International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I7P250

Volume 70 Issue 7, 479-490, July 2022

Original Article

A Reliable and Secure Inter-And Intra-State Routing Protocol for VoIP communication

Vinod Kumar[1], Om Prakash Roy[2]

[1,2]*Department of EE, North Eastern Regional Institute of Science and Technology, Nirjuli – 791109, Arunachal Pradesh, India.*

[1]*vinodnerist@gmail.com*

Received: 19 May 2022 Revised: 10 July 2022 Accepted: 14 July 2022 Published: 30 July 2022

Abstract *- Technological advancements increase the demand for communication over a reliable Voice over Internet Protocol (VoIP) network. The data communication in such a network is often attacked by intruders, which requires the implementation of a secure system for transmission. This paper presents a robust data communication network in which the proposed structure consists of two block architectures: Inter-State Routing (INTER-SR) and Intra State Routing (INTRA-SR). This architecture handles the data communication for the intra-structure route, and the INTRA-SR block handles inter structure route and data communication over a network. The proposed work focuses on constructing the deployment model using the distance formula to attain appropriate route discovery by considering 60 nodes. The inter-state architecture is developed using the interpolation structure and Neural Network to classify the nodes. Further comparison is performed with the approach such as a support vector machine (SVM). The outcome is simulated, considering the classification accuracy, throughput, and packet delivery ratio (PDR) rate to determine its robustness. The network's reliability is tested by improvement in the throughput and the PDR, taking a ratio of how many nodes are accepted to be in the network. It is observed that the throughput increases significantly when there is an increase in the reliable nodes, whereas the PDR is radical. The results show that the PDR rate improved by 15% and the throughput rate revamped by 21% compared to other classification approaches*.

Keywords *- Neural Network, Reliability, Security, Support Vector Machine, VoIP*.

1. Introduction

Technology has changed the way of living of human beings. More precisely, the data-driven approaches to technological advancements have made human life attractive and straightforward. VoIP is one of the examples of data-driven technological advancements in the world and gained a lot of consumer base due to its cheap and effective services. Such a system is based on internet protocol and is used worldwide for multimedia communication. It is viewed as a network with several communicating nodes and associated attributes. Different types of protocols are responsible for multimedia communication connections in this technology. In VoIP networks, codecs are an integral part of the communication system and convert data from analog to digital and vice versa [1, 2]. The basic components of the VoIP network are shown in figure 1.

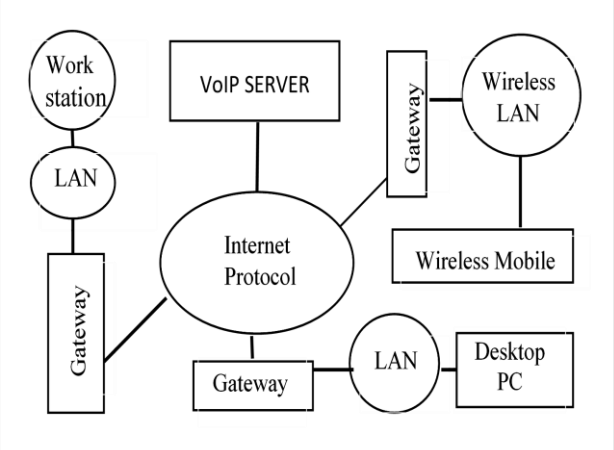


Fig. 1 Basic Components of a VoIP Network

VoIP is becoming a part of security applications, such as satellites carrying humans with VoIP services. Traditional security approaches are not up to the mark to handle VoIP networks and getting misused by making prank calls or by making calls for organizational promotions.

In [3], the authors focused on designing the VoIP network for security-related problems. The experimental study of authors in [4] shows that the suggested framework achieves considerably higher detection accuracy than present progressive detection schemes. Due to the expansion of VoIP technology in business communications, intruders are concentrating on fraud activities. The researchers found

higher accuracy with flood attacks but failed to discover spam calls. The accuracy of F-SVM (a combination of feature transformation and SVM) was observed to be low for harmonic attacks. To handle the delay-related applications with requirements of no error, reliability, and security for data packets is most important. These applications are in the area of military, disaster, medical diagnosis, etc.

The problem of node's unusual behavior due to attack and packet missing is very difficult [5]. Trusted routing needs to be developed to support a reliable environment as the intruders are generally more fond of internet of things (IoT) related networks such as VoIP due to easy access. Studying different tactics used by intruders for attacks is very important [6]. Most of the VoIP protocol architecture uses internet protocols version 6 (IPv6) communication for faster data transfer, reducing the security breach in data communication. As compared to IPv4, IPv6 is comparatively new and popular for security. Designing useful tools for IPv6 and machine learning techniques such as SVM and principal component analysis (PCA) need more testing for attacks based on IPv6. Machine learning techniques presently being used in IPv4-based networks is not applicable for detecting attack such as router advertisement (RA). RA attacks overlook the methods of IPv6 [7]. Identification of several new routing protocols is developed from time to time but is not found useful in vehicular ad hoc network (VANET) cases. When these protocols are applied for mobile ad hoc networks (MANET), performance, PDR, and packet delay are minimized. Mobile communication is not limited to voice and video sessions but has become multifunction power full of entertaining, file sharing, financing, etc. Accordingly, the telephony infrastructure, VoIP, transformed into a multimedia communication system not limited to the multifunctional device but a piece of low-cost equipment for international and multi-branch voice communication systems [8].

Communication worldwide is diverting towards VoIP without any security measures. It is easy in old switched-based networks for call management and connections between telephones compared to internet protocol (IP) based telephone network that operates with hundreds of calls. Confidentiality, integrity, and availability (CIA) is a security model accepted by society globally. Confidentiality means mechanisms that make sure that solely authorized individuals access secure information. Integrity refers to no alteration of the information. Availability refers to the time for which services remain operational [9].

The main idea of this research work is to enhance the architecture of machine learning by introducing a two-phase mechanism for intra-structure routing and an interpolation architecture for inter-state routing. The structure of the paper is initialized with an introduction. Related works with the necessary technique used by different researchers and necessary findings are presented in the form of a literature review in the second section. The third section explains the methodology, including block architecture, pseudo code, ordinal measures, and algorithm. The outcome of the results with necessary discussion is explained in the fourth section as results and analysis. Finally, the paper is concluded with future scope.

2. Literature Review

Mobile devices are increasing in numbers due to their powerful service to society. To reduce the load imbalance in load distribution for VoIP traffic and quality of service (QoS), improving the processing of incoming packets from multimedia internet protocol traffic becomes very important. If the route structure is not designed well, issues like data redundancy, line jamming, and line aggregation are faced. The authors in [10] proposed a packet scheduler, which distributes the load among the nodes in VoIP using machine learning architecture. Machine learning is used for efficient routing configuration for network engineers. Software-defined networks (SDN) can repeatedly calculate routing configuration within a short time. The authors in [11] also view the VoIP as an SDN and use machine learning for packet routing and security analysis measures. Packet scheduling is a part of appropriate routing, and QoS parameters must be considered. A cisco standard for network availability named Host Standby Routing Protocols (HSRP) is designed for data redundancy.

In [12], the authors applied open shortest path fast (OSPF) routing and presented an architecture that reduces the data redundancy and manages line aggregation for VoIP. Usage of machine learning is also observed in VoIP for routing and security purposes. The device used for the local area network (LAN) as a gateway to nodes is very important. The technical terms used in VoIP, such as bandwidth, delay, and codec, are responsible for the high quality of communication between network devices. The author in [1] discussed the VoIP protocols and presented telephony routing and network issues. Deep learning with arrays of sigmoidal neurons is becoming popular due to overcoming neural network problems during real-life challenges. A model is proposed in [13] based on deep learning by considering larger networks and hundreds of cells. The models based on Artificial Neural Networks (ANN) are also being used to analyze videos and voice quality. Due to the involvement of cost and time factors, it is impossible to provide a high level of services [14, 15] proposed machine learning-based classifiers for traffic control. Firstly evaluated multiple service channel analysis, secondly identified features to get high accuracy, after that probability of trained models, and finally, it analyzed data for benchmarking. In [16] employed feed-forward artificial neural network (FFANN) for approximation of a function f*. A classifier b = f*(a) gives input a to category b, and A FFANN defines b = f (a; Ɵ) for learning value of the parameters Ɵ resulting function approximation.

The main goal of the neural network is to reduce the errors and the backpropagation method to train feed-forward networks. The author in [17] took into account four learning rate values: 0.1, 0.3, 0.6, and 0.9. The backpropagation is empowered by including a momentum term for helping the initial stage of the algorithm. Neural networks (NN) trained with a backpropagation algorithm are called back propagation neural networks. In [18], assume a homogeneous sequence system to observe anomalies by comparison. The classification procedure is considered with the detection and training phases and uses multi-layer feed-forward ANNs, to train the network and with a backpropagation algorithm [19]. Levenberg–Marquardt (LM) algorithm using feed-forward ANNs tested for approximating a function problem. It is an efficient MATLAB implementation because of built-in matrix functions. Hidden Markov Model (HMM) demand is increasing because of learning and prediction.

To collect the QoS-related values, a measuring framework is set up based on Markov Model with evaluation reconstruction and learning phases. The First phase of evaluation is related to computation probability, the second finding a similar sequence of hidden states, and the final phase to find the sequence of state transition with output probabilities [20, 21] using speech enhancement algorithms with objective speech quality metrics (OSQM) for speech signal by using machine learning classifier and found with the 30 samples for every class result training classifier has low classification accuracy. ANNs are used for a huge number of applications and clustering problems. Machine learning technique such as decision tree is mostly applied for getting higher classification accuracy and fraud detection for VoIP [22]. In the field of Machine learning, the Grey wolf optimization (GWO) approach was already used in many areas of problem-solving but was found slow due to convergence and low graded output.

In [23], proposed inertia motivated GWO (IMGWO) to train ANN and apply in applied in the area of medical diagnosis [23]. The measurement was taken as mean squatted error and classification accuracies. Authors found it a good learning technique. In [24] tested, uniLoss on VoIP traffic shifted results to natural language processing. Further, the transport layer is selected as a payload for data packet input. UniLoss works better with neural networks, but more work is required, such as parameter selection. The user does not always have to want to hear the promotional message. HMM for dynamic voice spams is called intruders by using a set of features to train and classify HMM. Sometimes, it might be interesting to know the new events and offers, but in most cases, it is annoying. In [25], HMM and data accessed from Radio frequency identification (RFID) sensors were used to identify several activities such as tea making, bathroom use, phone call, meal making, eggs boiling, making juice, table cleaning, etc.

The protocol NLSR was developed in 2013 and was developed for intra-domain routing. The authors described NLSR by differentiating it from IP security and multipath routing protocols. NLSR is designed for a single domain but may help design an inter-domain routing in future implementation [26-28].

The routing protocols can be categorized as one inter-domain protocol and another intra-domain. The border gateway protocols are an example of inter-domain protocols. The author in [29] assumed gateway protocols that follow the shortest path routing. A weight is assigned to every link, and the shortest path from every origin to every destination is calculated considering the weight in place of the length of the links. In [30] defined insider attacks due to intrusion detection system (IDS) in incoming flow coming to the router sent back to its destination. The IDS approach is more acceptable by the industries due to the non-requirement of change in the routing protocols. But the author is limited to the protection of link state routing protocols and suggested new improvements in routing protocols using Delay Tolerant Network (DTN). Many workings for improvement of QoS are considered. But DTN being a challenged network, betterment of QoS is not possible [31, 32]. The mobile model was analyzed for the movement of the nodes. Distance between nodes is calculated using the received signal strength indication (RSSI) algorithm and used network simulator version 2 (NS2) for their VoIP system implementation [33-35]. The author in [36] presented an ad hoc VoIP network system with Global Positioning System (GPS) to observe gatekeeper connected and performed evaluation. The VoIP performance is examined with five codecs using IPv4, IPv6, and stream control transmission protocol (SCTP) [37 - 39]. The author analyzed QoS with experiments, proposed an algorithm for the effects of QoS, and applied a machine learning algorithm [40]. The QoS describes a qualitative measure of the precision, recall, accuracy, security, reliability, scalability, and availability of services. To maintain a higher service level for users, the reliability value must be between zero (0) and one (1) for error-free communication [41, 42].

3. Methodology

Security is essential for both inter and intra structure. Any undesired operation not relevant to the home network is termed an intrusion. An attack in which the attacker is from the outside of the home network, the intrusion is termed an internetwork intrusion. As shown in Figure 2(a), region R2 is an inter-region for R1 but an intra-region for R3. As security is at stake, the nodes serve in a given communication range and do not receive any data packet outside the communication range.

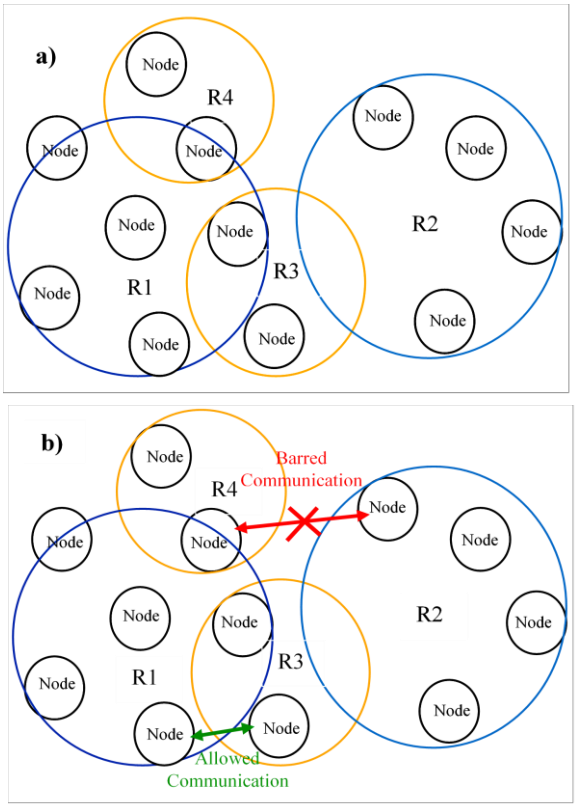


Fig. 2 Communication Range and Barred Communication

As presented in Figures 2 (a) and (b), each node in VoIP has a limited range of communication and has individual nodes in the communication range.

3.1. Proposed algorithm

The proposed algorithm is a two-block algorithm, namely INTER-SR and INTRA-SR, in which the INTRA-SR block handle the intra-structure route, and the INTER-SR block handles the inter-structure route and data communication. Figure 3 represents the proposed block architecture of INTER and INTRA-SR

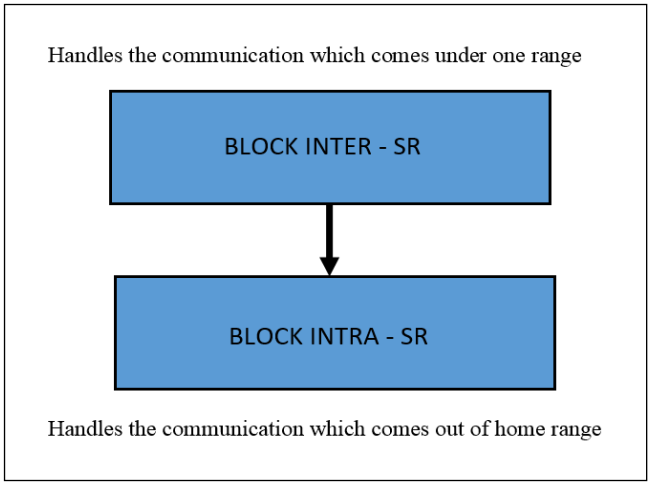


Fig. 3 Block Architecture of INTER INTRA-SR

3.2. Pseudocode

The data communication starts with user deployment in the network. A random deployment model is designed in which users are placed randomly in different regions. The pseudo code for deployment is as follows.

- For$_{each}$User in the User$_{List}$
- Generate Random X for the user
- Generate Random Y for the user
- Deploy

Once the nodes are deployed into the network, data packets are initialized, and the source node aims to hand over the data packet to its destination node. Coverage-based routing is performed if the destination node falls under the INTRA-SR block. The author in [43] used self-organizing algorithms based on the distance between nodes and energy consumption. In case of a node failure, the nearby node is important for re-considering the routes. The ordinal measures of routing are defined in Table 1. Using the distance formula, the source node computes the relative distance from every other node in the range. Let (x1, y1) be the GPS location of the source node and (x2, y2), (x3, y3), and (xn, yn) be the GPS location of the respective nodes.

Table 1. Ordinal Measures of Routing

No.	Measure Type	Description
1.	Total Node Count	30-60
2.	Range of Transmission	25 % of the total area according to 802.11
3.	Inter-Protocol Communication	IPv-6

The distance formula in Equation (1) calculates the distance between the nodes.

$$d = \sqrt{(x2 - x1)^2 + (y2 - y1)^2} \quad (1)$$

The source node looks for the most feasible node in the range by considering the load and the direction of transfer, as illustrated in Figure 4. In Figure 4(a), the source node had three options to transfer the data, but it selects the node towards the destination and checks whether it is overloaded. The selected node further follows the same procedure until the destination is not found. Regarding internode data transfer, the source node knew that the data packet must travel outside the boundary region.

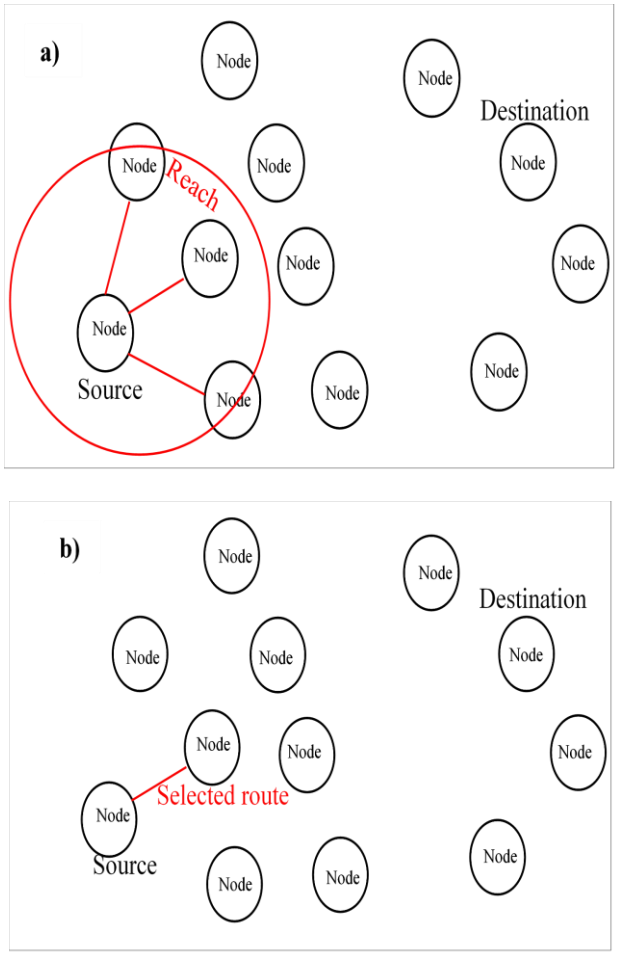


Fig. 4 Intra Route Discovery
(a) Reach of Nodes (b) Route Selection.

The researchers in [44] used Lagrange's interpolation method for route discovery when secret data transfers from source to destination. Research output revealed that integrating a covert channel in VoIP is a good security measure. Further, the security of VoIP traffic by analyzing user agents and discussing countermeasures remained the main idea.

The INTER-SR block uses it when it has to transfer the data from one region to another region. Any interpolation method works on two key values: share and network key. It is assumed that each region has its network key and a few nodes out of the total nodes in one region possess the share generated from the network key itself. If the network key is 7400, the shares are generated using the node id of the shareholder and two arbitrary constants, ‘a' and ‘b,' as mentioned in Equation (2).

$$Share_{value} = a + b \times node\ id + Network_{key} \qquad (2)$$

If the node id of the Share-Holder (SH) is 3 and the arbitrary constants are 1 and 2, then the share value would be 1+2×3+7400 = 7407.

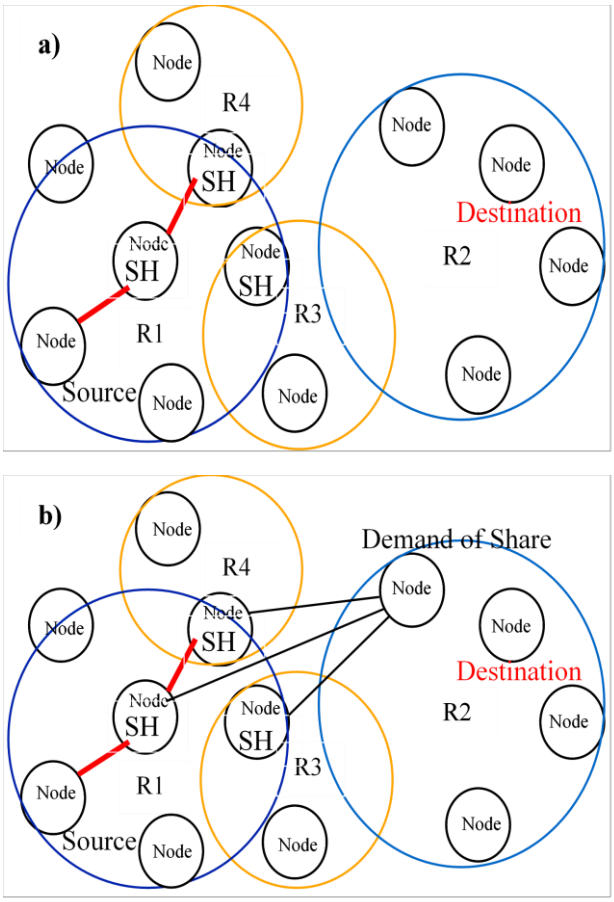


Fig. 5 Route Discovery and Inter Share Exchange

The node to be added in the respective path has to compute the network key utilizing the share value of the nodes. This process does not have to do repeatedly; once a node is verified, the node is kept in the trusted list until and unless the added node does not change its position beyond a given limit. Figure 5 (a) and (b) illustrate the process of (a) Inter Route Demand and (b) Inter Shares Demand

The demanding node uses the following Lagrange's interpolation in the following manner to evaluate the key of the network. Let there be 3 share values 7412, 7411, and 7432. The share calculation is based on Equation 2, which uses the network id and the share value.

For each share, the numerator and denominator have to be calculated. If the calculated share value is equal to the network key, then the node is added to the path and registered as a safe use for the entire network. The value of p in the case of proposed research work is 0.

$$Generated_{Key} = \frac{(p-p2)(p-p3)}{(p1-p2)(p1-p3)} Share_1 + \frac{(p-p1)(p-p3)}{(p2-p1)(p2-p3)} Share_2 + \frac{(p-p1)(p-p2)}{(p3-p1)(p3-p2)} Share_3 \quad (3)$$

Where $p1$, $p2$, and $p3$ represent the node id of the network.

The proposed research utilizes machine learning for intra-network prevention, which INTRA-SR and a combination of SVM handle. The researchers in [45] used SVM for traffic classification, considering the feature set of the nodes. The classification can't be semi-supervised in the case of intrusion detection, as any node can't be termed safe or unsafe at the initial stage.

The intrusion classification starts with the training behaviour based on the selected attributes. The training mechanism contains the Training Data and its associated label. The associated label demonstrates the class of the node.

The proposed algorithm uses a two-phase training and classification mechanism for intra-route intrusion. The first phase classifies the formed routes, and the second classifies the nodes from the classified routes. The proposed algorithm employs the feed forward back propagation neural network (FFBPNN) for node classification.

3.3. Algorithm

The algorithm for the route and node classification is shown in Algorithm 1.

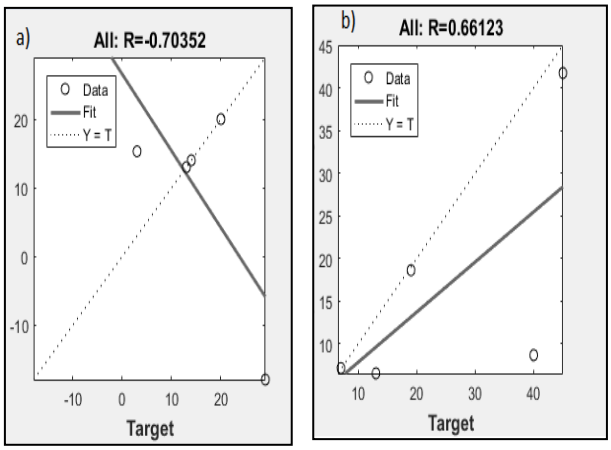
Algorithm 1

1. $Foreach\ route\ in\ route_{frame}$
2. $Input_{Parameter}(route) = Energy_{Consumed}\{route\};$
3. $Target_{Element}(route) = Route_{Id}$
4. $Other_{Route_{Target}} = XXX$
5. $Initialize\ SVM\ Structure$
6. $Kernel_{Type} = \frac{Linear}{ax+b=0}, \frac{Polynomial}{ax^2+bx+c=0}$
7. $Training_{Structure} = Plot_{Kernel}(Input_{parameter}, Target, Kernel_{type})$
8. $Test_{Data} = Input_{parameter}$
9. $Classified_{Route} = Simulate(Test_{Data}, Training_{Structure})$
10. $If\ Classified_{Route}\ in\ eachroute\ structure\ does\ not\ match\ with\ Target_{Element}$
11. $Suspected_{Route} + +$
12. End_{For}
13. $Foreach\ suspect\ in\ Suspected_{Route}$
14. $Input_{Parameter_{Node}} = Energy_{Conusmption}, Packet_{Loss}$
15. $Training_{Node_{Suspect}} = Initialize\ Neural\ Networks\ )$
16. $Test_{Data} = Input_{parameter_{node}}$
17. $Classified_{node} = Simulate_{Neural}(Test_{Data}, Training_{Node_{Suspect}})$
18. $If\ Classified_{node}\ in\ classified_{node}\ does\ not\ match\ with\ Target_{Element}$
19. $Suspected_{Node} + +$
20. End_{if}
21. End_{for}

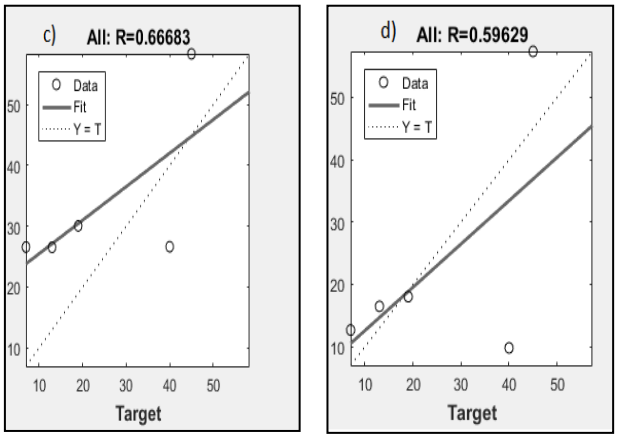
The proposed algorithm also tests the value of regression in the training architecture of Neural Networks. A set of 4 neurons are opted shown in Figure 6 (a), (b), (c), and (d), which contains the neuron count 20, 25, 18, and 15. The highest regression value is attained at neuron value 20. The entire training and classification are done with a neuron count of 20. Ordinal measures of Neural networks are shown in Table 2.

Table 2. Ordinal Measures of Neural Network

No.	Description	Value
1.	Maximum Attained Regression Value	.70
2.	Supplied Number of Neurons	20
3.	Total Supplied Iterations	100
4.	Average Number of Propagations	10-15
5.	Average Back Propagation count	3-6



(a) Neuron Count =20 (b) Neuron Count =25



(c) Neuron Count =18 (d) Neuron Count =15

Fig. 6 Neuron Count and Regression Value

4. Results and Analysis

The results of the proposed work are analyzed in different scenarios. The first set of outcomes is evaluated for verification of the algorithm proposed. The second set checks the accuracy considering the area, and the third is the combination of area and nodes proposed classification algorithm to determine the accuracy. Table 3 and figure 7 depict the classification accuracy by considering the area. It is known that more time is required for a large area to detect accuracy. However, accuracy decreases as the area increases for detection. Figure 7 shows the classification accuracy of the proposed work, neural network, and SVM. The accuracy of the proposed work for a 100*100 area is almost 100%. While, for neural and SVM, it is about 90% and 89%, respectively. However, if the area is increased further, such as 200 to 500 meters, then accuracy decreases, but the accuracy of the proposed one is greater than the other two. The average accuracy of the proposed for 2000 meters is 95.35, and the average of the neural network is 85.89.

Table 3. Area vs. Classification Accuracy

Area	Classification Accuracy Proposed	Classification- ion Accuracy Neural only	Classification- ion Accuracy SVM only
100*100	98.00	89.00	77.22
200*200	97.20	87.11	75.43
500*500	96.12	86.23	72.00
1000*1000	93.11	85.15	71.40
2000*2000	92.32	82.00	70.00

Thus, overall improved accuracy is $(95.35 - 85.89)/95.35 \times 100 = 10\%$. If we compare it with the SVM, the average classification accuracy is 73.21. The overall improved accuracy is $(95.35 - 73.21)/95.35 \times 100 = 23\%$.

Figure 8, based on data displayed in Table 4, describes the proposed work classification accuracy, neural network, and SVM with various nodes. It is observed in 50 nodes that classification accuracy is almost 95%, 83%, and 73% for the proposed work, neural and SVM, respectively. Consequently, the proposed classification accuracy is greater than the other two. It almost remains constant for 60, 70, 80, 100, and 120 in the case of the proposed work, but it decreases slightly for the Neural and SVM. The average proposed classification accuracy is 92, and that of neural network and SVM is 73.5 and 65.66, respectively. Thus, overall improved accuracy considering the neural network for the

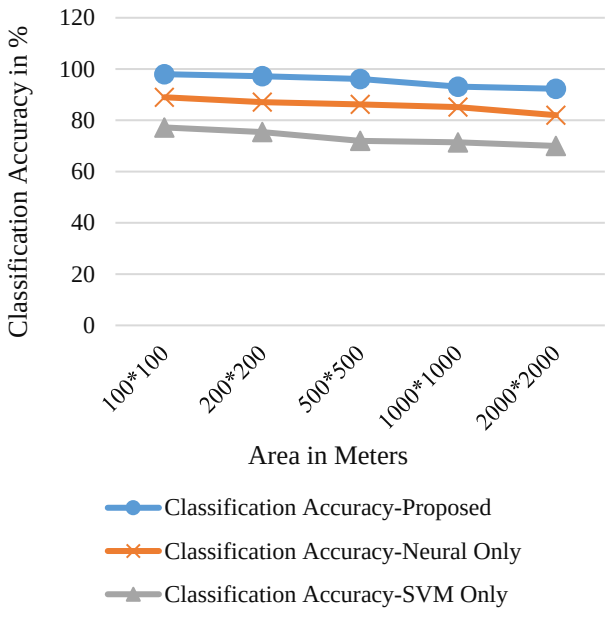


Fig. 7 Area vs. Classification Accuracy

proposed work is $(92 - 73.5)/92 \times 100 = 20\%$. Similarly, if we relate the accuracy of the proposed with SVM, it is improved by $(92 - 65.66)/92 \times 100 = 28\%$. Thus overall accuracy improved by 20% and 28% compared to neural network and SVM.

Table 4. Proposed Classification Accuracy With Different Numbers of Nodes

No of Nodes	Classification Accuracy- Proposed	Classification Accuracy- Neural only	Classification Accuracy- SVM only
50	95.00	82	73
60	93.00	79	71
70	92.80	74	68
80	91.00	72	65
100	90.55	69	62
200	90.00	65	55

Figure 9, based on data in Table 5, indicates the average proposed classification accuracy with area and nodes. It is seen that the average proposed classification accuracy with nodes 50 is higher than other nodes' size. For N=50, the proposed classification accuracy for 100 meters is 98%, while for N=100, it is 96%. If we consider N=150 and 200, then accuracy for 100 by 100 meters remains the same for both. Furthermore, as the area increases from 100 m to 2000m, the percentage accuracy also decreases.

The average accuracy for 50 nodes is 95.52, and that of other nodes for N=100 is 94.55. Similarly, for N=150 and 200

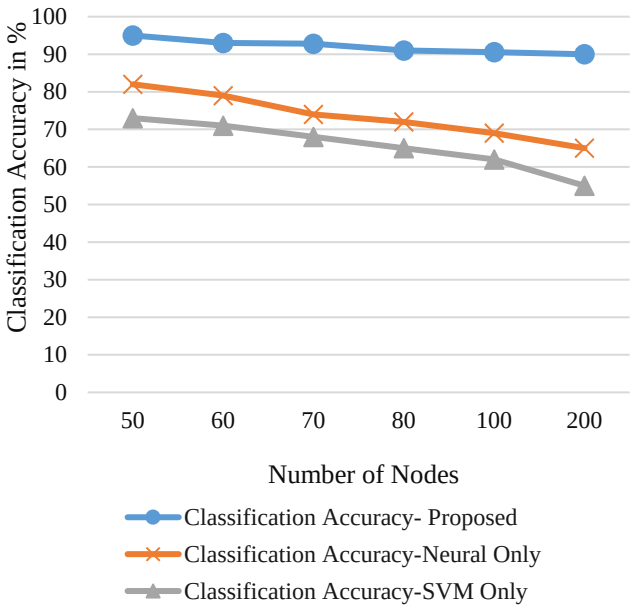


Fig. 8 Proposed Classification Accuracy with Different Number of Nodes

, it is 93.74 and 93.262. Thus, the overall improved accuracy of the proposed work for N= 50 and 200 is $(95.52 - 93.262)/95.52 \times 100 = 3\%$.

Table 5. Proposed Accuracy with Area and Nodes

Area	Average Proposed Classification Accuracy with N=50	Average Proposed Classification Accuracy with N=100	Average Proposed Classification Accuracy with N=150	Average Proposed Classification Accuracy with N=200
100*100	98.00	96.00	95.00	94.80
200*200	96.40	95.12	94.00	93.80
500*500	95.22	94.43	93.89	93.21
1000*1000	94.78	94.12	93.81	93.10
2000*2000	93.22	93.11	92.00	91.40

Figure 10 and Table 6 indicate the throughput rate of the proposed work in comparison to neural and SVM with the area. The average throughput rate of the proposed work is 12560 packets/second, and that of the other two SVM and Neural networks is 10560 packets/second and 9920 packets/second, respectively.

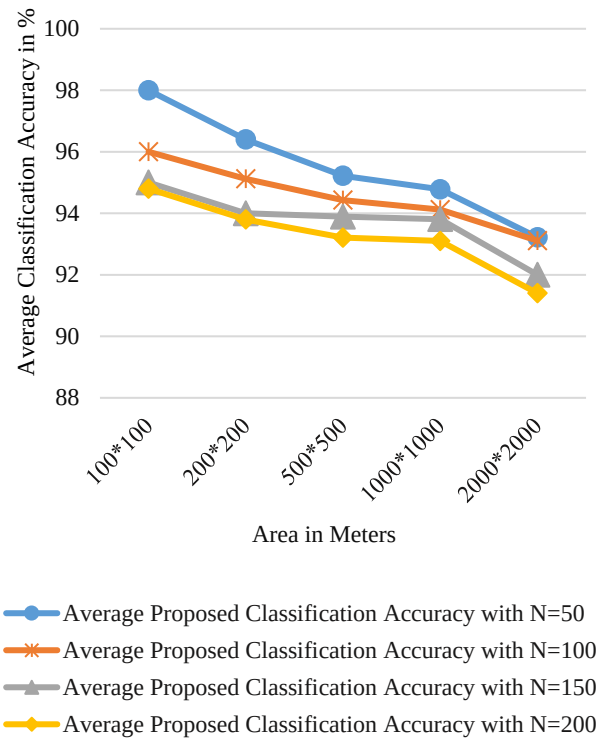


Fig. 9 Proposed accuracy with Area and Nodes

Table 6. Throughput Rate of Proposed Work

Area (Meters)	Through put Proposed	Through put Neural only	Through put SVM only
100*100	13000	10500	11000
200*200	12800	10200	10800
500*500	12600	9800	10500
1000*1000	12400	9600	10300
2000*2000	12000	9500	10200

In other words, the throughput rate decreases as the distance increase due to losses and travel speed. The effectiveness of the proposed work in comparison to SVM is $(12560 - 10560)/12560 \times 100 = 16\%$.

However, if we compared it with the neural network, the throughput rate of the proposed work improved by $(12560 - 9920)/12560 \times 100 = 21\%$. Thus, the overall throughput rate improved by 16% and 21% for SVM and neural networks, respectively.

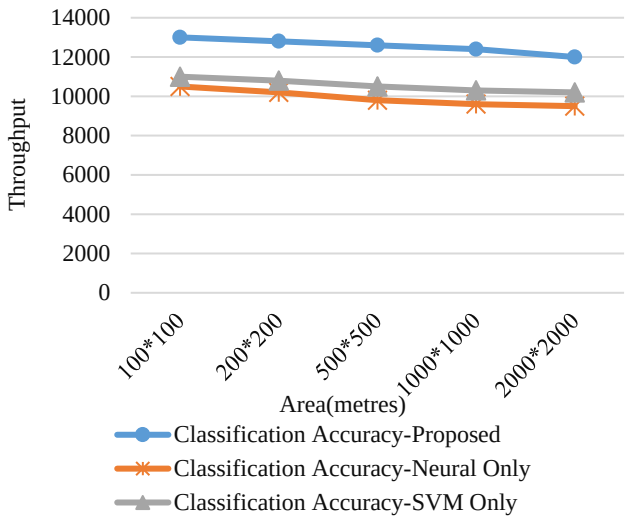


Fig. 10 Throughput rate of the proposed work

PDR is related to the actual number of data in the form of packets and their arrival at the final destination from its original source [46]. Figure 11 and Table 7 depict the PDR rate of the proposed work, neural network, and SVM for various nodes. It is observed with 50 number of nodes that the PDR rate is 0.97, 0.9, and 0.86 for the proposed work, neural, and SVM, respectively. Consequently, the proposed work PDR rate is greater than the other two. It decreases gradually for 50 to 100 nodes and decreases slightly for 150 to 200 nodes in the case of the proposed work.

Similarly, it decreases sharply for the Neural and SVM from 50 to 100 nodes and remains constant as the nodes increase.

Table 7. PDR Rate of Proposed Work

Number of Nodes	PDR Proposed	PDR Neural only	PDR SVM only
50	.97	.90	.86
60	.92	.81	.82
70	.88	.72	.76
80	.82	.66	.71
100	.76	.61	.60
200	.71	.58	.59

The average PDR rate of the proposed work is 0.84, and that of neural network and SVM is 0.71 and 0.72, respectively. Thus, the improved PDR rate of the work proposed compared to the neural network is $(0.84 - 0.71)/0.84 \times 100 = 15\%$. Similarly, the PDR of the proposed architecture, as compared to SVM, is improved by $(0.84 - 0.72)/0.84 \times 100 = 15\%$.

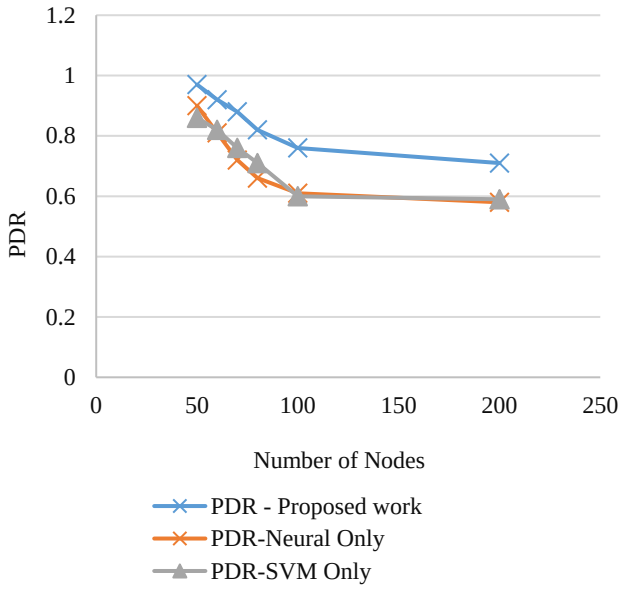


Fig. 11 PDR rate of the proposed work

Table 8. RtN vs. Improvement

RtN	% Improvement In Throughput	% Improvement In PDR
2/50 = .0400	2.000	2.520747
3/50 = .0600	2.225	2.503051
4/65 = .0615	2.451	2.716104
8/65 = .1200	3.150	2.365527
10/65 = .1500	3.690	2.694590
12/70 = .1700	4.015	2.967775

In addition, when a reliable node is added to the list, the average percentage growth is monitored and listed as follows. The evaluation is done based on PDR and throughput only. The evaluation is done on the reliability of

the total node count (RtN) mentioned in Equation (4). Where RtN is reliable to the total node count

$$RtN = \frac{Total_{Reliable_{Nodes}}\ through\ Interpolation}{Total\ Number\ of\ Applied\ Nodes} \quad (4)$$

The graphical representation is made in Figure 12 according to Table 8. It is observed that the throughput of the architecture increases significantly when reliable nodes increase in the network. Still, the total delivery ratio remains radical and stays in the range of 2-3%. The irrational pattern of the PDR is observed due to the other factors in the list of the delivery as load, delays in the packet transfers, etc.

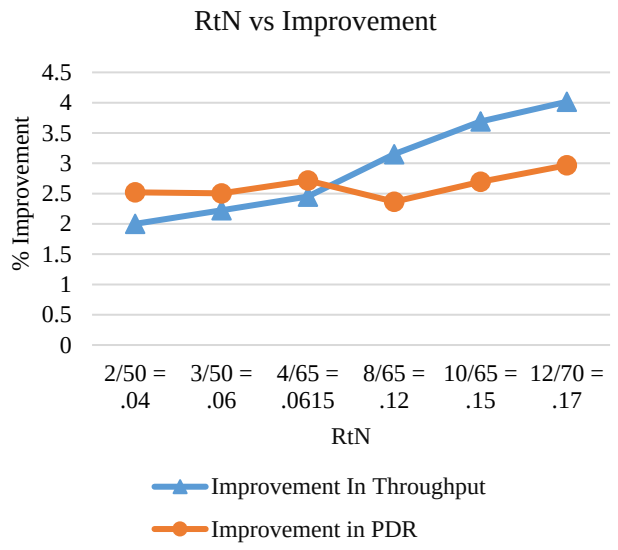


Fig. 12 RtN vs % Improvement

5. Conclusion and Future Work

This study work is presented with two block architecture which handles the intra-structure route and data communication between the nodes. The data communication is discussed using the deployment model, and the distance between the nodes is computed using the formula to measure the distance between two points. The classification of nodes and route discovery is explained in detail by thoroughly implementing the algorithms to determine the reach of nodes. Besides, the neural network has been considered in work proposed to classify the nodes. The effectiveness is measured by determining the throughput rate, PDR, and classification accuracy.

The detected classification accuracy is computed concerning different nodes and areas. The computed parameters have been further compared with the neural and SVM only. The average accuracy improved by 23% and 10% compared to the SVM and Neural network. However, the throughput rate revamped by 16% and 21%, contrary to SVM and Neural Network, respectively. The reliability of the proposed algorithm is tested using the applied node to accepted node ratio and the % improvement in throughput and the PDR in the architecture. As per the observation, the throughput increases significantly, but the PDR is radical to other factors also.

Consequently, the PDR rate of the proposed work was facilitated by 15% compared to other classification methods. Overall, it is computed that the proposed work provides a robust result contrary to other classification approaches and presents a more reliable and secure routing protocol for VoIP networks. Future work related to this research may be the application of deep neural network techniques for improving the reliability and security of routing protocol for VoIP.

Acknowledgment

The authors gratefully acknowledge the research facilities provided by NERIST (Deemed to be University). The research work of this paper has not received any grants from any funding authority in the public or commercial sector.

References

[1] Goode, B, "Voice over internet protocol (VoIP)," *Proceedings of the IEEE*, vol.90, no.9, pp.1495-1517, 2002.

[2] Chakraborty T., Misra I.S., Prasad R., "Technique for Improving VoIP Performance over Wireless LANs", In: VoIP Technology: Applications and Challenges," *Springer Series in Wireless Technology. Springer*, Cham, 2019.

[3] Vennila, G., Manikandan, M. S. K., and Suresh, M. N, "Dynamic voice spammers detection using Hidden Markov Model for Voice over Internet Protocol network," *Computers & Security*, vol.73, pp.1-16, 2018.

[4] Akbar, M. A., and Farooq, M., "Securing SIP-based VoIP infrastructure against flooding attacks and Spam over IP Telephony," *Knowledge and information systems*, vol.38, no.2, pp.491-510, 2014.

[5] Kaur, T., & Kumar, D, "A survey on QoS mechanisms in WSN for computational intelligence based routing protocols," *Wireless Networks*, 26(4) 2465-2486.

[6] Gandhi, U. D., Kumar, P. M., Varatharajan, R., Manogaran, G., Sundarasekar, R., & Kadu, S, " HIoTPOT: surveillance on IoT devices against recent threats," *Wireless personal communications*, vol.103, no.2 , pp.1179-1194, 2013.

[7] Anbar, M., Abdullah, R., Al-Tamimi, B. N., & Hussain, A, "A machine learning approach to detect router advertisement flooding attacks in next-generation IPv6 networks," *Cognitive Computation*, vol.10, no.2, pp.201-214, 2018.

[8] Vinnarasi, F. S. F., & Chandrasekar, A, "VANET routing protocol with traffic aware approach," *International Journal of Advanced Intelligence Paradigms*, vol.12, no. (1-2) , pp.3-13, 2019.

[9] Thomas Porter, C. I. S. S. P., & CCNP, C, "Practical VoIP Security," Elsevier, 2006.

[10] Paul, S., & Pandit, M. K, "A QoS-Enhanced Smart Packet Scheduler for Multi-core Processors in Intelligent Routers Using Machine Learning," *In Smart Intelligent Computing and Applications*, Springer, Singapore, pp. 713-720, 2019.

[11] Troia, S., Rodriguez, A., Martín, I., Hernández, J. A., De Dios, O. G., Alvizu, R., ... & Maier, G, "Machine-learning-assisted routing in SDN-based optical networks", *In 2018 European Conference on Optical Communication (ECOC)*, IEEE, pp.1-3, 2018.

[12] Oo, T. T., & Don, A. A, "Design and Implementation of Data and Voice Redundancy and Line Aggregation for VoIP with multiple links," *International Journal of Engineering & Technology*, vol.8, no.1.6, pp. 23-29, 2019.

[13] Xu, J., Wang, J., Qi, Q., Sun, H., & He, B, "Deep neural networks for application awareness in SDN-based network," *In 2018 IEEE 28th International Workshop on Machine Learning for Signal Processing (MLSP)*, IEEE, pp. 1-6, 2018.

[14] Sun, L., and Ifeachor, E. C, "Voice quality prediction models and their application in VoIP networks," *IEEE transactions on multimedia, Digital Object Identifier*, vol.8, no.4, pp. 809-820, 2006.

[15] Khatouni, A. S., Seddigh, N., Nandy, B., & Zincir-Heywood, N, "Machine Learning Based Classification Accuracy of Encrypted Service Channels: Analysis of Various Factors," *Journal of Network and Systems Management*, vol.29, no.1, pp.1-27, 2021.

[16] Moller, D. P, "Cybersecurity in Digital Transformation: Scope and Applications," *Springer* Nature, 2020.

[17] Elmi, A. H., Ibrahim, S., & Sallehuddin, R., "Detecting sim box fraud using neural network," *In IT Convergence and Security* 2012, Springer, Dordrecht, pp.575-582, 2013.

[18] Xiao, X., Wang, Z., Li, Q., Xia, S., & Jiang, Y, "Back-propagation neural network on Markov chains from system call sequences: a new approach for detecting Android malware with system call sequences," *IET Information Security*, vol.11, no.1, pp.8-15, 2017.

[19] Al-Akhras, M., Zedan, H., John, R., & Almomani, I, "Non-intrusive speech quality prediction in VoIP networks using a neural network approach," *Neurocomputing*, vol.72, no.(10-12), pp.2595-2608, 2009.

[20] Maheshwari, S., Mahapatra, S., Kumar, C. S., & Vasu, K, "A joint parametric prediction model for wireless internet traffic using Hidden Markov Model," *Wireless networks*, vol.19, no.6, pp.1171-1185, 2013.

[21] Jaiswal, R., & Hines, A, "Towards a Non-Intrusive Context-Aware Speech Quality Model," *In 2020 31st Irish Signals and Systems Conference (ISSC)*, IEEE, pp.1-5, 2020.

[22] Rebahi, Y., Nassar, M., Magedanz, T., & Festor, O, "A survey on fraud and service misuse in voice over IP (VoIP) networks," *Information Security Technical Report*, vol.16, no.1, pp. 12-19, 2011.

[23] Kumar, N., & Kumar, D, "An Improved Grey Wolf Optimization-based Learning of Artificial Neural Network for Medical Data Classification," *Journal of Information and Communication Technology*, vol.20, no.2, pp. 213-248, 2021.

[24] Xu, L., Zhou, X., Lin, X., Ren, Y., Qin, Y., & Liu, J., "A New Loss Function for Traffic Classification Task on Dramatic Imbalanced Datasets," In ICC 2020-2020 IEEE International Conference on Communications (ICC), IEEE, pp. 1-7, 2020.

[25] Gupta, S. K., Kumar, S., Tyagi, S., & Tanwar, S, "Energy efficient routing protocols for wireless sensor network," *In Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's Springer*, Cham, pp. 275-298, 2020.

[26] Wang, L., Lehman, V., Hoque, A. M., Zhang, B., Yu, Y., & Zhang, L, "A secure link state routing protocol for NDN," *IEEE Access*, vol.6 , pp.10470-10482, 2018.

[27] Ramalho, M, "Intra-and Inter-domain multicast routing protocols: A survey and taxonomy," *IEEE Communications Surveys & Tutorials*, vol.3, no.1, pp. 2-25, 2000.

[28] Chennikara-Varghese, J., Chen, W., Altintas, O., & Cai, S, "Survey of routing protocols for inter-vehicle communications," *In 2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, IEEE, pp.1-5, 2006.

[29] Altın, A., Fortz, B., Thorup, M., & Ümit, H, "Intra-domain traffic engineering with shortest path routing protocols," *Annals of Operations Research*, vol.204, no.1, pp.65-95, 2013.

[30] Qu, D., Vetter, B. M., Wang, F., Narayan, R., Wu, S. F., Hou, Y. F. ... & Sargor, C, *"Statistical anomaly detection for link-state routing protocols,"* In Proceedings Sixth International Conference on Network Protocols (Cat. No. 98TB100256), IEEE, pp. 62-70, 1998.

[31] Singh, A. V., Juyal, V., & Saggar, R., "Trust based intelligent routing algorithm for delay tolerant network using artificial neural network," *Wireless Networks*, vol.23, no.3, pp. 693-702.

[32] Rianto Nugroho, Fuad Djauhari, Galih Damas Priambodo, Novi Azman, "ATM VSAT Switchover Planning Telkom-1 Satellite Case Study to BRIsat Satellite," *International Journal of Engineering Trends and Technology(IJETT)*, vol. 69, no.11, pp.128-133, 2021.

[33] Vennila, G., Manikandan, M. S. K., & Suresh, M. N, "Detection and prevention of spam over Internet telephony in Voice over Internet Protocol networks using Markov chain with incremental SVM," *International Journal of Communication Systems*, vol.30, no.11, pp.3255,

[34] Vijayakumar, M., & Karthikeyani, V, "A Novel Approach of DBPQ with RSSI Queuing Technique for VoIP QoS over MANET," *Indian Journal of Science and Technology*, vol.9, vol.30, pp.1-8, 2016.

[35] Militani, D. R., de Moraes, H. P., Rosa, R. L., Wuttisittikulkij, L., Ramírez, M. A., & Rodríguez, D. Z., "Enhanced Routing Algorithm Based on Reinforcement Machine Learning," *A Case of VoIP Service*, 2021.

[36] Rattal, S., Badri, A., & Moughit, M., "A new wireless VoIP signaling device supporting SIP and H. 323 protocols," *Journal of Computer Networks and Communications*, vol.2014, 2014.

[37] Sathu, H., and Shah, M. A., "Performance comparison of VoIP codecs on multiple operating systems using IPv4 and IPv6," *International Journal of e-Education, e-Business, e-Management and e-Learning*, vol.2l, no.2 , pp.122, 2012.

[38] R. Surendiran, K. Alagarsamy, "Privacy Conserved Access Control Enforcement in MCC Network with Multilayer Encryption," *International Journal of Engineering Trends and Technology*, vol. 4, no. 5, pp.2217-2224, 2013. https://doi.org/10.14445/22315381/IJETT-V4I5P174

[39] Sielay Gebru, Prachi Kadam, "Simulation Based performance evaluation and comparison of wired VoIP services over UDP and SCTP protocol," *International Journal of Engineering Trends and Technology (IJETT)*, vol.33, no.9, pp.462-467, 2016.

[40] Kumar, V. & Roy, O. P, "QoS-Based Machine Learning Approach for Security of VoIP Services," *International Journal of Engineering Trends and Technology (IJETT)*, vol.70, no.2, pp.214-220, 2022.

[41] Newton, P. C., & Ramkumar, K., "TACA: Throughput Aware Call Admission Control Algorithm for VoIP Users in Mobile Networks," *In Advances in Computer and Computational Sciences*, Springer, Singapore, pp.259-270, 2017.

[42] A. Srikrishnan, Dr. Arun Raaza & Dr. B. Ebenezer Abishek, "Internet of Things (Iot) Network Security using Quantum Key Distribution Algorithm," *International Journal of Engineering Trends and Technology(IJETT)*, vol.70, no.2 , pp.19-23, 2022.

[43] Chen, D. R., Chen, L. C., Chen, M. Y., and Hsu, M. Y, "A coverage-aware and energy-efficient protocol for the distributed wireless sensor networks," *Computer Communications*, vol.137, pp. 15-31, 2019.

[44] Schmidt, S., Mazurczyk, W., Kulesza, R., Keller, J., & Caviglione, L., "Exploiting IP telephony with silence suppression for hidden data transfers," *Computers & Security*, vol.79, pp.17-32, 2018.

[45] Nassar, M., & Festor, O., "Monitoring SIP traffic using support vector machines, In International Workshop on Recent Advances in Intrusion Detection," *Springer, Berlin, Heidelberg*, pp. 311-330, 2008.

[46] Rath, M., Rout, U. P., Pujari, N., Nanda, S. K., & Panda, S. P., "Congestion control mechanism for real time traffic in mobile adhoc networks," *In Computer communication, networking and internet security*, Springer, Singapore, pp. 149-156, 2017.

[47] Ahson, S. A., and Ilyas, M. (Eds.), "VoIP Handbook: Applications, technologies, reliability, and security," *CRC Press*, 2008.