International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V70I2P225
Volume 70 Issue 2, 214-220, February, 2022
© 2022 Seventh Sense Research Group®

Original Article

QoS-Based Machine Learning Approach for Security of VoIP Services

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

[1]*Research Scholar,* [2]*Professor*
[1,2]*Department of EE, NERIST, Nirjuli – 791109, Arunachal Pradesh, India*

[1]vinodnerist@gmail.com, [2]oproy61@gmail.com

Abstract *- Voice over Internet Protocol (VoIP) involves the process of voice transmission via the internet in the form of data packets. VoIP faces several problems related to Quality of Service (QoS) issues like missing of data packets, delay, jitter and latency, resulting in poor voice quality. To improve VoIP services, the authors proposed a network design using a machine learning approach and calculated the quality of voice communication. Further, considered the number of nodes in the proposed work ranging from 5 to 30 and calculated the results with two scenarios, one before the attack and another after the attack. The results with the proposed approach as compared to the existing approach exhibit lower packet loss, throughput, latency and jitter. The proposed approach demonstrated the better QoS for the VoIP network, which is an improvement as compared to the existing approach.*

Keywords — *VoIP, machine learning, QoS, ABC, SVM, ANN.*

I. INTRODUCTION

Voice over Internet Protocol (VoIP) involves the process of analog signal transmission via the internet. Due to the advancement in communication technology, real-time voice transmission over the internet has become popular. The performance of the network is important and depends on protocols. Although various research works focused on Internet protocol (IP) extensions for providing support to communications [1]. The QoS for voice transmission on VoIP is related to the codecs used. The voice codecs are responsible for digital conversion and compression. The coding rate of various codecs depends on bit per second and frames per second of data transfer and is responsible for the quality of voice in a VoIP communication system. [2]. The basic purpose of improving the QoS is to reduce the loss of data packets in the VoIP communication system.

The VoIP data flow can be divided into two classes, one sensitive and another non-sensitive. The VoIP follows the communication protocols for the purpose of data transfer [3]. Machine learning (ML) is an emerging technique for computer systems to learn about data and performance with accuracy. In a communication environment, ML can learn the network situations dynamically in the QoS related errors. The network communication system can be categorized on the basis of QoS [4], [5]. The network is dependent on reliable and secure internet applications. To improve QoS, the internet service providers may work on providing the best services with accuracy and low computing load [6]. In a VoIP communication system, channel allocation is a very critical problem due to different applications required by the network [7], [8]. QoS and data security are necessary for the establishment of VoIP. Some of the pros and cons inhabited by VoIP service are summarized below.

A. Advantages of VoIP Communication

- Minimal voice calling cost.
- Highly flexible means of communication.
- It offers services such as voice mails and call forwarding.
- Totally a cost-free service for PC to PC communication.
- Advantages of International and long-distance calls.
- It has easy implementation and installation.
- It can be integrated with available services.

B. Disadvantages of VoIP Communication

- Un-ability to make calls under power shutdown.
- It has inadequate practicability in emergency situations.
- Totally relies on the quality of Internet Connection

C. VoIP Technology

Voice over Internet Protocol involves many components for successful voice communication such as CODEC (coder and decoder) for signal conversion, packetize digital data at one end and de-packetize for data at another end [9]. The Voice communication process is shown in Fig.1. Some most frequently used codecs are mentioned with data rate and packet size in Table I. The signalling protocol is part of VoIP communication and works at the application layer for managing multiple sessions. More protocols, for example, H 323 and Real-Time Protocol (RTP), are used in VoIP for data transfer [10]. Most of the researchers concentrated on the quality of experience (QoE) by using machine learning algorithms and choosing the appropriate machine learning method, but problems to improve the quality of service are still pending [11], [12].

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

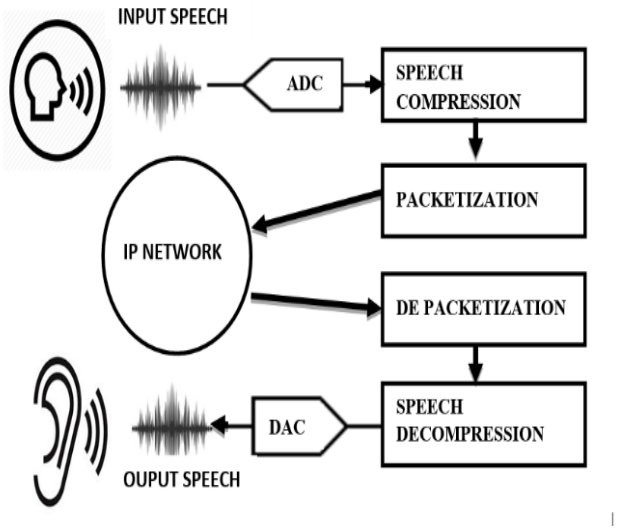

Fig. 1 VoIP communication process

This research work involves the analyses of the QoS parameters and best machine learning method for improvement of the voice quality in the VoIP communication process.

Table I. Frequently used CODECs for VoIP

Name of Codecs (ITU-T)	Bit Rate in kbps	Name of Codecs	Bit Rate in kbps
G.711	64	DVI	32
G.721	32	G.722.1 - MLT	24
G.722 –2 band	64	L16 – Linear PCM	128

This paper is presented in five sections, including the introduction to VoIP. Section 2 gives the details about the previous study in the form of a literature review. Section 3 is about the proposed implementation to improve the QoS in VoIP. The results with discussion are described in section 4 and finally concluded with section 5.

II. LITERATURE REVIEW

This section is related to the work done by different researchers to solve various problems for the improvement of VoIP technology. The researchers analyzed models to check the safety requirements in VoIP systems and raised questions about security frameworks [13], [14]. Recurrent Neural Networks (RNNs) and a real traffic dataset were built to protect from different attacks. The detection accuracy is shown higher as compared to the traditional machine learning approach. The results for DDoS incidents are compared after experimentation [15], [16]. The author advised using RFC (Request for Comments), resulting in the overall verification delay times through experiments and used a mutual key exchange in the encryption method to improve security [17].

To estimate the VoIP quality E-model has been combined without the requirement of time consumption and illustrated the QOS in service-oriented computing [18]. A statistical learning scheme based on the secure VoIP detection algorithm to recognize SPAM is proposed. An incremental support vector machine (ISVM) and the performance is tested using an experiment that reported a positive probability rate against the spammers [19], [20]. Research issues with future directions are discussed by identifying pitfalls [21]. ML algorithms show the enhancement in terms of bandwidth allocated in a real-time environment. Earlier research differentiated the internet data flowed and reviewed the techniques on the basis of Machine Learning [22], [23].

ML approaches were used to classify SDN-IoT networks and examined about random forest classifier with SFS data presented in sub-datasets [24], [25]. RL based routing protocol with reduced overhead and implementation of network scenarios is presented, such as traffic flows and routes. The network parameters are analyzed to implement a VoIP system. Communication quality predicted by using an E-model algorithm and experimental results showed user's QoE as an important factor [26]. The packet loss, delay, throughput and jitter affect DFI features of network communication is observed, and for improvement in QoS parameters, added network key performance indexes (KPIs) as input [27].

The author proposed a reinforcement learning-based approach for improvement in QoS parameters and observed that 3D charge-trap based storage devices deliver higher performance [28]. The reliability at the link level is examined, and the experimental setup evaluated a real-time application and a task offloading application [29]. The QoS issues, channel access mechanisms related to recent IoT standards and performance analysis transfer mechanisms in cellular networks are presented using machine learning techniques [30]. The power-saving in-network is an important factor. The levels of network communication are exploited to classify the application of ML [31].

The researchers found the stream control transmission protocol (SCTP) as a better VoIP application on the transport layer protocol within the range of acceptable latency. Further, suggested the integration of old traditional telephony systems and VoIP systems with IP Multimedia Subsystems (IMS) network through gateways. But the problem of QoS still remains with VoIP. The technology is undergoing a process of testing and needs improvement [32], [33].

III. METHODOLOGY

This part of the paper is related to the proposed approach to improve QoS with security in VoIP services. According to the literature reviews, lots of researchers made attempts to improve VoIP, but the required level was not achieved. Initially, the deployment area for the network is defined with nodes ranging up to 30 in numbers. The source node used a number of nodes resulting in root formation. In the proposed work, the author first incorporated Artificial Bee Colony (ABC) based optimization to enhance the voice packet security broadcasted over the network. Following this, Support Vector Machine (SVM) along with Artificial Neural Network (ANN) is used to reduce the instances of packet loss and latency during the transmission process.

To calculate the success of the design mentioned in this paper, QoS is enumerated with calculations reflecting throughput, dropped packets, jitter and packet loss rate. The overview of the design is given in Figure 2, and the hybrid algorithm is shown as Algorithm 1 to gain in the security of the VoIP network. In the initial stages, Artificial Bee Colony based optimization is performed. The fitness function is calculated to identify the best fit and highly optimized network nodes. The information is then passed to SVM that trains the optimized network. Further, the optimized training data is fed to ANN, where Training and classification of network nodes is performed to identify malicious nodes from non-malicious nodes

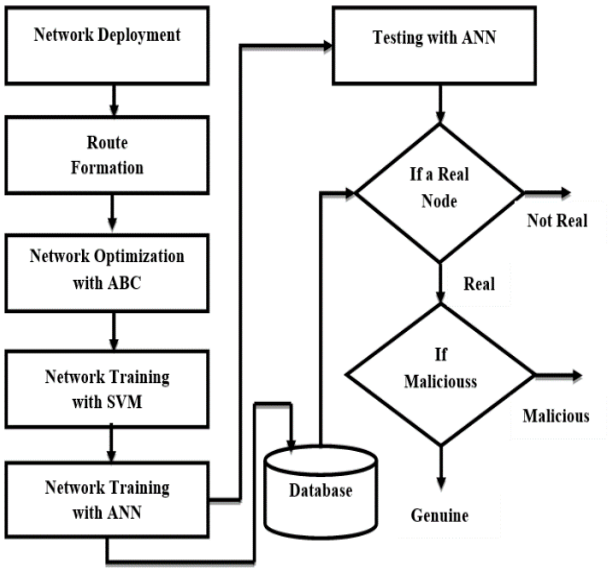

Fig 2: Flowchart for design

Algorithm 1.

1. Start ABC Algorithm for optimization of $Training_{data}$
2. Parameters Initialization
   x. U_{upper} // Boundary upper
   y. L_{lower} // Boundary lower
3. Calculate Length of $Training_{data}$
   $x.\ T_{length} = length(Training_{data})$
   //The training data size
4. Repeat iteration until T_{length}
5. Locating random nodes
6. $Node_{position} = random\ (0,1)(U_{upper} - L_{lower})$ //Locate nodes randomly
7. Calculating the distance matrix
   $x.\ Node_{distan} = \text{mini}(Node_2 - Node_1)$
   // Finding the distance between nodes
8. Calculating fitness score
   $x.\ fit_s = \sum_{i=0}^{n} Node_{distan}$
   //Representing nodes in the matrix
9. Calculation of the fitness function
   x. if $fit_{score} \geq 0, f_{fit} = \frac{1}{1+fit_s}$
   y. if $fit_{score} < 0, f_{fit} = 1 - absolute(fit_s)$
10. Selecting the node having the least fitness value
    $x.\ Best_{value} = mini(f_{value})$
    //Node select with least fitness value
11. $End_{iteration}$
12. Initialization of SVM parameters
    $x.\ OTraining_{data}$
    // optimization of node property for training data
13. $for_{each}\ N\ in\ Node_{total}$
14. Checking the node property
    x. $If\ Node_{prop} ==' Real'$
    y. $Group_1 = Node_{prop_N}$
15. Else
    x. $Group_2 = Node_{prop_N}$
16. $End_{if}\ End_{for}$
17. $train_{st} = SVMTrain\ (OTraining_{data}, Group, Kernel_{function})$
18. $OTraining_{st} = train_{st}.SVM$
    // identify training data for ANN
19. Initialization of ANN variables
    $x.\ E_{num}$
    // epochs number for iterations by ANN
    $y.\ N_{num}$ // Neurons used
20. Initializing ANN parameters
    $x.\ MSE$, Gradient, Mutaiton, validation
    $y.\ Levenberg\ Marquardt$
    // Name of the used technique
    $z.\ random$ // data division
21. $for_{each} T\ in\ OTraining_{st}$
22. $if\ OTraining_{st_T} == Node_{communicating}$
    //Communicating node
23. $cat_1 = property\ (OTraining_{st_T})$
    // real node
24. $Else_{if}\ cat_2 = property\ (OTraining_{st_T}$
    // Non-real node
25. $Else\ cat_3 = property\ (OTraining_{st_T}$
    // More number of properties
26. $End_{if}\ End_{for}$
27. $VoIP_{net} = Newff(OTraining_{st_T}, cat_{data}, N_{num})$
    // Training and category data
28. Initialize Training ANN
29. $VoIP_{trained} = Train(VoIP_{net}, OTraining_{data}, cat)$
    //Set training parameters
30. Initiation of testing with ANN
31. $Node_{current} = property\ (Node_{current})$
    //Current nodes property
32. $Node_{valid} = simulate\ (Cloud_{net}, Node_{current})$
33. $if\ Node_{valid} == True;$
    Return $Node_{genuine}$
    //Authenticity check for node
34. Else Return $Node_{malicious}$
    // assigning to a malicious node
35. $End_{if}\ End_{for}$

IV. RESULTS AND ANALYSIS

The proposed VoIP network is analyzed for QoS by measuring packet loss rate, throughput, latency and jitter. The values are taken under two conditions, one with a normal network another without a normal network condition. The details of values taken are presented in the form of tables, and accordingly, figures are plotted. Further, the discussion is given below each figure.

A. Packet Loss Analysis

Packet loss is the failure of data packets in between source and destination in a network. In the case of a reliable and secure VoIP network, it is hard to avoid packet loss for highly sensitive VoIP applications. The packet loss is calculated by considering the number of nodes for 5 to 30. Table II mention the percentage loss of packet before the attack and after the attack.

Table II. Packet Loss Analysis

Number of Nodes	Attack (before)		Attack (after)	
	ABC and SVM	Proposed	ABC and SVM	Proposed
5	1.1	0.4	1.31	0.51
10	1.4	0.6	1.69	0.72
15	1.8	1.1	1.99	1.34
20	2	1.4	2.32	1.62
25	2.1	1.6	2.33	1.73
30	2.3	1.7	2.65	1.79

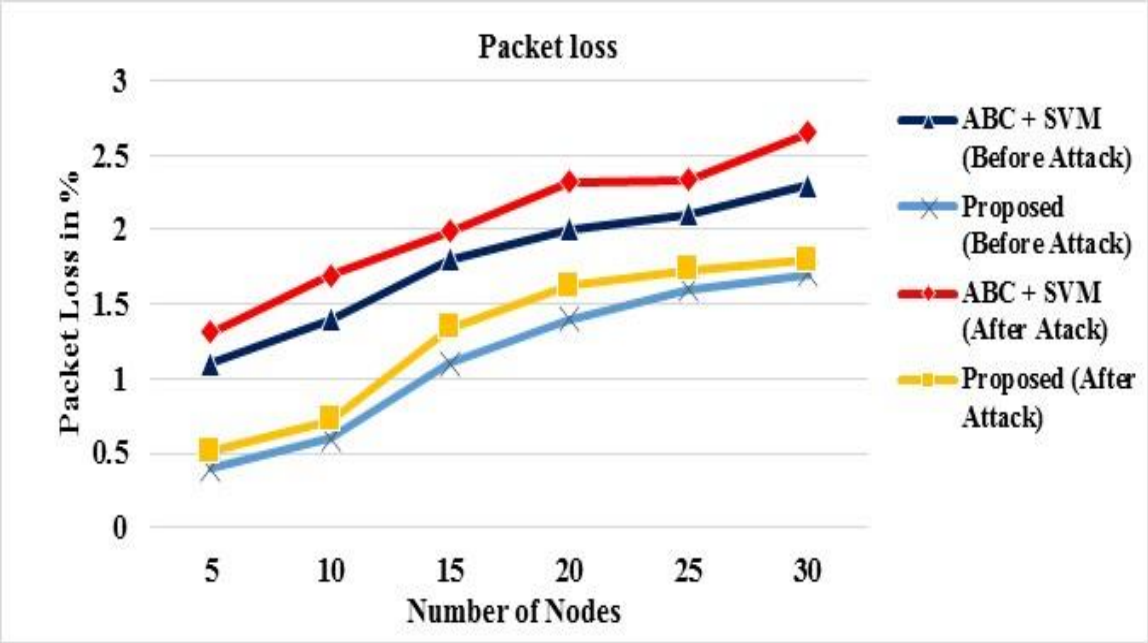

Fig. 3 Packet loss Analysis

All the values of packet loss are shown in Table II and plotted in Figure 3. It is observed in the approach proposed that the value as the average of loss of a packet is 1.13 % before the attack and 1.29 % after the attack. Whereas for ABC with SVM, the average values are 1.78 % and 2.05 % before the attack and after the attack, respectively. It is observed that there is a reduction in packet loss by introducing the proposed approach.

B. Throughput Analysis

Throughput is a number of bits passed through the medium in a specific period of time from the source to the destination in a VoIP network. It is calculated by considering the number of nodes from 5 to 30. Table III mention the percentage of throughput for the proposed and ABC with SVM before attack then after the attack. It is calculated and plotted valued of throughput in percentage.

Table III. Throughput Analysis

Number of Nodes	Attack (before)		After (after)	
	ABC and SVM	Proposed	ABC and SVM	Proposed
5	98.5	99.4	98.41	99.33
10	98.2	99.1	98.11	98.92
15	97.8	98.7	97.66	98.59
20	97.6	98.4	97.42	98.11
25	97.3	98.3	97.02	98.13
30	97.2	98.2	97.04	97.92

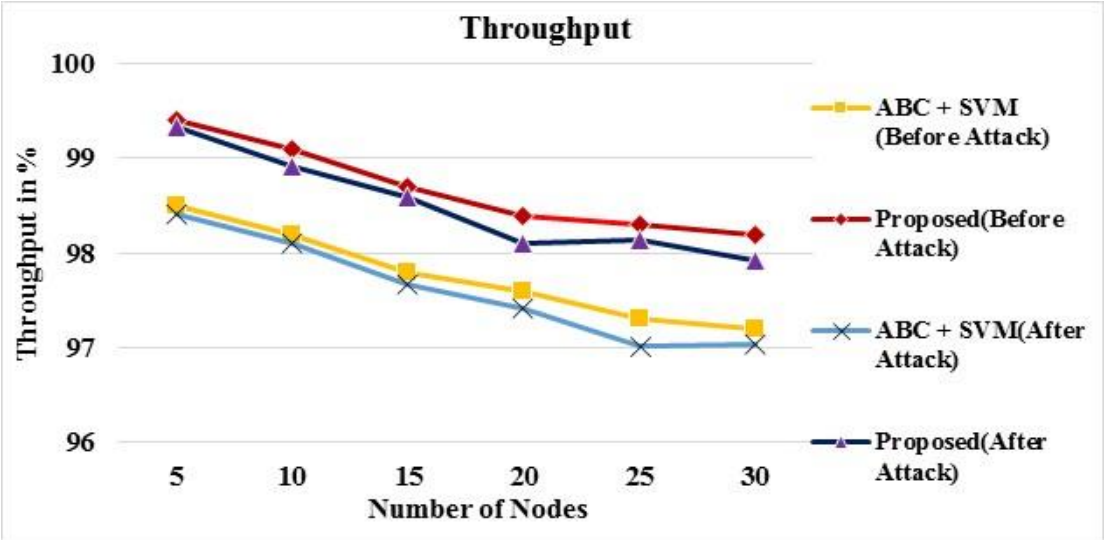

Fig. 4 Throughput Analysis

All the values of throughput are shown in Table III and plotted in Figure 4. It is observed for ABC with SVM and the proposed approach that the average throughput is 97.8 % and 98.7 %, respectively, before the attack. Whereas, for ABC with SVM and the proposed approach, the average throughput is 97.6 % and 98.5%, respectively, after the attack. The value of throughput improved with the proposed approach.

C. Latency Analysis

Latency is related to the time it takes in a network to deliver a packet from source to destination associated with it. The latency comparison is performed to calculate the delay in ms by considering the number of nodes for 5 to 30. Table IV mention the latency values in ms for the proposed and ABC with SVM before the attack, then proposed and ABC with SVM after the attack.

All the values of latency are shown in Table IV and plotted in Figure 5. It is observed in the case of before attack from the proposed approach that the average latency value of 1.27 ms is lower as compared to the average value of ABC with SVM, which is 1.87 ms.

Table IV. Latency Analysis

Number of Nodes	Attack (before)		Attack (after)	
	ABC and SVM	Proposed	ABC and SVM	Proposed
5	0.7	0.3	0.95	0.34
10	1.2	0.8	1.62	0.93
15	1.8	1.1	2.13	1.27
20	2.2	1.5	2.56	1.73
25	2.5	1.8	2.87	2.14
30	2.8	2.1	3.13	2.48

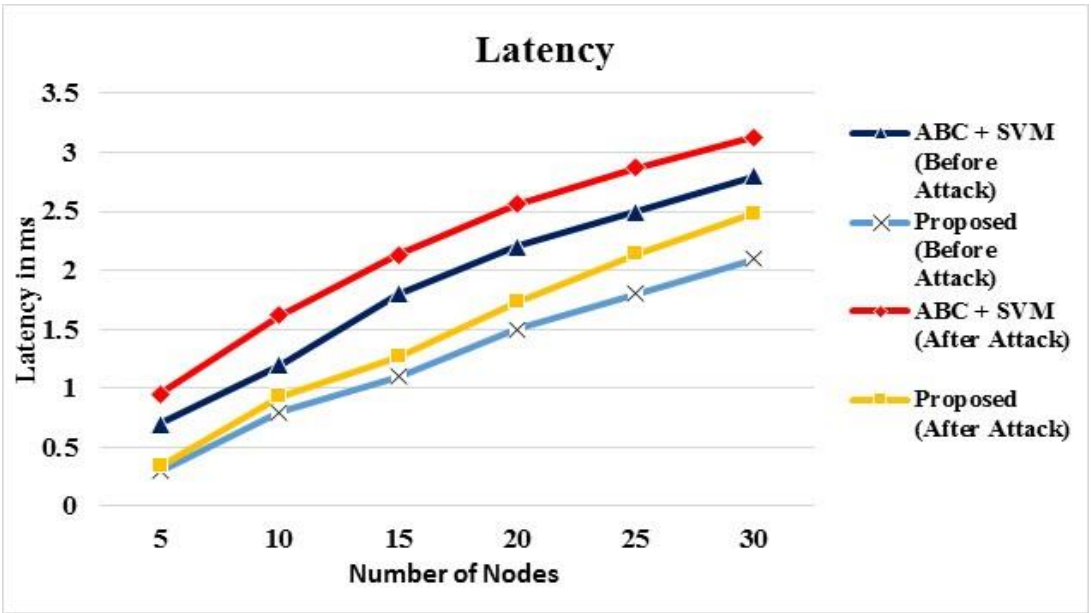

Fig. 5 Latency Analysis

Moreover, in the case of after attack, the average values of latency increased as 1.48 ms and 2.21 ms for proposed and ABC with SVM, respectively. The proposed approach shows the overall lower latency for improved and secure VoIP services.

D. Jitter Analysis

Jitter is one of the main criteria for the evaluation of the quality of service. Jitter in VoIP network is related to the variations of delay. It is calculated jitter values in ms by considering the number of nodes from 5 to 30. Table V mention the jitter values in ms for the proposed and Artificial Bee Colony (ABC) with SVM before the attack, then proposed and Support Vector Machine (ABC) with SVM after the attack. All the values of latency are shown in Table V and plotted in Figure 6.

Table V. Jitter Analysis

Number of Nodes	Attack (before)		Attack (after)	
	ABC and SVM	Proposed	ABC and SVM	Proposed
5	1.1	0.47	1.39	0.51
10	1.9	0.82	2.35	0.91
15	2.3	1.25	2.74	1.43
20	2.5	1.62	3.12	1.94
25	3.1	2.11	3.69	2.54
30	3.5	2.73	4.19	3.12

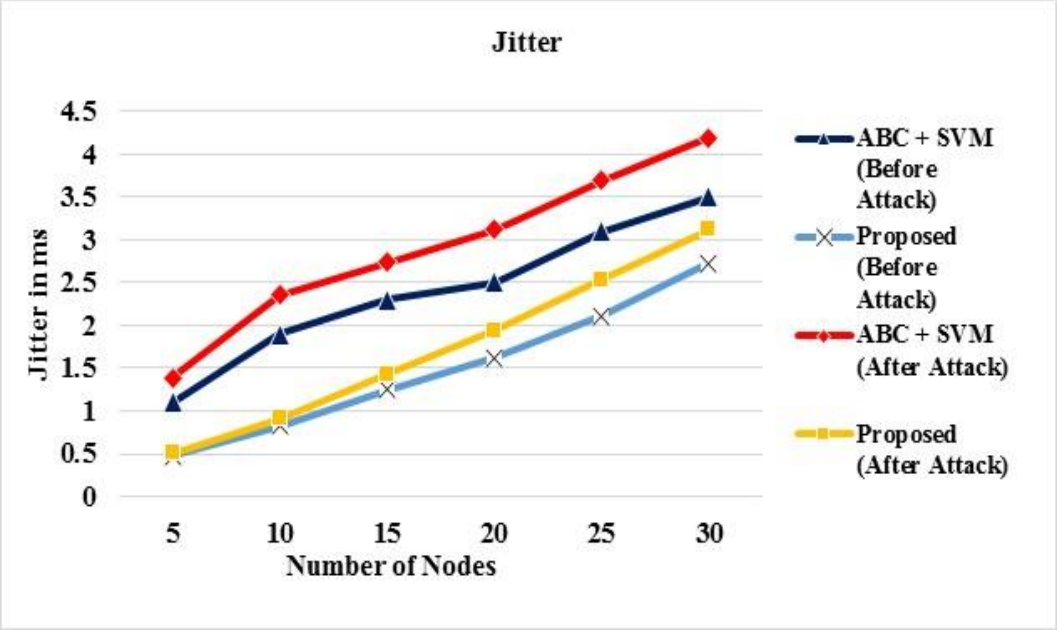

Fig. 6 Jitter Analysis

It is observed in the case of before attack from the proposed approach that the average jitter value of 1.5 ms is lower as compared to the average jitter value of ABC with SVM, which is 2.4 ms. However, in the case of after attack, the average values of latency increased to 1.74 ms and 2.91 ms for proposed and ABC with SVM, respectively. The proposed approach shows the overall lower jitter for VoIP applications.

V. CONCLUSION

This research work it is designed a VoIP network to enhance the QoS using MATLAB simulator. Also, the problem of handover in VoIP has been resolved by using INTER-SR and INTRA-SR in hybridization as routing algorithms. It has considered the number of nodes in the proposed work ranging from 5 to 30 and calculated the results with two scenarios, one before the attack and another after the attack.

The values for packet loss, throughput, latency and jitter are computed for the VoIP network. The results with the proposed approach as compared to the existing approach exhibit the lower loss of a packet with 1.13% (before the attack) and 1.29 % (after the attack). The throughput average with 98.7% (before the attack) and 98.5% (after the attack), Latency average with 1.27 ms (before the attack) and 1.48 ms (after the attack). The jitter average is 1.5 ms (before the attack) and 1.74 ms (after the attack). The proposed approach demonstrated the QoS parameters in terms of security of the VoIP network, which is an improvement as compared to the existing approach.

REFERENCES

[1] H. Petander, E. Perera, K. C. Lan, and A. Seneviratne, Measuring and improving the performance of network mobility management in IPv6 networks, IEEE Journal on selected areas in communications. 24(9) (2006) 1671-1681.

[2] M. Bouhorma, and A.A. Boudhir. VoIP over manet (voman): Qos & performance analysis of routing protocols for different audio codecs, International Journal of Computer Applications. 36(12) (2011) 22-26.

[3] F. Pacheco, E. Expósito, M. Gineste, A framework to classify heterogeneous Internet traffic with Machine Learning and Deep

Learning techniques for satellite communications, Computer Networks. 173 (2020) 1-31.
[4] G. Zhu, J. Zan, Y. Yang, and X. Qi, A supervised learning-based QoS assurance architecture for 5G networks, IEEE Access. 7 (2019) 43598-43606.
[5] Y. F. Huang, C. B. Lin, C. M. Chung, and C. M. Chen, Research on QoS Classification of Network Encrypted Traffic Behavior Based on Machine Learning, Electronics. 10.1376 (2021)1-24.
[6] M. A. Ridwana, N. A. M. Radzib, and F. Abdullah, Quality-of-Service Performance Comparison: Machine Learning Regression and Classification-Based Predictive Routing Algorithm, Turkish Journal of Computer and Mathematics Education (TURCOMAT). 12(14) (2021) 2808-2817.
[7] T. Chakraborty, S. Ghosh, S. Barik, S. Kar, and S. Chatterjee, VoIP-HDK2: A novel channel allocation technique for QoS aware VoIP communication over heterogeneous networks, Procedia Computer Science. 171 (2020) 62-71.
[8] G. Ilievski, and P. Latkoski, Efficiency of Supervised Machine Learning Algorithms in Regular and Encrypted VoIP Classification within NFV Environment, Radioengineering. 29(1) (2020) 243-250.
[9] D. Gao, J.Cai, C. H. Foh, C. T. Lau, and K. N. Ngan, Improving WLAN VoIP capacity through service differentiation, IEEE Transactions on Vehicular Technology. 57.1 (2008) 465-474.
[10] V. Kumar, and O. P Roy, Reliability and security analysis of VoIP communication systems, Rising Threats in Expert Applications and Solutions, Singapore: Springer. (2021) 687-693.
[11] J. Pieper, J. Frey, C. Greene, Z. Soetan, T. Thompson, and S. Voran, Mission-critical voice quality of experience access time measurement methods, US Department of Commerce, National Institute of Standards and Technology. 8275 (2019) 1-49.
[12] Z. G. Hu, H. R. Yan, T. Yan, H. J Geng, and G. Q Liu, Evaluating QoE in VoIP networks with QoS mapping and machine learning algorithms, Neurocomputing. 386 (2020) 63-83.
[13] O. Gavilanez, F. Gavilanez, and G. Rodriguez, Audit Analysis Models, Security Frameworks and Their Relevance for VoIP. arXiv preprint arXiv 1704.02440 (2017) 143-151.
[14] W. Nazih, Y. Hifny, W. Elkilani, T. Abdelkader, and H. Faheem, Efficient detection of attacks in SIP-based VoIP networks using a linear l1-SVM classifier, International Journal of Computers Communications & Control. 14(4) (2019) 518-529.
[15] W. Nazih, Y. Hifny, W.S. Elkilani, H Dhahri, and T Abdelkader, Countering DDoS Attacks in SIP Based VoIP Networks Using Recurrent Neural Networks, Sensors. 20.5875 (2020) 1-15.
[16] Z. Tsiatsikas, A..Fakis, D. Papamartzivanos, D. Geneiatakis, G. Kambourakis, and C. Kolias, Battling against DDoS in SIP: Is Machine Learning-based detection an effective weapon?, 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE) IEEE. 4 (2015) 301-308.
[17] B. Son, E. Nahm, and H. Kim, VoIP encryption module for securing privacy, Multimedia tools and applications 63(1) (2013) 181-193.
[18] R. Shankesi, M.Al-Turki, R Sasse, CA Gunter, and J. Mesequer, Model-checking DoS amplification for VoIP session initiation, European Symposium on Research in Computer Security, Heidelberg, Berlin: Springer. (2009) 1-320.
[19] J. Lee, K. Cho, C. Y. Lee, and S. Kim, VoIP-aware network attack detection based on statistics and behavior of SIP traffic, Peer-to-Peer Networking and Applications. 8(5) (2015) 872-880.
[20] G. Vennila, M. S. K. Manikandan, and M. N. Suresh, 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. 30(11) (2017) 1-15.
[21] M. Usama, J. Qadir, A. Raza, H. Arif, K. L. A. Yau, and Y. Elkhatib, Unsupervised machine learning for networking: Techniques, applications and research challenges, IEEE access. 7 (2019) 65579-65615.
[22] O. Salman, I. H. Elhajj, A. Kayssi, and A. Chehab, A review on machine learning-based approaches for internet traffic classification, Annals of Telecommunications. 75(11) (2020) 673-710.
[23] R. Moreira, F. D. O. Silva, P. F. Rosa, and R. L. Aguiar, A smart network and compute-aware Orchestrator to enhance QoS on cloud-based multimedia services, International Journal of Grid and Utility Computing. 11(1) (2020) 49-61.
[24] A. I. Owusu, and A. Nayak, An Intelligent Traffic Classification in SDN-IoT: A Machine Learning Approach, IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), IEEE. 7127(2) (2020) 1-6.
[25] C. Alvares, D. Dinesh, S. Alvi, T. Gautam, M. Hasib, and A. Raza, Dataset of attacks on a live enterprise VoIP network for machine learning-based intrusion detection and prevention systems, Computer Networks. 197 (2021) 108283.
[26] D. R Militani, H. P de Moraes, R. L Rosa, L. Wuttisittikulkij, Enhanced Routing Algorithm Based on Reinforcement Machine Learning—A Case of VoIP Service, Sensors. 21(2) (2021) 504.
[27] Y. Zhou, and A. Zhang, Improve the DFI-based Network Traffic Classification Performance by Using QoS Metrics, Journal of Advances in Computer Networks. 8(2) (2020)36-43.
[28] Z. Zhu, C. Wu, C. Ji, and X. Wang, Machine learning assisted OSP approach for improved QoS performance on 3D charge-trap based SSDs, International Journal of Intelligent system. 22286 (2020)1-14.
[29] A. Akbar, M. Ibrar, M. A. Jan, A. K. Bashir, and L. Wang, SDN-Enabled Adaptive and Reliable Communication in IoT-Fog Environment Using Machine Learning and Multi-objective Optimization, IEEE Internet of Things Journal. 8.5 (2020) 3057-3065.
[30] S. K. Sharma, and X. Wang, Toward massive machine-type communications in ultra-dense cellular IoT networks: Current issues and machine learning-assisted solutions, IEEE Communications Surveys & Tutorials. 22.1 (2019) 426-471.
[31] A. Saeed, and M. Kolberg, Towards optimizing WLANs power saving: Novel context-aware network traffic classification based on a machine learning approach, IEEE Access. 7 (2018): 3122-3135.
[32] S. Gebru and P. Kadam, Simulation Based performance evaluation and comparison of wired VoIP services over UDP and SCTP protocol, International Journal of Engineering Trends and Technology (IJETT), 33.9 (2016) 462-467.
[33] S. Jalendry and S. Verma, A Detail Review on Voice over Internet Protocol (VoIP), International Journal of Engineering Trends and Technology (IJETT), 23(4) (2015) 161-166.