INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Enhanced Network Security for Improved Trustworthiness of VoIP Applications via Cuckoo Search and Machine Learning

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

1 Research scholar, Department of EE, North Eastern Regional Institute of Science and Technology, Nirjuli – 791109, Arunachal Pradesh, India
2 Professor, Department of EE, North Eastern Regional Institute of Science and Technology, Nirjuli - 791109, Arunachal Pradesh, India

OPEN ACCESS

Received: 27.07.2021
Accepted: 01.03.2022
Published: 15.04.2022

Citation: Kumar V, Prakash Roy O (2022) Enhanced Network Security for Improved Trustworthiness of VoIP Applications via Cuckoo Search and Machine Learning. Indian Journal of Science and Technology 15(15): 677-688. https://doi.org/10.17485/IJST/v15i15.1379

* **Corresponding author**.

vinodnerist@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To offer network design for secure Voice over Internet Protocol (VoIP) services with improved Quality of Services (QoS) parameters. **Methods:** The network area is created with required number of nodes. INTRA-SR process is employed for tracing of the route from the source node and INTER-SR is involved to reach a destination node. Cuckoo Search (CS) based optimization followed for the broadcasted voice packets. The Machine learning classifiers as SVM and ANN applied to decrease the instances of loss of voice packets. Simulation work is performed by using MATLAB 2018 and results obtained plotted in graphs using MS-Excel. **Findings:** The proposed design evaluated by incorporating CS algorithm to minimize the packet drops. SVM and ANN hybrid used to locate secure routing path. The QoS for throughput, latency and jitter are observed. The results exhibited higher average throughput of 98.8% irrespective of the attack instances. Lower average latency and jitter of 1.9s and 2.51ms are also exhibited by the proposed work. Similarly, latency work employing Ant Colony Optimization (ACO) with multiplex and multicasting (MM) is 2.66s that get increased to 3.16s due to attack. **Novelty/Applications**: The proposed algorithm significantly enhanced by deployment of highly protected network design with QoS and security. Application of ANN and SVM shown the improvement in performance for VoIP services. In addition to the regression analysis validates the results by applying other optimization algorithms.

Keywords: Voice over Internet Protocol; Cuckoo Search; Support Vector Machine; Artificial Neural Network; Machine Learning

1 Introduction

A technique VoIP that converts simple sound signals to computerized information that could be easily communicated via internet. This technology usually requires a VoIP application to be installed in the system and uninterrupted connection to internet for real time transmission of video, voice and multimedia. These applications require

codecs for the process of voice transfer in the form of data packets over the communication channel. Internet offers a flexible, cost effective, and convenient platform for VoIP applications that have become an integral part of most of the business, organizations and market. Hence, larger section of users now relies on VoIP applications instead of public switch telephone network (PSTN) as a means of communication. Some of the popular VoIP applications are shown in Figure 1. It is not practically feasible to have a single global phone number that can be reachable round the clock and over the globe. However, some of the VoIP applications such as Viber and WhatsApp require this as an identifier to address VoIP communication via internet and also requires the specific application to be installed on both the communicating devices [1,2].

The present day's society is turning towards IP based technology such as VoIP. According to a survey by Transparency Market Research Centre up to the year 2021, the VoIP market size predicted to rise up to 136.76-billion-dollar globally with about 348.5 billion of subscribers. Due to the limited of numbers for connections, users may not be able to get network access particularly in crowded areas. The data packets travel from network to network and path to be followed may get divert through untrusted area causing security attacks [3].

Fig 1. Popular VoIP applications

Security of VoIP networks is a challenging task, and it needs experts from several areas such as network security, operations, management, control, and user's services. The user's hardware devices, signaling gateways, routers, switches and signaling media involved in VoIP communication system remains at risk from attacks. The security protocols cannot be ignored and the secret information may be modified by intruders for personal benefit. VoIP network architecture should include security controls such as traffic monitoring, user authentication, authorization and policy-enforcement [4].

VoIP got considerable amount of users in the area of communication world but still faces many challenges such as security, confidentiality, integrity and, authenticity. Phishing attacks are at a high increasing level. In addition to services related to sensitive information and solution to the problem remains unsolved [5,6]. Virtual Private Network (VPN) monitoring and assessment is big challenge under full service operation conditions. VPN technology can be used as a QoS measure for VoIP security and not found fruitful for adding more security stacks [7,8]. The attacks causes to block the important resources to users. Adversarial attacks related to image data which mostly cannot be applied to network traffic classification. To develop improved model based on SVM is a big challenge [9–11].

Intruders generally attack VoIP services due to inheritance of several weak points. The protocol designers must address such issues before implementation. The efficiency of already developed algorithms for cyber security are not sufficient against cyber-attacks and the focus on fitness function for improvement of cyber security is the basic requirement. The Security and QoS are till important in the present day's world and different new machine learning techniques are under use by many researchers. The research work need to include parameters for classification, number of samples used and to reduce the strain real checking as well as to verify at the human level [12–15].

While designing a VoIP security over a distributed peer to peer communication, a triple authentication method was employed to offer secure multimedia communication using SIP and evaluated for cryptographic peer recognition to create a trust worthy communication platform [16]. Because of increase in random cyber-attacks at security level author used live Voice Detection (LVD) technique and biometric features for safety of VoIP system [17]. Authors addressed the security of VoIP by collecting the VoIP stream using packet length with transmission frequency and characterized the region reachable by malicious applications. Further, proposed a VoIP detection model to identify Nash equilibrium using practical algorithm [18]. Secure protocol for VoIP communication took advantage of two factor agreement named as authentication and evaluation but against both active and passive attack instances [19].

It was proposed a Construction by Selection method to scrutinize the payload media data of VoIP services and encrypting media traffic along with differentiating unencrypted and encrypted traffic[20]. A scheme offering a multipath solution is designed for low band width networks. The experimental outcomes demonstrated the enhanced quality of packets and reducing the packet loss while delivered across longer distances by employing large number of communication nodes[21,22]. The author proposed artificial immune systems with incremental learning. For making identification model the technique of unsupervised clustering is applied to identify abnormal data detection algorithms for VoIP applications. The effect of virtualization analyzed over the VoIP quality and evaluated the design with and without security. The outcomes demonstrated the delay in security measures[23].

Machine learning algorithms in providing necessary protocols for VoIP network are considered and complemented surveys on intrusion detection. The different comparisons provided important guidelines for network security[24,25]. The author proposed Ant Colony Optimization (ACO) based mechanism involved in MM design to enhance the security of VoIP service in wireless LAN. The secure VoIP service involved the implementation of Verifiable Secret sharing to MM design. Simulation results had displayed effectiveness for round time with delivered packets as compared to existing studies[26].

1.1 CS algorithm (CSA)

The CSA is based on the brood parasitic in other species in line with Levy's flying behavior of other birds and flies. This algorithm follows the living cuckoo process. According to this process a cuckoo lays egg once and then keeps that it in another nest. Further, some cuckoos grow, some are thrown and some destroyed in between or at final stage. The best egg is selected from host nests. The algorithm is one of the powerful metaheuristics and very suitable for a discrete type of problems. The algorithm is based on three assumptions, first of all cuckoo selects a nest randomly to lays one egg in it, then the nests with high egg quality (problem solving) are passed on to further generation, finally, the original owner of the nests can identify cuckoo eggs that may be probability Pa $\in$ [0, 1][27,28].

Some of the past studies related to CS based approaches are mentioned in Table 1 along with the objectives and techniques used.

Table 1. Cuckoo search objectives and techniques used in past approaches

Author	Proposed approach	Objective	Tool and techniques used
[29]	CS based model with Support Vector Machine	Online indoor positioning in IoT network.	MATLAB and data set of RSSI dataset of UCI repository for simulation work.
[30]	CS algorithm and quantum evolution approach	To minimize quality related factors in routing data packets	Implementation of Visual C++, windows 7 OS. WAXMAN model for random network topology.
[31]	CS based approach for feature selection.	Phishing websites prediction for improvement of accuracy	WEKA tool on open dataset from NASA store.
[32]	CS based hybrid approach with distribution of load	Security in TCP flood and DDoS environment.	Fuzzy based machine learning classifier. Simulation work with CloudSim tool.
[33]	Cuckoo Search eXtreme gradient boosting (CS-XGB) model using ML for optimization	Online airline system using websites for predicting consumer recommendations.	VADER (Valence Aware Dictionary for Sentiment Reasoning), Word2Vec algorithm, TF-IDF statistical measure
[34]	CS with Identity based approach.	Virtual Machine (VM) damages. Minimize the CPU usages and RAM due to DDoS attack.	MATLAB 2017 and cloudsim simulator to analyse collateral damages.

1.2 Support Vector Machine (SVM)

A statistical based supervised learning algorithm was introduced in 1995 known as SVM that could be used to solve problems of regression classification and forecasting. SVM utilize kernel functions to convert the input data into high feature to solve classification. SVM, like other conventional ML methods can gain strong generalization capacity with a few support vectors. Researchers have designed a models by adding SVM with less data set and improved design elements successfully[35].

SVM as a supervised learning method, has become a successful approach to solve classification and regression problems. SVM reports outstanding results in multiple domains. Researchers have mainly focused on SVM learning algorithms but now research is going on to find efficient kernel to improve accuracy. Linear, Gaussian, or polynomial are Standard kernels and are

unable to take benefit from specific data sets. This has driven the research to find alternative kernels to be used in the areas of multimedia such as VoIP [36].

1.3 Artificial Neural Networks (ANN)

ANN is computer systems promoted by the brain of human beings. Such type of systems are made up of units connected internally known as neurons. Every neuron can communicate with a signal processed by a receiving neuron and usually setup in layers and every layer make some sort of change in the data provided [37].

ANN applications gained popularity in different areas of human need and are competitive as compared to statistical models in terms of usability. It is highly recommended to analyze data by scholars in the social sciences and arts without its practical application of science and engineering. The ANN application can make models more accurate and user-friendly with larger inputs. The human brain is similar as a multidisciplinary device that specializes in sending signals, which can communicate easily to perform specific tasks. A key feature of these minds is their unique ability to process information. It creates many complexes that connect ”neurons” in the form of things that work jointly in solving a particular problem on a routine basis [38].

To meet the rising demand of reliable and secure VoIP solutions, we addressed the network security for offering an enhanced quality of VoIP service. To achieve this, we implemented Cuckoo Search for optimizing the network followed by SVM and ANN hybrid classifiers to identify malicious and genuine nodes. The paper is organized in six sections, after introduction as first section which include the VoIP technology, its applications along with security threats and QoS matters. The simulations work is performed using MATLAB/SIMULINK software. The proposed methodology discussed within section two and the results with discussion outlined in section three. Conclusion and future works is summarized as section four. At the end acknowledgement and references are mentioned as section five and section six respectively.

2 Methodology

This section of the paper categorized in two subsections. First subsection describes the important parameters of network deployment and the second subsection describes the implementation of CS with SVM and ANN hybrid classifiers to enhance to network security of the deployed network.

2.1 Deployment parameters

The network area of 1000 by 1000 sq. m is created with 50 to 500 nodes for the study of VoIP service. This defined network has predefined nodes labelled as a source node as well as for destination node. Table 2 lists the important parameters of network design. INTRA-SR process is employed for tracing of the route from the source node while following number of nodes. However, to reach a destination node that is present at longer distance other network INTER-SR is involved in addition to INTRA-SR.

Table 2. Parameters used in Network Design

Parameter	Description
Deployment Area	1000 × 1000 sq. m
Routing Technique	INTRA-SR and INTER_SR
Number of Nodes	50 to 500 nodes
Labelled Nodes	2 (Source and Destination Node)

2.2 Implementation of CS

This section describes about the improvement in security of the communication process dealt with the implementation of Cuckoo Search based optimization of the broadcasted voice packets. SVM and ANN as two Machine learning classifiers also integrated following network optimization to decrease the instances of loss of voice packets and communication delay observed during real time communication using VoIP applications. Figure 2 outline the major steps involved in the implemented strategy.

The integrated routing approach implemented in the last stage is followed by CS on the basis of brood parasitism [39]. To minimize the packet, drop during transmission optimization algorithm is incorporated in the present design. Further SVM and ANN hybrid is used to locate secure routing path for secure VoIP communication.

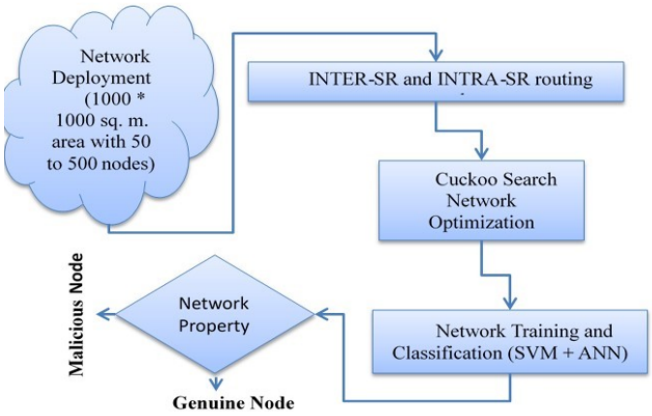

Fig 2. Outlined work methodologies

2.3 Implementation of SVM and ANN

The ordinal architecture of SVM and ANN is provided in this research. A supervised learning models SVM is used to train data for classification and regression problems. Data set containing various features related to problem is categorized in to two categories defined on basis of features. SVM training finds the category of the new examples to make it binary linear classifier. An SVM model can show visible data sets of various categories. New data sets are then correlated into the category of the dataset predicted that depends on the gap on which it falls. SVM performs efficiently both the linear classification and the non-linear classification. The concept of kernel comes in role when nonlinear classification is applied. Kernel searches for a hyperplane that can differentiate the training data by mapping the non-linear separable dataset into high-dimensional feature spaces. The issue with SVM is that, it is a binary classifier and the computation complexity of the algorithm increases in case of use for multi-class classification. The solution to the binary classification comes to be ANN which is a layered architecture and can accommodate multiple classes at once. There are three layers of ANN propagation model as follows.

2.3.1 Input Layer

The first layer of ANN is known as the input layer. The main purpose of this layer is to receive the inputs values for observation. The input layer is connected to its next layer that is known as the hidden layer. Three-layered architecture is connected with the layers by using nodes. Each node that exists in the input layer passes variables to every node of the hidden layer.

2.3.2 Hidden Layer

The hidden layer take input from the input layer and process it internally in the network, and last it pass processed data to every node at output layer. The processing of is performed by using weighted connections of the system. It is connected from both sides means the input layer or output layer.

2.3.3 Output Layer

It is the last layer of ANN and receives input from the hidden layer in the form of weighted connections. It generates output values against the prediction of weighted connection.

2.4 CS Optimization with SVM and ANN

This hybrid speeds up the communication while selecting only the genuine nodes. The number of steps followed in the approach based on CS with SVM and ANN are mention in Algorithm 1.

Algorithm 1.

CS optimized SVM and ANN Algorithm

1. Input: $D_{training}$ // training data
Cat_{data} // category data
2. Initialize CS variables

E_{num} // number of eggs representing sensor nodes property
$data_{ot}$ // optimized training data
3. Calculate length of optimized training data
$L = length(data_{opt_{train}})$ //Training data length for optimization
4. Initializing variable:
$data_{ot} = []$ //initializing empty matrix
5. $For_{each}\ i\ in\ L$
6. $E_{current} = data_{ot_i}$ // representing selected $node_{property}$ from current data sensor nodes
7. $E_{th} = average(data_{ot})$ // representing $threshold_{property}$
8. $if\ E_{current} < E_{th} = other\ Th_{properties}$ // threshold properties
9. $F_{fit} = fit(E_{current}, E_{th})$
10. $F_{fit} = \begin{cases} 1, & True \\ 0, & False \end{cases}$
11. $Best_{property} = CS(F_{fit}, D_{training}, CS_{variables})$
12. End_{for}
13. Initialize SVM parameters
$data_{ot}$ // optimized nodes property of training data
14. $for_{each}\ N\ in\ E_{num}$
15. Evaluate node property
$If\ Node_{prop} ==' Real'\ ; Group_1 = Node_{prop_N}$
16. Else ; $Group_2 = Node_{prop_N}$
17. End_{if}
18. End_{for}
19. $train_{st} = SVMTrain\ (data_{ot}, Group, Kernel_{function})$
20. $data_{ot} = train_{st}.SVM$ // identify training data for ANN
21. Initialize parameters for ANN
E_{num} // Total epoch
Itr_{num} // Total iteration
N_{num} // Total neuron
//Levenberg Marquardt techniques.
//Random data division
22. $Foreach\ i\ in\ data_{opt_{train}}$
23. If $(data_{opt_{train}}\ belongs\ to\ over_{load})$
24. Assign $cat_1 == data_{ot_i}$ // abnormal sensor node
25. If $(data_{ot}\ belongs\ to\ under_{load})$
26. Assign $cat_2 == data_{ot_i}$ // abnormal sensor node
27. Else ; Assign $cat_3 == data_{ot_i}$ // representing normal storage space
28. End_{if}
29. End_{for}
30. $Net_{storage} = Newff(data_{ot}, cat, N_{num})$ //call neural networks initialization function
31. $Net_{train} = train(Net_{storage}, data_{ot}, cat)$ // Network training for calls
32. $E_{c_{prop}} = property(E_{current})$ // property of current sensor node
33. $R_{verify} = simulate(Net_{train}, E_{current})$ //verifying result.
34. If $R_{verify} == True$
35. $Network_{property} = genuine$ //consider for data transmission
36. Else ; $Network_{property} = malicious$
37. End_{if}
38. Output: $Network_{property}$ // distinguishes malicious and genuine nodes

The proposed architecture utilizes SVM for the selection of the data which has to be passed to ANN in order to train the ANN for the identified labels. SVM uses polynomial plane for the creation of the hyperplane. The selected support vectors are passed to ANN for training. The support vectors as visible in Figure 3.

Neural networks uses the following ordinal measures for the propagation of the data into 15 layers of network. In order to train the system, the selected data is populated for multiple state actions and a total of 15 feature vector, divided into t=0-5

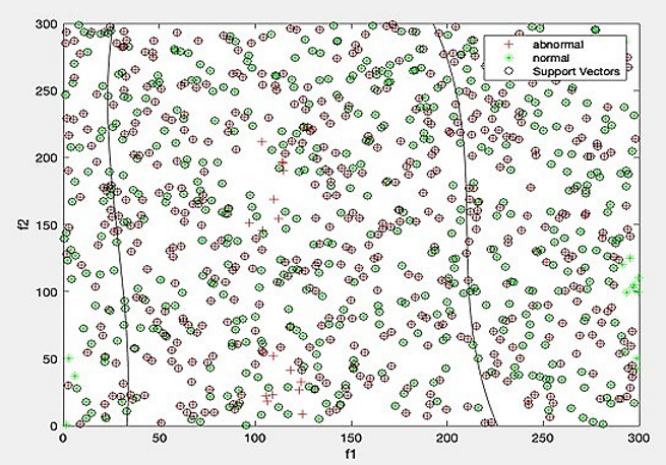

Fig 3. Results of polynomial kernel

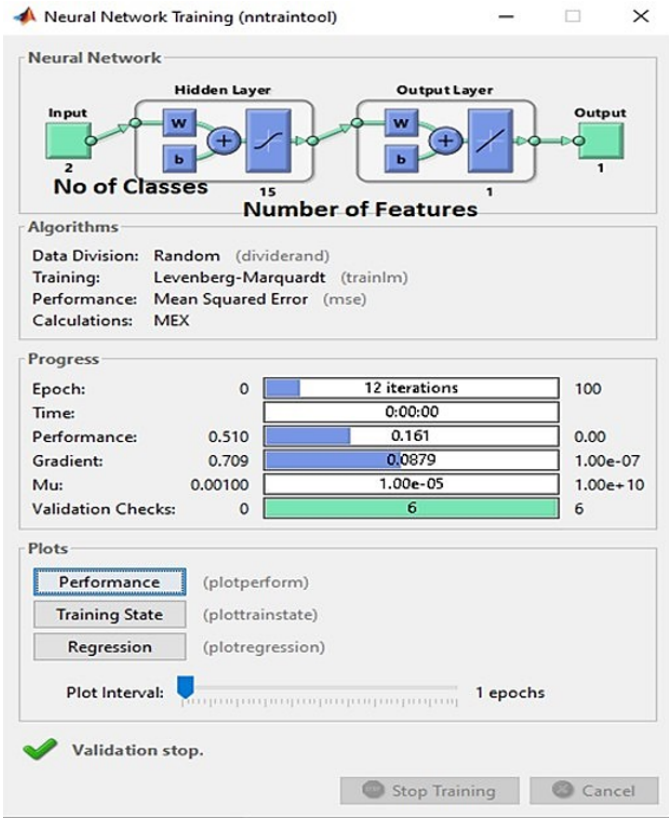

Fig 4. Neural network propagation model

time frames with each frame containing 3 values of attributes namely the "Throughput, Power Consumption" and "Delay" of the discovered route. The propagation network follows Levenberg Training model which validates the data utilizing the MSE generated in each propagation as shown in Figure 4. There are 4 certain stopping criteria's for the training to stop. The Algorithm 1 initially performs CS based node optimization then SVM and ANN hybrid based classification to identify the genuine and malicious nodes. CS exhibits local as well as global coverage while fitness function helps CS to trace better route. The optimized output is fed to machine learning classifiers as optimized training data. The implemented strategy aids in tracing best and secure route with enhanced data transmission speed. The network updates the input weight by modifying the gradient θ until the new weight value becomes equal to the old weight value. The proposed algorithm refers weight to the input data which is passed through the sigmoid function of Levenberg architecture. The increment or decrement in the gradient descent can be calculated by Levenberg model. The aim to train the system is to increase the classification accuracy. The proposed algorithm, views the classification accuracy as an object which gets it maximum value when the weight is propagated through most suitable elements of the category. Hence a hybrid classification algorithm is designed in which the selected support vectors from SVM is passed to propagation behavior algorithm.

3 Results and discussion

The proposed algorithm utilized the concept of attaining maximum overall regression in order to get maximum classification accuracy. In addition to the regression analysis performed with CS+SVM+ANN, the proposed algorithm also validates the results by applying Artificial Bee Colony (ABC) as optimization algorithm and Particle Swarm Optimization (PSO) as an artificial intelligence (AI) technique for approximation [40]. The proposed algorithm is simplified to observe optimization performance as a comparison result which is illustrated in Table 3.

Table 3. Regression Statistics

Record Count	R-Proposed	R-ABC+SVM+NEURAL	R-PSO+SVM+NEURAL
1000	.83	.72	.71
2000	.86	.73	.77
5000	.90	.76	.80
10000	.94	.82	.85

As clear from Table 3, the regression value (R) of the proposed algorithm architecture which incorporates Cuckoo Search, in combination with two classification algorithms namely SVM and ANN, is highest in comparison with other swarm based algorithms illustrated in the survey and hence CS-SVM-ANN architecture is proved to be most significant for the processing.

The proposed strategies described in the last section are also evaluated in this section under two scenarios, namely, VoIP service in present of attack and VoIP service without attack in terms of throughput, observed latency or delay in communication and jitter. The proposed design is also evaluated against existing study of Ramasamy and Eswaramoorthy who had integrated Ant Colony Optimization (ACO) with MM to enhance the security of VoIP services [26]. Table 4 presents the throughput observation by the proposed design (CS with SVM and ANN) and Ramasamy and Eswaramoorthy work (ACO with MM) [26] for VoIP service both before and after the attack instance. The node count used for the study ranges from 50 to 500 involving both INTRA-SR and INTER-SR routing protocol.

Table 4. Throughput Comparison (%)

Node count	Throughput Before Attack (Ramasamy and Eswaramoorthy) [26]	Throughput Before Attack (Proposed)	Throughput After Attack (Ramasamy and Eswaramoorthy) [26]	Throughput After Attack (Proposed)
50	98.9	99.5	98.6985	99.438
100	98.7	99.3	98.4595	99.208
200	98.3	99.1	97.9815	98.978
300	97.9	98.7	97.5035	98.518
400	97.5	98.3	97.0255	98.058
500	96.6	97.9	95.9500	97.598

Figure 5 provides a graphical comparison of the proposed design against the existing work of Ramasamy and Eswaramoorthy. The bar graph compares the throughput of both the studies represented by Y-axis against the node count represented by X-axis.

It is observed that for a particular number of nodes, the proposed work exhibited higher throughput irrespective of the attack instances as compared to Ramasamy and Eswaramoorthy's work. Overall, Average throughput of proposed work was 98.8% that get lowered to 98.633% due to attack. However, throughput of Ramasamy and Eswaramoorthy's work was 97.98% that get lowered to 97.603% due to attack. In other words, throughput comparison shows that due to attack the proposed work get compromised by 0.167% as compared to Ramasamy and Eswaramoorthy's work that get compromised by 0.38%.

Table 5. Jitter Comparison (ms).

Node count	Jitter Before Attack (Ramasamy and Eswaramoorthy)[26]	Jitter Before Attack (Proposed)	Jitter After Attack (Ramasamy and Eswaramoorthy)[26]	Jitter After Attack (Proposed)
50	1.5	0.54	1.772	0.608
100	2.4	0.94	2.843	1.068
200	2.7	1.90	3.200	2.172
300	3.6	2.70	4.271	3.092
400	4.7	4.10	5.580	4.702
500	5.6	4.90	6.651	5.622

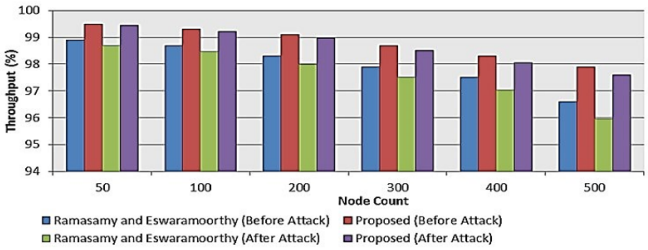

Fig 5. Throughput comparison

Jitter is an important parameter that governs the quality of VoIP based communication. It is observed due to issue in the delivery of voice packets at the destination. Jitter observed for the proposed and the Ramasamy and Eswaramoorthy's work is listed in Table 5 for node count varying from 50 to 500. Table 5 and Figure 6 shows that jitter for the proposed work is much lower than the existing work due to the implementation of the SVM and ANN hybrid classifiers that increases the quality of network employed for the packet transmission. On an average jitter of the proposed and Ramasamy and Eswaramoorthy's work is 2.513ms and 3.41ms that get increased to 2.87ms and 4.05 ms due to attack, respectively. In other words, attack has increased the jitter by 0.364ms of proposed and 0.636ms of Ramasamy and Eswaramoorthy's work.

Next, parametric values of latency comparison are listed in table 6 Latency is calculated to have an idea of overall communication delay adjoining the implemented methodology for VoIP communication. Latency of proposed work is compared against Ramasamy and Eswaramoorthy for before and after the attack.

Table 6. Latency Comparison (s).

Node count	Latency Before Attack (Ramasamy and Eswaramoorthy)[26]	Latency Before Attack (Proposed)	Latency Before Attack (Ramasamy and Eswaramoorthy)[26]	Latency Before Attack (Proposed)
50	0.7	0.5	0.82	0.562
100	1.5	1.1	1.772	1.252
200	2.3	1.5	2.724	1.712
300	2.9	2.1	3.438	2.402
400	3.9	2.5	4.628	2.862
500	4.7	3.7	5.58	4.242

Figure 7 shows that average latency of the proposed work employing CS with hybrid SVM and ANN is 1.9 s that get increased to 2.172 s due to attack. Similarly, latency of Ramasamy and Eswaramoorthy's work employing ACO with MM is 2.66 s that

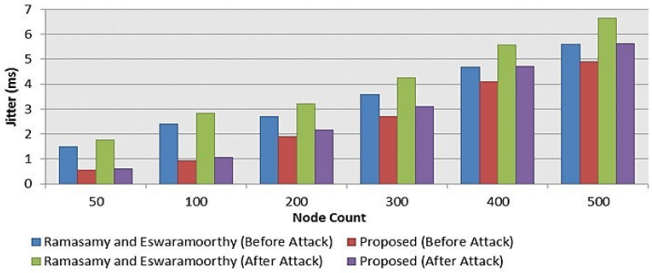

Fig 6. Jitter comparison

get increased to 3.16 s due to attack. The lower latency is observed in proposed work than the existing work. The nodes with average increase in latency of 0.272 s and 0.493 s has been observed for proposed and Ramasamy and Eswaramoorthy's work due to attack.

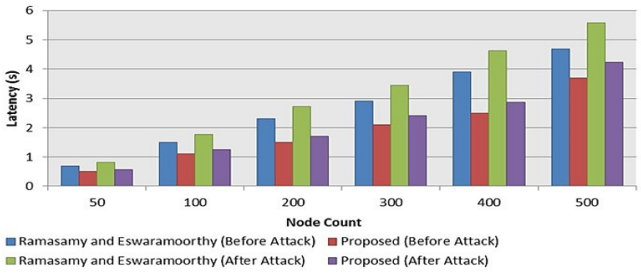

Fig 7. Latency comparison

The results from the research works compared with the results of past studies in the form of tables (Tables 4, 5 and 6). The study has addressed the key issues of VoIP communication system such as throughput, jitter and latency.

4 Conclusion and future works

This study had designed a highly secure wireless network to offer an improved VoIP service. INTER-SR and INTRA-SR routing techniques implemented for transmitting voice packets between source node and destination node. Authors had involved CS for optimizing network along with hybrid machine learning classifiers (SVM with ANN) to trance a secure route while distinguishing between malicious and genuine nodes. The effectiveness of the approach designed is calculated with number of nodes from 50 to 500 under attack and normal condition. Comparative study against existing work demonstrates higher throughput of proposed work to be $\sim$ 98% against $\sim$ 97% of existing work under both attack and normal scenarios. Lower average latency and jitter of 1.9 s and 2.51ms are also exhibited by the proposed work. In addition to the regression analysis to get maximum classification accuracy validates the results by applying other optimization algorithms such as ABC and PSO.

Overall, the proposed design successfully demonstrated the deployment of highly protected network design to offer secure VoIP service. Cuckoo search is commonly used for solving continuous problems and fails to solve discrete type of problem efficiently. The algorithms are still under developments for optimization due to the problem in adaptability. Because of the obtained results not up to the mark the future research need to study and explore more techniques to improve the parameter, step size, link processing and coupling functions between variables. To improve the reliability and security more approaches such as Deep Reinforcement Learning (DIL), Auto Encoder (AE) and Deep Belief Network (DBN) may be applied to protect the VoIP network from cyber security threats.

References

1) Tole S, Lina H, Deris S, Agus RM. Riyadi Munawar Agus, Subroto Imam Much Ibnu. WhatsApp, viber and telegram: Which is the best for instant messaging? *International Journal of Electrical & Computer Engineering*. 2016;6(3):2088–8708. Available from: http://dx.doi.org/10.11591/ijece.v6i3.10271.

2) Kenton OH, Michael M, Richard H, Simon R, Jessica M. Everyday dwelling with WhatsApp. *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. 2014;15:1131–1143. Available from: http://dx.doi.org/10.1145/2531602.2531679.
3) Mohammed B, Ismail S, Tamer R, Bou NA. Maximizing embedding capacity for speech steganography: a segment-growing approach. *Multimedia Tools and Applications*. 2021;7:1–22. Available from: https://doi.org/10.1007/s11042-020-10228-6.
4) Elhalifa C, Lian L. Security of VoIP networks. *2nd International Conference on Computer Engineering and Technology IEEE*. 2010;16:3–104. Available from: https://doi.org/10.1109/ICCET.2010.5485790.
5) Nikooghadam M, Amintoosi H. Perfect forward secrecy via an ECC-based authentication scheme for SIP in VoIP. *The Journal of Supercomputing*. 2020;76(4):3086–3104. Available from: https://dx.doi.org/10.1007/s11227-019-03086-z.
6) Alkhalil Z, Hewage C, Nawaf L, Khan I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*. 2021;3(6). Available from: https://dx.doi.org/10.3389/fcomp.2021.563060.
7) Qinyin C, Dong N, Jingbo X, Hsien-Wei T. Research on assessment method of network quality performance for a private data network. *Microsystem Technologies*. 2019;9:1–8. Available from: https://doi.org/10.1007/s00542-019-04383-6.
8) Faycal B, Najib EK, Ayoub B. Scalability evaluation of VOIP over various MPLS tunneling under OPNET modeler. *Indian Journal of Science and Technology*. 2009;10(29):1–8. Available from: https://doi.org/10.17485/ijst/2017/v10i29/117369.
9) Khundrakpam JS, Tanmay D. Efficient classification of DDoS attacks using an ensemble feature selection algorithm. *Journal of Intelligent Systems*. 2020;29(1):71–83. Available from: https://doi.org/10.1515/jisys-2017-0472.
10) Sadeghzadeh AM, Shiravi S, Jalili R. Adversarial Network Traffic: Towards Evaluating the Robustness of Deep-Learning-Based Network Traffic Classification. *IEEE Transactions on Network and Service Management*. 2021;18(2):1962–1976. Available from: https://dx.doi.org/10.1109/tnsm.2021.3052888.
11) Ehteram M, Singh VP, Ferdowsi A, Mousavi SF, Farzin S, Karami H, et al. An improved model based on the support vector machine and cuckoo algorithm for simulating reference evapotranspiration. *PLOS ONE*. 2019;14(5):e0217499–e0217499. Available from: https://dx.doi.org/10.1371/journal.pone.0217499.
12) Dantu R, Fahmy S, Schulzrinne H, Cangussu J. Issues and challenges in securing VoIP. *Computers & Security*. 2009;28:743–753. Available from: https://dx.doi.org/10.1016/j.cose.2009.05.003.
13) Subashini P, Krishnaveni M, Dhivyaprabha TT, Shanmugavalli R. Review on Intelligent Algorithms for Cyber Security. *Handbook of Research on Machine and Deep Learning Applications for Cyber Security*. 2020;p. 1–22. Available from: https://doi.org/10.4018/978-1-5225-9611-0.ch001.
14) Chaddad L, Chehab A, Kayssi A. OPriv: Optimizing Privacy Protection for Network Traffic. *Journal of Sensor and Actuator Networks*. 2021;10(3):38–38. Available from: https://dx.doi.org/10.3390/jsan10030038.
15) Anupam S, Kar AK. Phishing website detection using support vector machines and nature-inspired optimization algorithms. *Telecommunication Systems*. 2021;76:17–32. Available from: https://dx.doi.org/10.1007/s11235-020-00739-w.
16) Pecori R, Veltri L. 3AKEP: Triple-authenticated key exchange protocol for peer-to-peer VoIP applications. *Computer Communications*. 2016;85:28–40. Available from: https://dx.doi.org/10.1016/j.comcom.2016.04.005.
17) Satapathy A, Livingston LMJ. A Comprehensive Survey of Security Issues and Defense Framework for VoIP Cloud. *Indian Journal of Science and Technology*. 2016;9(6):1–3. Available from: https://dx.doi.org/10.17485/ijst/2016/v9i6/81980.
18) Addesso P, Cirillo M, Mauro MD, Matta V. ADVoIP: Adversarial Detection of Encrypted and Concealed VoIP. *IEEE Transactions on Information Forensics and Security*. 2020;15:943–958. Available from: https://dx.doi.org/10.1109/tifs.2019.2922398.
19) Ravanbakhsh N, Mohammadi M, Nikooghadam M. Perfect forward secrecy in VoIP networks through design a lightweight and secure authenticated communication scheme. *Multimedia Tools and Applications*. 2019;78:11129–11153. Available from: https://dx.doi.org/10.1007/s11042-018-6620-2.
20) Choudhury P, Kumar KRP, Nandi S, Athithan G. An empirical approach towards characterization of encrypted and unencrypted VoIP traffic. *Multimedia Tools and Applications*. 2020;79:603–631. Available from: https://dx.doi.org/10.1007/s11042-019-08088-w.
21) Alouneh S, Abed S, Ghinea G. Security of VoIP traffic over low or limited bandwidth networks. *Security and Communication Networks*. 2016;9:5591–5599. Available from: https://dx.doi.org/10.1002/sec.1719.
22) Wang R, Gao X, Gao J, Gao Z, Chen K, Peng C. An artificial immune and incremental learning inspired novel framework for performance pattern identification of complex electromechanical systems. *Science China Technological Sciences*. 2020;63(1):1–13. Available from: https://dx.doi.org/10.1007/s11431-019-9532-5.
23) Kolhar M, Alameen A, Gulam M. Performance evaluation of framework of VoIP/SIP server under virtualization environment along with the most common security threats. *Neural Computing and Applications*. 2018;30:2873–2881. Available from: https://dx.doi.org/10.1007/s00521-017-2886-y.
24) Christabelle A, Dristi D, Syed A, Tannish G, Maheen H, Ali R. Dataset of attacks on a live enterprise VoIP network for machine learning based intrusion detection and prevention systems. *Computer Networks*. 2009;197:108283–108283. Available from: https://doi.org/10.1016/j.comnet.2021.108283.
25) Mauro MD, Galatro G, Fortino G, Liotta A. Supervised feature selection techniques in network intrusion detection: A critical review. *Engineering Applications of Artificial Intelligence*. 2021;101:104216–104216. Available from: https://dx.doi.org/10.1016/j.engappai.2021.104216.
26) Ramasamy S, , and KE. Ant Colony Optimization Based Handoff Scheme and Verifiable Secret Sharing Security with M-M Scheme for VoIP. *International Journal of Intelligent Engineering and Systems*. 2017;10(5):267–277. Available from: https://dx.doi.org/10.22266/ijies2017.1031.29.
27) Vijayalakshmi M, Rao DS. QoS aware multicasting using the enhanced differential evolution cuckoo search routing protocol in MANET. *International Journal of Mobile Network Design and Innovation*. 2018;8(4):215–215. Available from: https://doi.org/10.1504/IJMNDI.2018.095241.
28) Mellal MA, Adjerid S, Williams EJ, Benazzouz D. Optimal replacement policy for obsolete components using cuckoo optimization algorithm based-approach: dependability context. 2012. Available from: http://hdl.handle.net/123456789/14928.
29) Amjad K, Asfandyar K, Iqbal BJ, Fazli S, Abdullah K, Atif K, et al. Cuckoo Search-based SVM (CS-SVM) Model for Real-Time Indoor Position Estimation in IoT Networks. *Security and Communication Networks*. 2021. Available from: https://doi.org/10.1155/2021/6654926.
30) Yassine M, Amar RC, Mohammed M, Dalila A. A hybrid quantum evolutionary algorithm with cuckoo search algorithm for QoS multicast routing problem. *International Journal of Communication Networks and Distributed Systems*. 2019;22(3):329–361. Available from: https://doi.org/10.1504/IJCNDS.2019.098873.
31) Akash S, Navneet S, Pawan A, Rohit B. Phishing Website Prediction by Using Cuckoo Search as a Feature Selection and Random Forest and BF-Tree Classifier as a Classification Method. *Rising Threats in Expert Applications and Solutions* . 2021;p. 765–776. Available from: https://doi.org/10.1007/978-981-15-6014-9_92.
32) Anandaraj APS, Indumathi G. Improved cuckoo search load distribution (ICS-LD) and attack detection in cloud environment. *Concurrency and Computation: Practice and Experience*. 2021;33(3). Available from: https://doi.org/10.1002/cpe.5226.

33) Jain PK, Yekun EA, Pamula R, Srivastava G. Consumer recommendation prediction in online reviews using Cuckoo optimized machine learning models. *Computers & Electrical Engineering*. 2021;95:107397–107397. Available from: https://dx.doi.org/10.1016/j.compeleceng.2021.107397.
34) Priyanka V, Shashikala T, Wilfred GW. A request aware module using CS-IDR to reduce VM level collateral damages caused by DDoS attack in cloud environment. *Cluster Computing*. 2021;23:1–7. Available from: https://doi.org/10.1007/s10586-021-03234-2.
35) Moazenzadeh R, Mohammadi B, Duan Z, Delghandi M. Improving generalisation capability of artificial intelligence-based solar radiation estimator models using a bio-inspired optimisation algorithm and multi-model approach. *Environmental Science and Pollution Research*. 2022;4:1–9. Available from: https://dx.doi.org/10.1007/s11356-021-17852-1.
36) feng Ji Y, bao Song L, Sun J, Peng W, ying Li H, feng Ma L. Application of SVM and PCA-CS algorithms for prediction of strip crown in hot strip rolling. *Journal of Central South University*. 2021;28(8):2333–2344. Available from: https://dx.doi.org/10.1007/s11771-021-4773-z.
37) Imran M, Khan S, Hlavacs H, Khan FA, Anwar S. Intrusion detection in networks using cuckoo search optimization. *Soft Computing*. 2022;3:1–3. Available from: https://dx.doi.org/10.1007/s00500-022-06798-2.
38) Abiodun OI, Jantan A, Omolara AE, Dada KV, Mohamed NA, Arshad H. State-of-the-art in artificial neural network applications: A survey. *Heliyon*. 2018;4(11):e00938–e00938. Available from: https://dx.doi.org/10.1016/j.heliyon.2018.e00938.
39) Yang XS, Deb S. Engineering optimisation by cuckoo search. *International Journal of Mathematical Modelling and Numerical Optimisation*. 2010;1(4):330–343. Available from: https://dx.doi.org/10.1504/ijmmno.2010.035430.
40) Khuat TT, Le MH. A Novel Hybrid ABC-PSO Algorithm for Effort Estimation of Software Projects Using Agile Methodologies. *Journal of Intelligent Systems*. 2018;27(3):489–506. Available from: https://dx.doi.org/10.1515/jisys-2016-0294.