of Electrical Engineering Notre Dame, IN 46556

[18] Zhao, J., Bai, J., Zhang, Q., Yang, F., Li, Z., Zhang, X., Zhu, X., & Bai, R. (2018). The discussion about mechanism of data transmission in the OSI model. Proceedings of the 2018 International Conference on Transportation & Logistics, Information & Communication, Smart City (TLICSC 2018).

[19] Xiao Jiang, Peng Li, Bin Li, Yulong Zou, Ruchuan Wang (2022). Secrecy performance of transmit antenna selection for underlay MIMO cognitive radio relay networks with energy harvesting. IET Communications. 16(3), 227-245.