A Reliable and Secure Wireless Network for VoIP Applications

Vinod Kumar and O. P. Roy

Abstract In a wireless communication system, the Quality of Service (QoS) becomes an active area of research as the demand for real-time applications like voice or video communication increases day by day. In this paper, a new hybrid INTER-SR & INTRA-SR based reliable wireless network is designed for Voice over Internet Protocol (VoIP) applications. It is mainly consisting of one optimization algorithm named as Genetic Algorithm (GA) in conjunction with two classification approaches such as Artificial Neural Network (ANN) and Support Vector Machine (SVM). The proposed algorithm selects a reliable and more reliable route based on the nodes properties such as energy consumption and delay. In the end, three distinct QoS parameters such as routing overhead, delay and jitter are analyzed for two communication scenarios such as with attack and without attack in MANET simulator. The results demonstrate that the proposed algorithm performs with satisfying results compared to individual routing and optimization approaches.

Keywords Wireless network · Voice over internet protocol · Reliability · INTER-SR · INTRA-SR · GA · SVM · ANN

1 Introduction

The present day's society observes a revolutionary change in communication technologies to make life comfortable. VoIP is the technology to make communication possible over IP networks [1]. Using VoIP is very advantageous such as cost per call [2]. Further, VoIP technique suffers from many disadvantages, which makes people still remain on phone calls [3]. The major drawback faced by the VoIP calls is the packet loss and the delay that occurs during the congestion problem over IP networks. Another problem is the wastage of bandwidth [4]. A list of codecs along with their

V. Kumar (✉) · O. P. Roy
Department of EE, NERIST, Nirjuli, Arunachal Pradesh 791109, India
e-mail: vinodnerist@gmail.com

O. P. Roy
e-mail: oproy61@gmail.com

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2020

P. K. Mallick et al. (eds.), *Electronic Systems and Intelligent Computing*, Lecture Notes in Electrical Engineering 686, https://doi.org/10.1007/978-981-15-7031-5_1

Table 1 Codec in general VoIP

Codec	Format size	Codec	Format size
G. 729	10	G. 729 A	10
LPC	14	G-723.1	30
G. 729 E	10	G-729 D	10

format size is listed in Table 1. The payload produced by VoIP is small as the VOIP is sensitive to delay; the larger is the size of the payload, more time is required by the VoIP to generate the payload, and hence increase the delay. VoIP systems still exist on data networks that means there may be a lack of security and types of attacks related to any data network [5, 6]. In the VoIP, the voice message is translated into IP packets. The data travels from different access points and chances of data loss increases within the route while transmitting the data from its source to destination [7]. From an existing survey, it has been observed that Denial of Service is one of the most common attacks that affect VoIP data. Therefore, it is necessary to design a reliable network.

2 Related Work

A number of protocols are coming into existence with improved security features, but still not meet the desired requirement. Gupta and Shmatikov [8] have presented a reliable network of VoIP protocol. The researchers started a replay attack that affects voice and break the security of the transport layer [8]. VoIP evaluation has also been performed by Audah et al. [9] using distinct codec schemes in NS-2 simulator The author has examined the performance in terms of Quality of Service (QoS) [9]. Also, Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporally-Ordered Routing Algorithm (TORA) have been analyzed in OPNET simulator [10]. It has been concluded that the data VoIP packet transmission using the TORA protocol has been transmitted with better quality against the large data traffic [10]. Furthermore, for VoIP data transmission carried out using AODV and DSR routing mechanism has been conducted by Jasani [11]. The results indicate that data transmission using AODV routing is more suitable compared to DSR while VoIP packet is transmitted in the MANET network [11]. Sanchez-Iborra and Cano [12] have investigated the quality of MANET routing protocols in transmitting video data using OLSR and AODV [12].

3 Proposed Algorithm

The objective is to make VoIP data reliable and secure. A number of researchers have contributed in this direction but not attained desired security. To increase data security

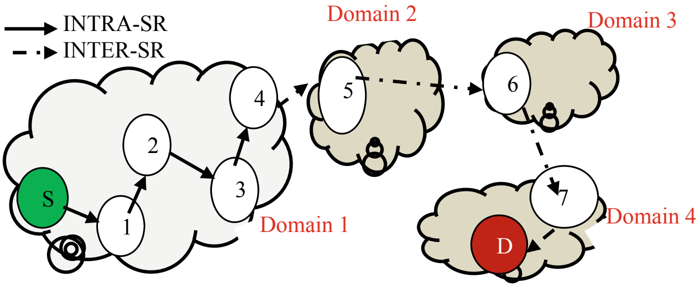

Fig. 1 Simulation area of (1000 × 1000 m^2)

of VoIP application, SVM and ANN are used for decreasing routing overhead and packet loss. The route has been selected based on the concept of INTER-SR (Inter-State Routing) and INTRA-SR (Intra State Routing). INTER-SR is a type of protocol in which the data is transmitted from one domain to another domain, whereas, in INTRA-SR, the data is transmitted within the domain.

3.1 Network Design

A network of 1000 × 1000 m^2 is created with N number of nodes as shown in Fig. 1. Nine nodes are deployed denoted by (1–7), S and D. Nodes 1 to 4 and S comes under domain 1 and the route formation occurred due to INTRA-SR process. To reach data from source to destination, we also need INTER-SR technique in combination with INTRA-SR technique.

3.2 Security and Prevention

The problem of routing in VoIP-based communication model is solved by integrating INTRA-SR and INTER-SR approach. The problem of security and prevention is not covered by this approach, explained in the result and analysis.

To resolve this problem, we designed a hybrid mechanism using SVM and ANN techniques. SVM is a binary classifier for checking two conditions for the malicious node or genuine node. To validate the detection probability of SVM for the malicious or normal node, ANN and SVM are used as a classifier. In route formation, the data is transmitted to the nearby node as shown in Fig. 2, node 2 pass VoIP packet to node 3 by using the concept of distance. But, the routing mechanism of VoIP does not check whether the node is dropping the message or not. To degrade the VoIP packet drop of the proposed wireless network, an optimization scheme has been used with novel fitness function. The fitness function helps to select the node as in Table 2.

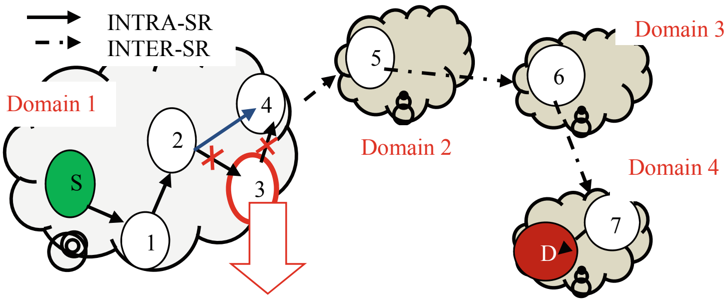

Fig. 2 Reliable network using GA with (SVM & ANN) approach

Table 2 Node's properties

Nodes	Energy consumption (mJ)	Delay (ms)
2	10	4
3	12	3
4	12	2

In domain 1, during route formation, VoIP message packet is forwarded by node 1 to node 3. But, node 3 is not an accurate node as it drops data packet. It is necessary to pass data to a genuine node, which has been performed here, using GA. The GA checks energy consumed by each nearby node as in our example, node 3 and node 4 consumes same energy, therefore, in such condition, one must go for checking other parameters that is a delay in this case. Node 4 forward data with less delay (≅2 s) and hence node 1 transmits data to node 4.

Malicious Detection of VoIP communication using GA with SVM and ANN

Required Input: T ← Training Data as nodes properties. C ← Target/Category in terms of communicating and non-communicating nodes. N ← Number of Neurons, MN ← Malicious Nodes,

Obtained Output: Start

1 **To optimized the T, Genetic Algorithm (GA) is used**

2 **Set up basic parameters of GA:** Population Size (P) – Based on the number of properties, CO – Crossover Operators, MO – Mutation Operators OT – Optimized Training Data **Fitness Function**:

$$F(f) = \begin{cases} 1(True); & if\ F_s < F_t = Threshold_{Properties} \\ 0(False); & Otherwise \end{cases}$$

where F_s: Current Node Properties and F_t: Threshold properties for all nodes based on energy consumption, delay and position

Calculate Length of T for R
Set Optimized Training Data OT = [] For i in range of R
$F_s = T(i) = SelectedNode_{Properties}$. // Current Data from N
$F_t = Threshold_{Properties}$. // Average of All Data
$F(f) = FitFun(F_s, F_t)$. Nvar = Number of variables
$Best_{Prop}$ = OT = GA (F(f), T, Nvar, Set up of GA)
End – For SVM training data initialization OT - Nodes optimized
For I = 1→ All Nodes If Node Property (I) == Real
Define Cat category of training data Cat (1) = Node Properties (I)
Else Cat (2) = Node Properties (I) **End - If**
End – For Train_Struct=SVMTRAIN (T, Cat, Kernel function)
OT= Train_Structure.SupportVector //finding ANN training data
Initializing ANN basic parameters – Number of Epoch (E) // ANN Iterations – Number of Neurons (N)
F i = 1 → OT If T belongs to the properties of communicating nodes
Group (1) = Training data properties according to renodes
Else if T belongs to properties of non-communicating nodes
Group (2) = Training data properties for non-real nodes
Else Group (3) = Training data Extra properties **End – If**
End – For Initialize ANN for data
VoIP-Net = Newff $(T, Group, N)$
VoIP = Train (VoIP, Training data, Group) **Testing:**
Current Node = Nodes Properties in Cloud-Net
Authentication = simulate (Cloud-Net, Current Node)
If Authentication = True Genuine node not consider as a malicious
Else MN = Malicious Node
End Return: MN a list of Malicious Nodes
End

Above algorithm is designed using hybridization of SVM, ANN and GA. Algorithm first uses SVM using radial basis function (RBF) as a kernel and find the most helpful properties for ANN which are called support vectors. ANN is used to train and classify nodes authorization which helps in the improvement of network performance.

4 Results and Analysis

In this research, the performance of the communication system for VoIP message transmission is considered with two cases, one communication without attack and another communication with attack. The effect of occurring malicious node inside the network when making the voice call and data packet transmitted between the source and destination node through different domain nodes have been discussed. The performance has been analyzed by constructing network with multiple nodes (5, 10, 15, 20, 25 and 30). The quality of transmitting VoIP message transmission has been observed on the basis of delay, packet loss and throughput. The network simulation environment consists of 30 numbers of nodes that were positioned randomly using random waypoint as a mobility model. The simulation parameters are mentioned in Table 3. The results such as routing overhead, average delay and average jitter have been computed in two scenarios that is communication with and without attack. To obtain accurate results, the network is simulated at least ten times and their average values are noted in the form of Tables 4, 5 and 6.

Figure 3 demonstrates the routing overhead for a reliable network that is used for VoIP application. A very close variation has been observed for three different approaches such as (1) with INTER-SR & INTRA-SR, (2) with GA and (3) for Proposed Algorithm. For route construction, INTER-SR with INTRA-SR has been used, which enables the user to communicate with the remote user that is located in different domains. The route optimization is performed with GA as an optimization technique. GA helps to find the properties of each node based on energy consumption, delay and node's coordinate and the data transmission is done based on node's properties rather than the concept of the closest node within the route. Later on, the problem of identifying the best node has been resolved using SVM in hybridization with the ANN algorithm. The graph is shown in Fig. 3 indicates that the proposed

Table 3 Simulation parameters

Considered parameters	Variation of parameters
Area	1000×1000 m^2
Nodes	5, 10, 15, 20, 25 and 30
Number of malicious nodes	10
Simulation time (s)	400 s
Routing protocol	INTER-SR and INTRA SR
Mobility model	Random waypoint

Table 4 Routing overhead analysis

Number of nodes	Communication without attack			Communication with attack		
	INTER-SR & INTRA-SR	With GA	Proposed algorithm	INTER-SR & INTRA-SR	With GA	Proposed algorithm
5	2540	2000	1800	4521	3254	1726
10	3002	2154	1985	5264	3642	1875
15	4251	3869	3125	5728	4782	3745
20	5126	3985	3547	6357	4759	3675
25	6482	5264	4597	8581	5025	4871
30	7356	6542	5942	9264	6235	5297

Table 5 Delay analysis

Number of nodes	Communication without attack			Communication with attack		
	INTER-SR & INTRA-SR	GA	Proposed algorithm	INTER-SR & INTRA-SR	GA	Proposed algorithm
5	1	0.6	0.5	5	4	2
10	6	5	4	8	8	4
15	8.2	8	2	14	10	5
20	15	9	2	16	12	6
25	25	11	2.5	22	19	8
30	30	18	10	40	22	10

Table 6 Jitter analysis (ms)

Number of nodes	Communication without attack			Communication with attack		
	With INTER-SR & INTRA-SR	With GA	Proposed algorithm	With INTER-SR & INTRA-SR	With GA	Proposed algorithm
5	1.9	1	0.3	3.5	3	2.5
10	1.8	1.1	0.35	7	5.9	3
15	6.5	3.2	1.8	16	14	4.6
20	11.5	4	2.5	20	18	8.7
25	8	4.2	3	21	20	12
30	15	6.5	4.5	28	22	24

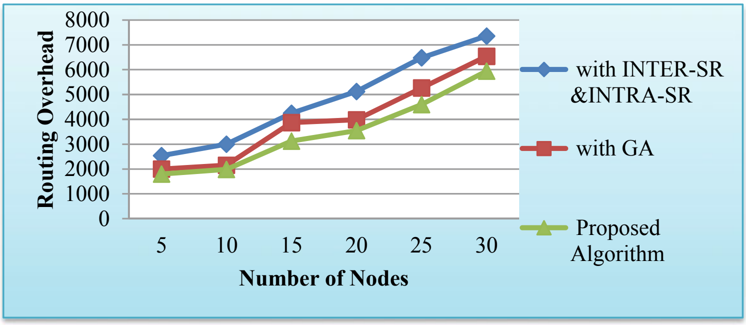

Fig. 3 Routing overhead without Attack

algorithm transmits data with small routing overhead compared to individual routing and routing with optimization approach.

Figure 4 represents the routing overhead observed with the variation of the number of nodes in the presence of an attack. The graph indicates that with the increase in

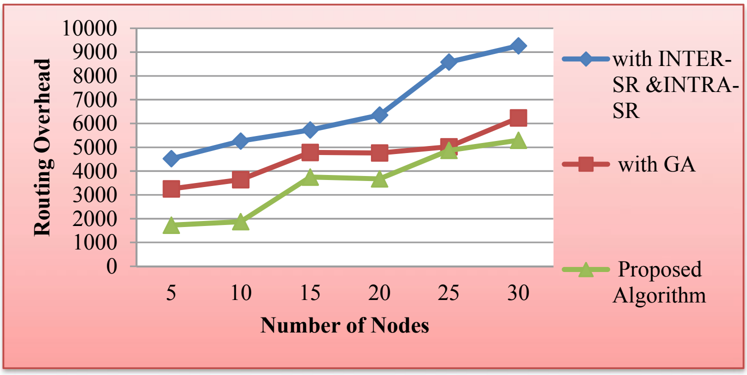

Fig. 4 Routing overhead with Attack

the communicating nodes within the network, the routing overhead increased and the maximum routing overhead measured for 30 numbers of nodes with INTER-SR and INTRA-SR, with GA and for the proposed algorithm are 9264, 6235, and 5297, respectively.

To show the effectiveness of the proposed algorithm, we evaluated average delay and jitter by generating VoIP messages in a large amount. The attained results related to average delay obtained without and with attack are shown in Figs. 5 and 6. The difference of delay values measured with INTER-SR and INTRA-SR, with GA and for combination of all that is proposed algorithm has been presented in Fig. 5. From the above graph, it has been observed that the average delay values recorded for with GA are almost twice and for the proposed algorithm almost thrice compared to the simple routing techniques performed by INTER-SR and INTRA-SR combination.

The jitter observed without attack and with the attack for VoIP application with three different algorithms is shown in Figs. 7 and 8, respectively. It is clear from Figs. 7 and 8 that when the classification algorithm in addition to the optimization approach is used, the occurrence of jitter has been reduced in a great extent.

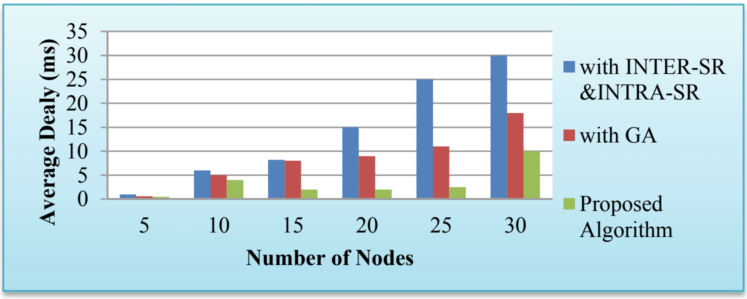

Fig. 5 Average delay without attack for VoIP application

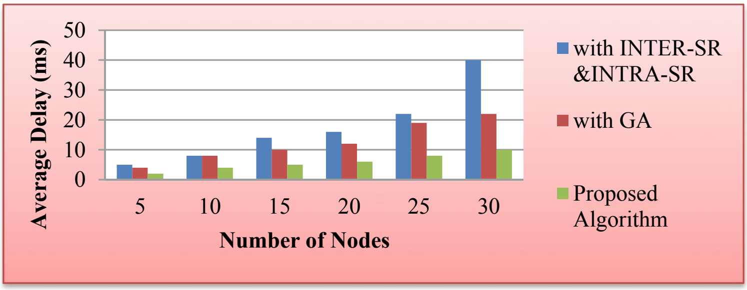

Fig. 6 Average delay with attack for VoIP application

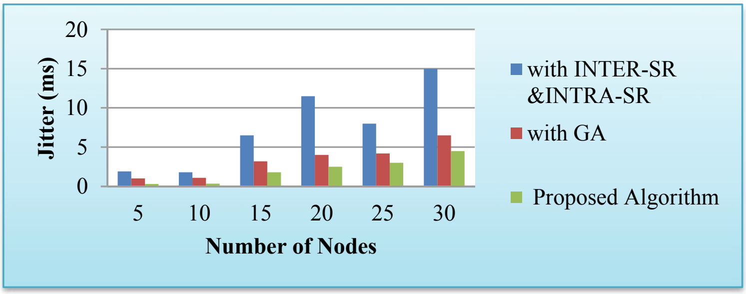

Fig. 7 Average jitter without attack for VoIP application

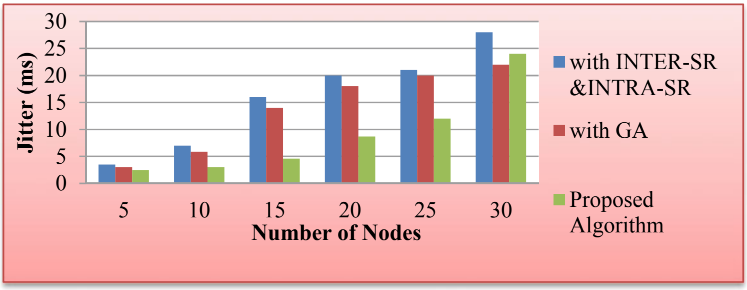

Fig. 8 Average jitter with attack for VoIP application

5 Conclusion

In the paper, we have presented a reliable wireless network for VoIP-based applications. For routing, the concept of INTER-SR and INTRA-SR has been used to resolve the problem of handover as the data has to be transmitted from one domain to another domain. Two different scenarios of data communications such as in the presence of with and without attack have been presented for three approaches as discussed in the results and analysis section. The performance of the designed network has been examined based on routing overhead, average delay and average jitter for VoIP application. The results demonstrated that better results compared to existing routing protocol has been obtained that guarantee the desired delay and jitter required for data transmission in VoIP applications in a wireless network.

References

1. Mohd Ali A, Dhimish M, Mather P (2019) WLAN protocol and network architecture selection for real-time applications (2019)
2. Chakraborty T, Misra IS, Prasad R (2019) VoIP over wireless LANs—Prospects and challenges. In: VoIP technology: applications and challenges, Springer, Cham, pp 71–93
3. Alsaadi MS, Alotaibi ND (2019) Routing protocols design and performance evaluation in wireless mesh networks. Int J Technol Diffus (IJTD) 10(1):60–74
4. Chakraborty T, Misra IS, Prasad R (2019) Technique for Improving VoIP performance over wireless LANs. In: VoIP technology: applications and challenges, Springer, Cham, pp 95–121
5. Abualhaj MM, Al-Tahrawi MM, Al-Khatib SN (2019) A new method to improve Voice over IP (VoIP) bandwidth utilization over Internet Telephony Transport Protocol (ITTP). In: Proceedings of the 2019 8th international conference on software and information engineering.ACM, pp 192–195
6. Estepa R, Estepa A, Madinabeitia G, Davis M (2018) Improving the energy efficiency of VoIP applications in IEEE 802.11 networks through control of the packetization rate. In: XIII Jornadas de Ingeniería telemática (JITEL 2017). Libro de actas, pp 23–29
7. Hsieh WB, Leu JS (2018) Implementing a reliable VoIP communication over SIP-based networks. Wirel Netw 24(8):2915–2926
8. Gupta P, Shmatikov V (2006) Key confirmation and adaptive corruptions in the protocol security logic. In: Proceedings of the Joint Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA'06), pp 113–142
9. Audah L, Kamal AAM, Abdullah J, Hamzah SA, Razak MAA (2015) Performance evaluation of voice over IP using multiple audio codec schemes. Asian Research Publishing Network (ARPN). J Eng Appl Sci 10:8912–8919
10. Ravikanti S, Preeti G (2015) Evaluating the performance of reactive unicast routing protocols with OPNET simulator in MANETS under VOIP. Int J Innov Res Sci Eng Technol **4**(7) (2015)
11. Jasani H (2012) Evaluations of AODV and DSR for QoS requirements. In: Proceedings of the 1st annual conference on research in information technology ACM, pp 1–6 (2012)
12. Sanchez-Iborra R, Cano MD (2014) An approach to a cross layer-based QoE improvement for MANET routing protocols. Netw Protocols Algor 6(3):18–34