Mitigating Gray Hole attack in Mobile AD HOC Network using Artificial Intelligence Mechanism

Puneet Kamal, Rajeev Sharma, Abhishek Gupta, Gaurav Kumar

Abstract*: A mobile ad hoc network (MANET) is a combination of multiple mobile nodes, which are interconnected by radio link. In MANET, sensor nodes are free to move, and each node can act as a host or router. Routing is one of the most challenging tasks because nodes move frequently. Therefore, in MANET, the routing protocol plays an important role in selecting the best route to efficiently transmit data from the source node to the destination node. In this paper, the best path with efficient Ad Hoc on Demand Distance Vector (AODV) routing protocol is chosen as the routing mechanism. The properties of each node are categorized using firefly algorithm. The Artificial Neural Network (ANN) is trained as per these properties and hence in case if the gray hole node is detected within the route, it is identified and the route between the source and the destination is changed. At last, to show how effectively the proposed AODV with Firefly and ANN works is computed in terms of performance parameters. The throughput and PDR is increased by 4.13 % and 3.15 % compared to the network which is affected by gray hole attack. The energy up to 44.02 % has been saved.

***Index Terms*: Mobile ad hoc network, gray hole attack, cuckoo search, support vector machine, Ad Hoc On-Demand Distance Vector**

I. INTRODUCTION

In recent years in the era of mobile networking, Mobile Ad Hoc Network (MANET) has achieved good popularity among the researchers. The basic concept of MANET is based on the presented devices that are joined to each other to build the network [1]. It is totally different from other old presented network or traditional networks. MANET is not based on any type of pre-defined network or any infrastructure to carry out their actions. The changing nature of MANET minimizes its cost and working interval of time. The basic structure of Mobile Ad Hoc Networks is shown in Fig. 1. The routing protocols that started the multi-hop data transfer in these networks build the backbone of MANET. The type of attack on these networks must be changed by change with the change in the topology presented in these dynamic networks [2]. To deal with such type of attacks the routing protocols presented in this network must be powerful. The routing protocols must be deal with changing topologies but the mischievous attacks remain the concern to be fixed. Now, by calculating the performance of MANET, the functionality that it supports can be identified. Network layer parameters can be termed as the network performance metrics that are evaluated and resolve in this research [3].

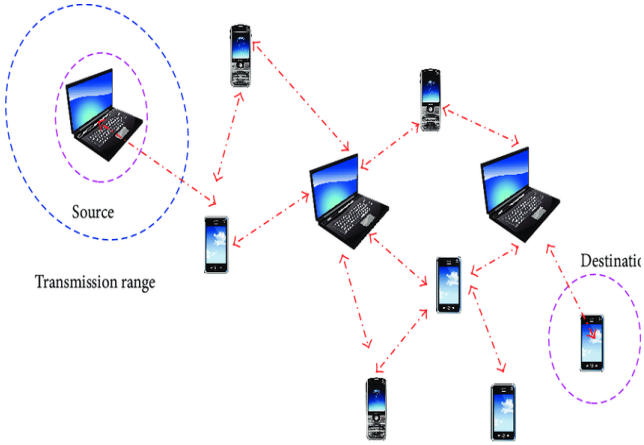

Figure 1: Mobile ad hoc network [5]

A. MANET Routing

In MANET, a particular device work as a host as well as a router. All the nodes presented in the topology are considered to be cooperative and trustworthy in all the routing protocols like ad hoc on-demand distance vector (AODV), Dynamic source routing (DSR) etc. Due to this, the MANET routing protocols are very susceptible to a different type of denial of service (DoS) attacks, mainly packet dropping attack. Packet dropping attack may be divided into Full packet drop and Partial packet drop attack. Black hole attack is the keyword used for full packet drop attack and the grey hole attack is the term used for partial packet drop attack. The particular nodes do not take part in the action of route discovery in Full packet drop attack. It used to draw the data traffic by the help of false routing information [4]. Black hole attack trickles all the data packets received by it. The un-wanted node takes part generally in the process of route discovery in Partial packet drop attack. It forwards the general reply packet received from the destination.

The capability of the network is slightly decreased when the source node sends the data packets through the path in which the gray hole node. The efficiency degrades as some of the data packets are dropped on the way. As a result, to deal with attacks, there is a need to provide security in the ad-hoc network. Due to this reason, Mitigating Gray hole Attack

Revised Manuscript Received on June 15, 2019.

Puneet kamal, Computer Science and Engineering, Chandigarh Engineering College, Landran, Mohali, India.
Rajeev Sharma,Computer Science and Engineering, Chandigarh Engineering College, Landran, Mohali, India.
Abhishek Gupta,Computer Science and Engineering, Chandigarh Engineering College, Landran, Mohali, India
Gaurav Kumar,Computer Science and Engineering, Chandigarh Engineering College, Landran, Mohali, India

mechanism is introduced which helps in reducing the impact of smart gray hole attack in the network [5].

B. Gray hole attack

Gray hole attack or in another word selective forwarding attack can be term as the rejection of the service attack. Gray hole attack is totally different from a black hole attack. Here; Firstly the sensor node does not part as a malevolent but after some time it turns into malevolent one and becomes malicious as it trickles selective data packets. There are two types of gray hole attacks in the MANET as illustrated in Fig. 2. The first one in the class of gray hole attack is a Sequence Number based gray hole attack. In this type of class, the node gives a false route reply by transporting high destination sequence number with minimal hop count to the source node [6]. On getting the reply packets the source node starts transporting the data packets with the help of the route which contains gray hole node. After that selectively drops the data packets. The second type of class of gray hole attack is Smart gray hole attack. It is totally different from the sequence number based gray hole attack in which the node behaves normally through the route discovery process. After that , it drops several feature of the data packets. The gray hole node functions in an erratic manner in the network and as a result, it is difficult to find these type of attacks rather than the black hole node where the damaged node drops all the essential data packets [7].

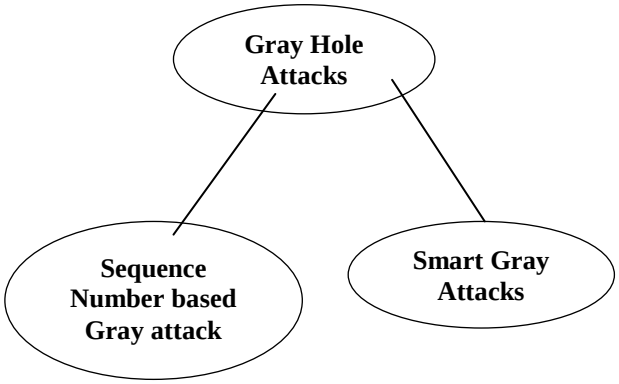

Figure 2: Type of gray hole attack

II. RELATED WORK

MANET employed a number of routing protocols for the transmission of data as per the demand generated by the destination node. Numerous of researchers have used different routing algorithms as well as techniques to distinguish gray hole node in MANET, a few of those are described in the following section.

Shalika, et.al (8, 2017) have presented a protective mechanism against the malicious nodes that exist within the AODV routing protocol. Support Vector Machine (SVM) has been used to differentiate the behaviour of the nodes. A threshold value has been set, if the value is higher than the defined value the node is considered as malicious node otherwise considered as a genuine node.

Jaspal Kumar et.al (9, 2013), have analyzed the effect of black hole node against the AODV routing protocol. The effect of black hole attack is determined with high efficiency.

Gurung and Chauhan (10, 2019) Have presented a modified AODV protocol, which works on the basis of the sequence number. The effect has been analyzed to detect the black hole node in various size of the network. The performance has been increased in terms of PDR, throughput but the routing overheads are increased.

Swapnil et al. (11, 2019) have studied different routing algorithms such as AODV, DSDV and DSR. Also, the effect of malicious nodes such as gray hole node, black hole nodes has been discussed. In addition, a comparative analysis was conducted between preventive trust-based protocols to ensure high security and minimize the impact of these malicious attacks. The DSR protocol under black hole attack is implemented and the performance of packet transmission rate, throughput, and a number of received packets and the average end-to-end delay has been analyzed. Improvements in these factors of the agreement make it safer and more reliable. Therefore, it applies to areas where security is critical.

III. Methodology

In this research, a network is designed by deploying n number of nodes in a defined area network of height and width (1000×1000) square meter as shown in the fig.3 below.

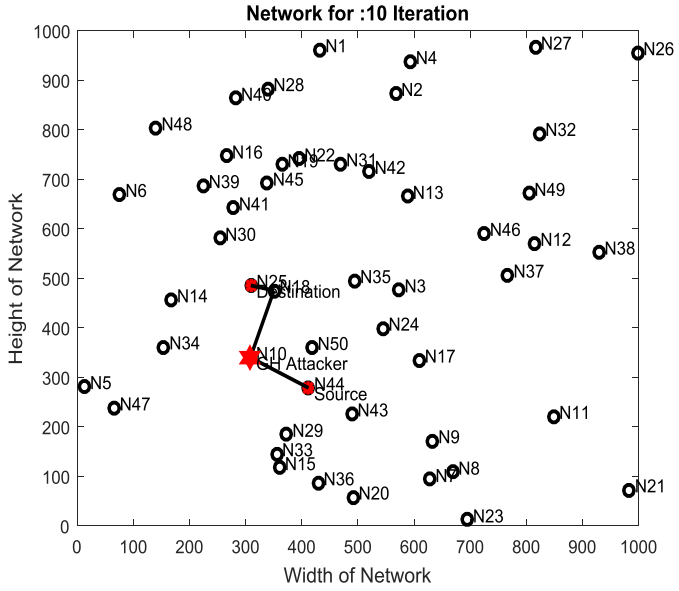

Figure 3: Network area with Route Formulation

The route is formed between source and destination using AODV as a routing protocol. AODV routing algorithm works in two phases (i) Route Discovery (ii) Route Maintenance. Initially, the route request is sent by the source node by transmitting Hello packet to their neighboring nodes.For the data transmission source node generates RREQ (Route request) within the entire network.

The nodes N1, N4 and N3 are the nearby nodes of the source device. In response to this RREQ message, N1 sends a RREP (Route Reply) by intimating the source node that it has the desired route and stored the address into its table.

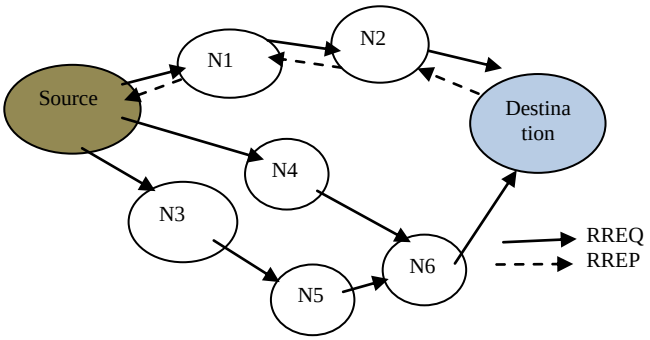

Figure 4: AODV Process

The same process is repeated by the node N2 and hence after the formation of route data transmission starts. The algorithm followed during the experiment is written below. The problem in this process is that the AODV does not know about the genuinity of the node that whether it is actual or fake node. Therefore, to resolve this problem, the properties of nodes are categorized based on the fitness function of Firefly Algorithm.

Algorithm: Firefly

Input: Nodes properties (delay, energy consumption)
Output: List of nodes

Initialize Firefly Algorithm: Network Area, Number of nodes and number of rounds

Defined Fitness function and properties of Nodes
For (I = 0 to Rd)
For (J = 0 to R)
For all Pop
Calculated value of R and find R_{best} node's property
If value (R) < value (R_{best})
Update light intensity of node' = I_L
End
End
End
Best Node = Sort (= I_L, FitFun)
Create a list of nodes

End
Return; List of nodes= genuine and gray hole node
End

A value has been selected based on the nodes collision rate, delay and energy consumption rate. On the basis of these properties, a well-known classifier named as ANN is trained, which helps to distinguish among the gray hole node and the genuine node. The trained architecture of ANN is shown in the fig.5.

The layers with different neurons are shown in fig. 5 marked by red colour. The algorithm on which the training process is completed is performed using "Levenberg-Marquardt" principle. The progress of trained structure is measured on the basis of different parameters marked under yellow block and plots as represented below.

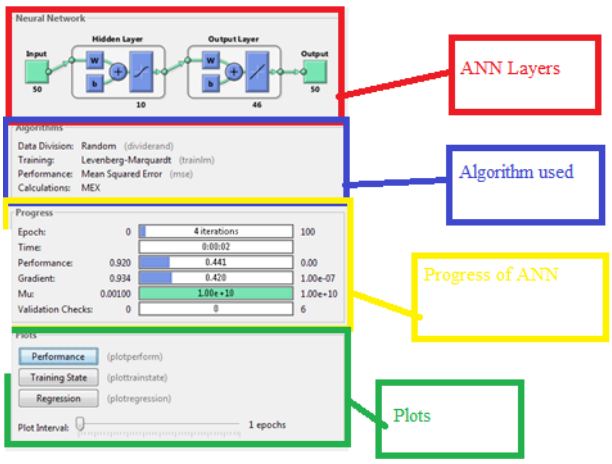

Figure 5: Trained ANN Structure

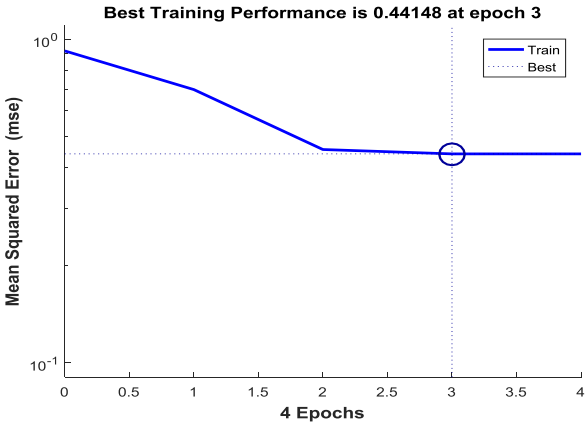

Figure 6: MSE of ANN

The performance of trained ANN is measured on the basis of Mean Square Error parameters. Less is the MSE higher is the training rate of ANN. The MSE of trained ANN structure used in the proposed work is depicted by a circle. The algorithm for ANN is written below.

ANN Algorithm:

Input: List of nodes as a Training Data (T_r), Target (G) and Neurons (N)
Output: Classified gray hole node
Initialize the performance parameters: Epochs (E), MSE, Gradient, Mutation and Validation Points
For each set of T_r
$Group = Categories\ of\ Trainingdata$
End
Initialized the ANN by applying T_r and G
Net = Newff (T_r, G, N)
Set the training parameters as per the need and train the network
Net = Train ($Net, Trainingdata, Group$)
Classify = simulate (Net, Single node properties)
If Classify = True
Optimal Node = distorted Node

Else
Gray hole node = distorted Node
End
Return; classify gray hole node
End

IV. RESULT AND DISCUSSION

The results are examined in MATLAB by deploying n number of nodes with defined co-ordinates. The source, as well as the destination node, is pre-defined. After data transmission, the following parameters are observed as explained in the following section. The simulation parameters considered in the designed MANET is listed in table 1.

Table 1: Simulation Parameters for AODV & Gray Hole node

Parameter	Value
Simulator	MANET
Mobility Speed	5 m/s
Deployed Nodes	50
Designed Area	1000×1000
Routing protocol	AODV
Optimization Technique	Firefly
Classification Approach	ANN

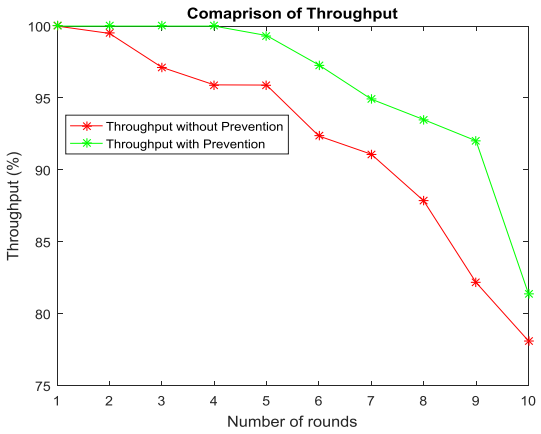

Figure 7: Throughput

Throughput measured for the proposed work in the presence and absence of gray hole node is depicted in fig. 7. From the fig.7, it is clear that the network delivered packets with high efficiency when the network is prevented from gray hole node denoted by the green line. When there is no prevention approaches are applied to the network, the data packets dropped due to the occurrence of gray hole attack. The values examined for 10 numbers of iterations are listed in the table below.

Table 2 Throughput (%)

Number of Rounds	Without Prevention	With Prevention
1	78.11	81.40
2	1.00	1.00
3	91.09	97.29
4	95.90	1.00
5	92.35	93.50
6	97.13	1.00
7	87.85	94.92
8	82.17	92.02
9	95.91	99.34
10	99.49	1.00

The average value measured for the proposed work in the presence of gray hole attacker node and after preventing the network from the attacker node is listed in table 2. The average value examined without preventing the network from gray hole node and when the network is prevented from the gray hole node are 92 % and 95.8% respectively. Thus there are an improvement of 4.13 % has been obtained.

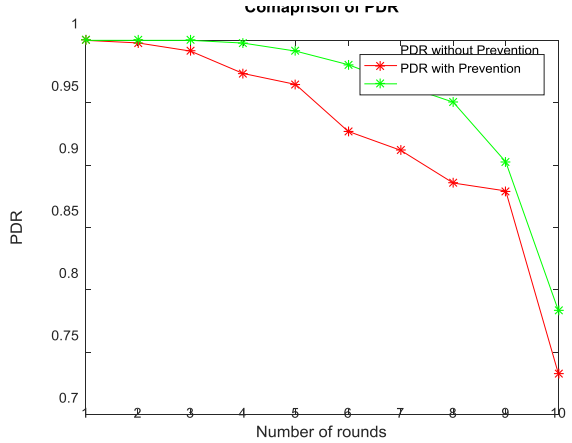

Figure 8: PDR

The PDR examined after the simulation of the proposed network without and with gray hole attack is represented in fig. 8. From the graph it is clearly seen that initially, PDR for the network in case of gray hole attack and after the detection and removal of gray hole attack are constant.

After the first round, the PD R decreases very sharply when there is no prevention algorithm is applied in the network. This is due to the presence of gray hole node, which drops the entire packet and hence decreases the PDR.

Table 3 PDR

Number of Rounds	Without Prevention	With Prevention
1	0.7330	0.7835
2	0.8856	0.9504
3	0.9647	0.9647
4	0.9914	0.9914
5	0.9271	0.9805
6	1.0000	1.0000
7	0.9735	1.0000
8	0.9119	0.9978
9	0.8793	0.9026
10	0.9979	1.0000

The average value examined without preventing algorithm and with prevention algorithms are 0.926 and 0.957 respectively. Thus these are an improvement of

3.35 % has been obtained.

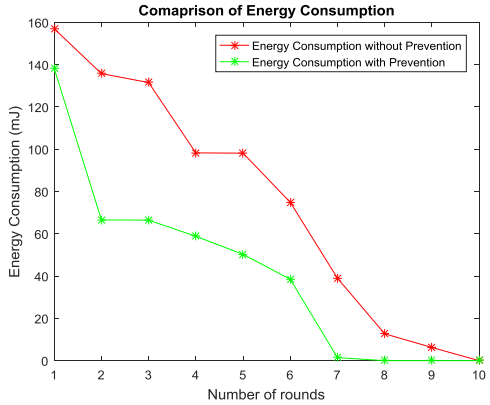

Figure 9: Energy Consumption

Energy consumption is also one of the main parameters on the basis of which the performance of the network can be examined. The measured values of energy consumption with and without prevention techniques (FF and ANN) are depicted in fig.9, with the values are written in table 2.

Table 4 Energy Consumption

Number of Rounds	Without Prevention	With Prevention
1	131.5527	58.8380
2	0	0
3	157.0053	138.2269
4	98.2824	1.4373
5	12.7164	0
6	74.9114	66.5910
7	135.7827	66.4481
8	98.1564	50.2909
9	39.0052	38.4992
10	6.2427	0

75.32 mJ and 42.03 mJ have been examined in the presence of gray hole attack and after the prevention of network from gray hole attack. Thus, the energy upto 44.02 % has been saved.

A.Comparison of proposed with Existing Work

The experiment has been performed in the appearance of a single attacker node, the value of PDR examined in the presented work is compared with the existing work proposed by Gurung and Chauhan in 2019. The authors have worked to identify the gray hole attack using AODV routing protocol and the performance has been measured on the basis of PDR. The comparison is shown in the fig. 10.

Table 5: Comparison of PDR

Proposed Work	**Gurung and Chauhan (2019)**
0.957	0.941

From the fig.10, it is clear that the PDR using proposed firefly with the ANN approach is higher compared to the existing work. There is an enhancement of about 1.7 % has been obtained compared to the existing work. This is due to the detection of gray hole node in an appropriate way and hence change the route or the network is protected.

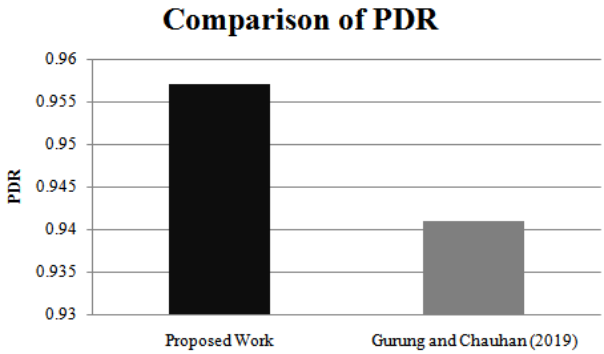

Figure 10: Comparison of PDR

V. Conclusion

In this research, we have identified gray hole attack using the concept of neural network. ANN helps to distinguish between the malicious node as well as the genuine node based on the optimized properties of nodes. In case, if the gray hole attacker node finds in the network, it has been detected as its properties are different compared to the normal nodes properties. The nodes properties have been matched with the dataset of ANN. Therefore, the performance of the network has been enhanced in terms of different parameters as discussed above. Also, the comparison of PDR has been performed to show the enhancement of the proposed work. There is an increment of 1.7 % has been obtained compared to the existing work presented by Gurung and Chauhan (2019).

REFERENCES

1. GBanerjee, S. “Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks”. In *Proceedings of the world congress on engineering and computer science* , 2008 pp. 22-24.
2. Sen, J., Chandra, M. G., Harihara, S. G., Reddy, H., & Balamuralidhar, P. “A mechanism for detection of gray hole attack in mobile Ad Hoc networks”. In *2007 6th International Conference on Information, Communications & Signal Processing, 2007*, pp. 1-5. IEEE.
3. Vishnu, K., & Paul, A. J. . “Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks”. *International Journal of Computer Applications*, *1*(22),2010, pp: 38-42.
4. Kanthe, A. M., Simunic, D., & Prasad, R.. “A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks”. *International journal of computer applications*, *53*(16), 2012, pp: 23-30.
5. Jhaveri, R. H., Patel, S. J., & Jinwala, D. C, “DoS attacks in mobile ad hoc networks: A survey”. In *2012 second international conference on advanced computing & communication technologies* , 2012 pp. 535-541. IEEE.
6. Kumar, A., & Chawla, M. (2012). “Destination-based group Gray hole attack detection in MANET through AODV”. *International Journal of Computer Science Issues (IJCSI)*, *9*(4), 292.
7. Jain, S., Jain, M., & Kandwal, H. “Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks”. *International Journal of Computer Applications*, *1*(7),2010 , pp: 37-42.
8. Shalika, E., Bal, J. S., & Dhir, V. “A Review on Implementation of AODV Technique for Isolation of Gray Hole Attack in MANET”, 2018.

9. Kumar, J., Kulkarni, M., & Gupta, DEffect of Black hole Attack on MANET routing protocols. *International Journal of Computer Network and Information Security*, *5*(5), 2013, pp: 64.
10. Gurung, S., & Chauhan, SA dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. *Wireless Networks*, *25*(4), 2019pp:1685-1695.
11. Swapnil S. Bhalsagar, Manish D. Chawhan, Yogesh Suryawanshi, V. K. Taksande (2019) Performance Evaluation of Routing Protocol under Black hole Attack In Manet And Suggested Security Enhancement Mechanisms, Volume-8 Issue-5 March, 2019, pp 1-7.

AUTHORS PROFILE

Puneet kamal,received my B.Tech degree in Computer Science And Engineeering from CGC landran Mohali. I am Currently pursuing M.TECH in computer science and engineering at Chandigarh Engineering College (CEC),Landran, Mohali, India. Her Research Interest includes computer networking.

Rajeev Sharma, received his Bachelor's degree in Computer Science and Engineering from Desh Bhagat College of engineering and Technology., India .MTECH from Guru nanak dev eng.college ,Ludhiana ,Punjab,India and Persuing phd from Chandigarh University.

Abhishek Gupta, received his bachelor's degree from Himachal Pradesh university in 2004and done his M.tech from Lovely Professional university in 2012.He has teaching experience of 13 years. He is perusing his Phd in CSE from Chandigarh University.

Mr. Gaurav Kumar, M.Tech (ECE), is an Assistant Professor and Researcher at the department of Electronics & Communication Engineering, Chandigarh Engineering College, Landran. He worked on various projects and Patents for last 10 years. He has done his Masters in Engineering from GNDEC, Ludhiana. His area of interest is Communication Engineering.