Performance Improvement by Identification and Elimination of Gray Hole Nodes in MANETs

Anamika Jain
M.Tech. Research Scholar
GZS PTU Campus,
Bathinda, Punjab

Paramjeet Singh, PhD
Associate Professor
GZS PTU Campus,
Bathinda, Punjab

Shaveta Rani, PhD
Associate Professor
GZS PTU Campus,
Bathinda, Punjab

ABSTRACT

Mobile Ad-hoc Networks (MANETs) are widely used in various applications due to its ability to communicate without any fixed infrastructure like in military and civilian applications. MANETs are wireless infrastructure-less (Ad-hoc) network comprising of mobile nodes. Mobile nodes can enter and leave the network at any time. Due to its inherent characteristics like dynamic topology, autonomous nodes and self organizing ability these networks are vulnerable to various security attacks. MANETs are still an emerging technology in wireless communication. Security is very important in this modern era especially in MANETs. Without any security, nodes may selectively drop packets without forwarding them. This type of security issue is known as Gray Hole attack. In this paper a novel scheme is proposed for identification and elimination of Gray Hole attack. This technique uses a redefined modified extended data routing information (RM-EDRI) table that is maintained by every node on the network.

General Terms

Network, Security, Attacks in MANET

Keywords

MANETs, AODV Protocol, Gray Hole attack, RM-EDRI table

1. INTRODUCTION

MANETs are collection of two or more mobiles nodes like laptops, PDAs and mobile phones which can communicate with other mobile nodes those come under the transmission range of each other. Mobile nodes works both as a host and router means can send and receive data and forward the data packet that is destined for other nodes. Mobile nodes cooperate with each other and forward the packets i.e. multi-hop packet transmission [1]. Since MANETs are infrastructure less type of networks, nodes can dynamically create path for transmission i.e. they are self-organized self-configurable, self-creating and autonomous networks. Due to absence of centralized administration, security is always a constraint for MANETs. Attacks on MANETs are either classified as Active or Passive. Passive attacks are attacks those that do not alter messages communicated between source and destination but only view and posses data. They do not interrupt communication. Active attacks are those that interrupt the communication between source and destination and alter, modify or delete the data exchanged between them. Alteration could also be false data entry in the network [2].

In these types of networks, communication between the nodes is carried out using blind trust on each other. Because of this blind trust, some nodes may be compromised and behave maliciously and drop the packets without forwarding them which are not destined for them. This paper addresses the Gray Hole attack which is a variation of Black Hole attack. In this attack, malicious node selectively forward or drop packets. It solely means nodes can switch from normal node to malicious node and vice versa. So it is not easy to detect Gray Hole attack as malicious node sometime may behave as normal node. In this paper, a new technique is proposed for improving the performance of the network by identifying the malicious node and not using them for data transmission. According to this, every node maintains the history of previous instances malicious nodes in the network and based on that node creates the path for further communication. This scheme is implemented using AODV (Ad- Hoc on Demand Distance Vector) routing protocol on mobile ad-hoc networks.

The rest of the paper summarizes as follows. Section 2 explains gives a brief literature review. Section 3 describes the Proposed Methodology and Section 4 discusses the results and finally section 5 concludes the paper.

2. LITRRATURE SURVEY

Various techniques have been proposed to detect and prevent gray hole attacks. Review of these techniques is presented as below:

Shrishti Jain et al. [1], have presented a technique for Gray Hole detection based on the behaviour and performance of the nodes in MANET. In this technique behavioral anomaly is applied to the suspected node and the IDS (Intrusion Detection System) node detects the anomaly in the data generated by the Gray Hole node and broadcast the block message to all other nodes. Vani A. Hiremani et al. [3], have proposed a method to eliminate the cooperative Black Hole and Gary Hole attacks using MEDRI table. In this, each node maintains MEDRI (Modified Extended Data Routing Information) table. The extension to the table helps in finding packet routing problems in MANET. When a node suspected to be malicious due to NACK from the receiver, source node invokes a method which uses MEDRI table, enquires from the neighboring nodes about the suspicious node and finds the Black Hole and Gary Hole node in the network.

Jasleen Arora et al. [4], have proposed a technique to detect and eradicate Gray Hole nodes in the mobile ad-hoc network. The environment used is cluster based network. This mechanism is based on the miss ratio of each node. The node whose miss ratio is above certain threshold is said to be malicious. Gundeep Singh Bindra et al. [6], have discussed a technique for Detection and Removal of Co-operative Black Hole and Gray Hole Attacks in MANETs. In this method, each node maintains EDRI (Extended Data Routing Information) table along with routing table. This table maintains the history of nodes i.e. how many times it has been behaved maliciously along with other information about the suspicious behaviour of the nodes. When a node suspected to be malicious due to NACK from the receiver, source node invokes a method which uses this table and finds the malicious node.

Onkar V.Chandure et al. [9], have elaborated a mechanism for protecting the network by detecting and removing the nodes with malicious activities. This mechanism work as when a genuine node finds a suspicious node in the network by looking at data routing information table, it invokes security mechanism. Based on entries in DRI table, suspected node is enquired using cooperative node and when level of suspicion about the suspected node increases, a Malicious Node Detection procedure is activated. Vishnu K et al. [11], have proposed a method to detect and eliminate cooperative Black/Gray Hole attack in MANET. Firstly a backbone of trusted nodes is created over the network. Whenever source node wants to send data, it requests for an unused IP address from one of the trusted nodes. When source node sends RREQ and also a request for restricted IP (RIP) address, intermediate node sends RREP message to source node. If intermediate node also replies for RIP address along with RREP message, then that node is suspected to be Black/Gray Hole node otherwise that node is a normal node. After that Black/Gray Hole detection procedure is initiated.

Jaydip Sen et al. [12], have explained a mechanism for detection of Gray Hole attack in MANETs. The proposed mechanism consists of four modules namely Neighborhood Data Collection, Local Anomaly Detection, Cooperative Anomaly Detection and Global Alarm Raiser. This mechanism checks for malicious node both locally and cooperatively in global area. This enhances the correctness of the detection mechanism of the Gray Hole node. After it is confirmed that particular node is malicious, it sends notification to the all other nodes in the network by using global alarm raiser. Sanjay Ramaswamy et al. [13], authors have introduced a technique to prevent cooperative black hole attack in wireless ad-hoc networks. In this method, they used DRI (data routing information) table and cross-checking mechanism by slightly modifying the AODV protocol. Each node in the network maintains a DRI table. If both the fields of the table are 0 then that node is suspicious node and is further enquired using cross checking mechanism. In cross checking, source node enquires about suspicious node from its neighbor node by sending further request packet.

3. PROPOSED METHODOLOGY

3.1 AODV

AODV (Ad –Hoc On demand Distance Vector) protocol is an on demand routing protocol. It is a reactive routing algorithm that has capabilities as low processing overhead, low memory overhead, and low network utilization. Each node maintains a table that contains the routing information for its neighbor nodes. When source node wants to transmit packets to the destination, it checks its routing table for the fresh route if available otherwise starts Route Discovery process. Source node sends RREQ (Route Request) message to all its neighbors and these nodes forward this message to their neighbors if they don't have fresh route to the destination or if they are not destination node. The node which has path to the destination or node which itself is a destination sends RREP (Route Reply) message to the sender and according to that path source node transmits its packet.

3.2 Gray Hole Attack

It is a type of active attack which occurred at network layer. It is a variation of black hole attack. In this, malicious nodes intercepts packet from the particular node by replying positively to the route request packet. After receiving packets from the source node, malicious node selectively keeps and drops packets. This is also called as selective forwarding attack. Figure 1 gives the description of Gray Hole attack. This Gray Hole attack is like a slow poison in the network which does not let know how many data packets will be lost. That why it is harder to find the Gray Hole attacker node. This attack degrades the network performance by decreasing packet delivery ratio and throughput and increasing end to end delay and disturbing route discovery process.

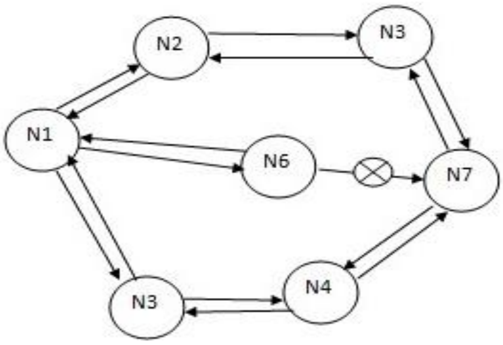

Figure 1 Gray Hole Attack

3.3 Proposed Technique

A novel technique is proposed to overcome the problem of Gray Hole attack based on the sequence number. Sequence Number is the unique number of the data packet in MANET. This is an increasing value. The next packet should have higher sequence number than the last packet transmitted. The proposed solution uses this sequence number to find the malicious node. Each node keeps the history of the sequence number of the last packet sent to every node and last packet sequence number received from the intermediate node along with the other information about the nodes. This sequence number field is added in the extended modified data routing information table and table is named as redefined modified extended data routing information table and shown in table 1. This technique uses RM-EDRI table during route establishment phase and finds the malicious node which wants to communicate with it.

Description of the different fields of table:

From field describes that if the source node has ever transmitted data coming from the respective node. The value is 1, if it is true; otherwise it is 0.**Through** field describes that if the source node has ever transmitted data through the respective node. The value is 1, if it is true; otherwise it is 0.**Last Packet S.N (Sent)** filed describes the sequence number of the last packet which was sent by the source node to the respective node. **Last Packet S.N (Received)** filed describes the sequence number of the last packet received by the source node from the respective node.**CTR** describes the counter; the number of times the respective node found to be malicious in its history.**BH** The value is 1, if the respective node is malicious in its last attempt; otherwise it is 0. **Timer** field specifies the time for which node is not considered for communication. **Packet Size (S)** is the packet size at source. **Packet Size (D)** is the packet size at destination. **Results** this compares the packet size at source and packet size at destination.

Table 1: RM-EDRI table

Node_Id	From	Through	Last Packet S.N (sent)	Last Packet S.N (received)	CTR	BH	Timer	Packet Size (S)	Packet Size (D)	Results
1	1	1	3404	3394	0	0	0	1024	1024	Yes
4	1	1	898	901	1	0	0	1024	800	No
6	0	1	904	-	0	0	0	1024	1024	Yes

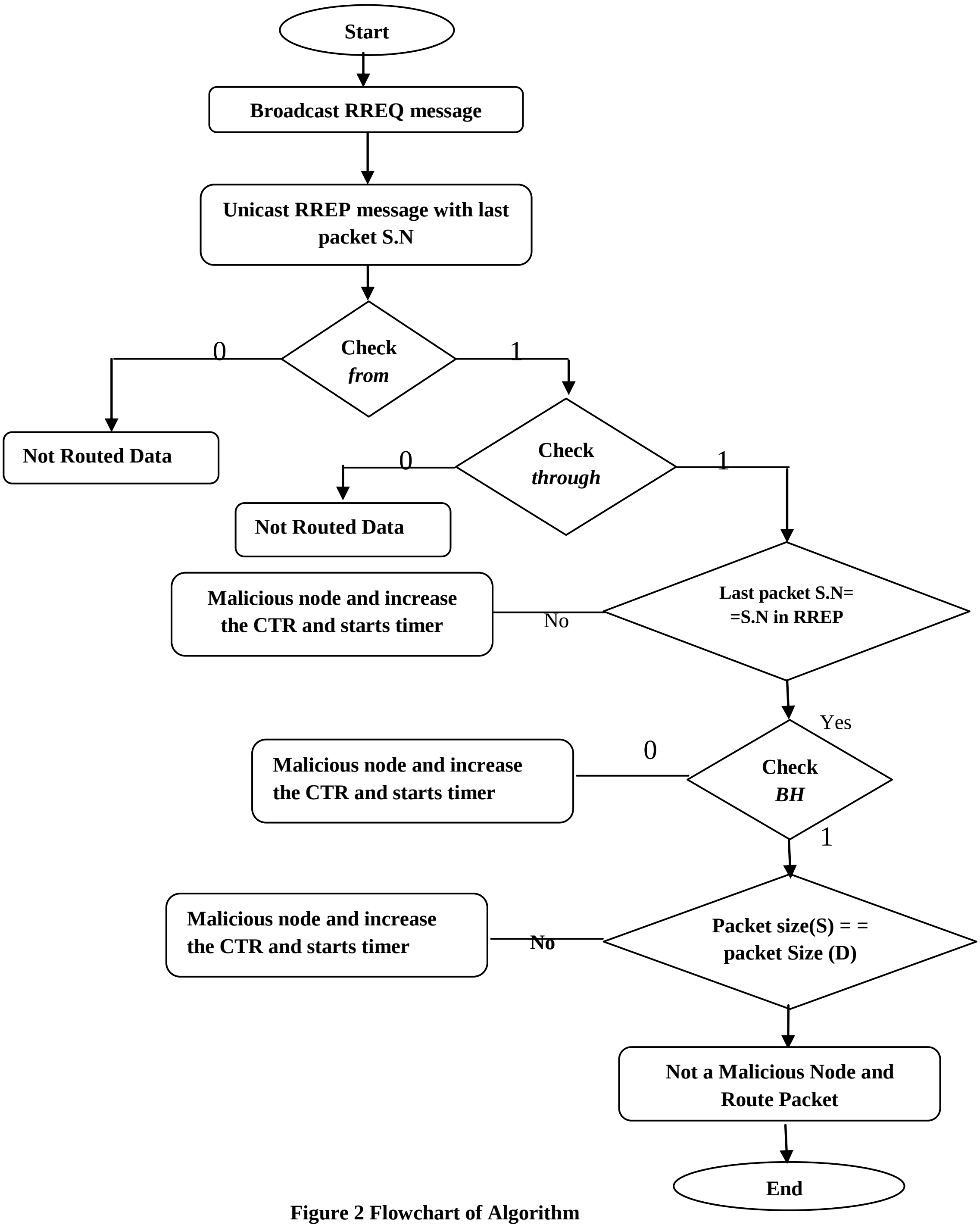
Start
Broadcast RREQ message
Unicast RREP message with last packet S.N
Check *from*
0
1
Not Routed Data
Check *through*
0
1
Not Routed Data
Malicious node and increase the CTR and starts timer
No
Last packet S.N= =S.N in RREP
Yes
Malicious node and increase the CTR and starts timer
0
Check *BH*
1
Malicious node and increase the CTR and starts timer
No
Packet size(S) = = packet Size (D)
Not a Malicious Node and Route Packet
End

Figure 2 Flowchart of Algorithm

Algorithm: Figure 2 describes how algorithm works.

1. Source node send RREQ message to its neighbours to find the destination node.
2. The intermediate node unicasts the RREP message along with the sequence number of the last packet received from the source node.
3. Each node maintains a table having information about the routing called RM-EDRI (Redefined Modified Extended Data Routing Information) table.
4. Source node checks the 'from' field; if the value is 0 or 1 then checks the '*through'* field; if the value is 1 or 0.
5. If both the values are 1; then compare the last packet sent sequence number value to sequence number value in the RREP message. If values do not match then the node is malicious and increases the value of counter field and starts the timer one otherwise proceed further.
6. Now check the *'BH'* field of the table; if its value is 1 then increase the counter and starts the timer and node is declared to be malicious.
7. Otherwise compare the packet size at source with the packet size at destination and if does not match then it's a malicious node otherwise not a malicious node.

4. SIMULATION RESULTS

The simulator used for simulation in this work is NS-2 simulator. NS-2 (Network Simulator) is a discrete event network simulator. Proposed technique is implemented using Ad-hoc On Demand Distance Vector (AODV) Protocol. Proposed technique has been tested on different environments i.e. on 10 nodes, 20 nodes and 40 nodes. The proposed technique has been compared with the previous technique.

4.1 Simulation Parameters

Table 2 shows the simulation parameters used in simulation.

Table 2: Simulation Parameters used for Simulation

Parameter	Value
Simulation Area	2700*2700
Mobile Nodes	10,20,40
Mobility Model	Random Way point
Packet Type	TCP, UDP
Traffic Type	FTP
Routing Protocol	AODV
Antenna	Omni-Directional
MAC	802.11
Simulation Time	110Sec

4.2 Evaluation Metrics

1. Throughput: Throughput of the network can be described as total packets delivered to the destination in total simulation (in time). This can be calculated by dividing number of packets received by the destination with the time. It is measured in terms of *kbps*.

2. End to End Delay: This metric is defined as time a packet takes to reach to the destination. This delay takes into account the sum of time each packet takes to reach to the destination and number of packets. This is measured in *ms*.

3. Packet Delivery Ratio: Packet delivery ratio is described as the ratio of total packets received at the destinations to the total packets sent by the sources.

4.3 Results and Comparison

The performance of the network of proposed technique is tested and compared with proposed technique using different parameters under different scenarios.

4.3.1 Throughput (in kbps)

The graph represents the throughput analysis with respect to number of nodes. Figure 3 clearly shows the improvement in throughput value of proposed technique as compared to existing technique. The main reason behind this is due to secure algorithm that identifies the malicious node using the sequence number sent by the node and increases the number of packets delivered to the destination.

Table3: Comparison between Existing Technique and Proposed Technique in terms of throughput

Simulation Scenario	Throughput (Existing Technique)	Throughput (Proposed Technique)
N1 (10 nodes)	534.47	569.06
N2 (20 nodes)	1142.87	1185.34
N3 (40 nodes)	787.22	840.58

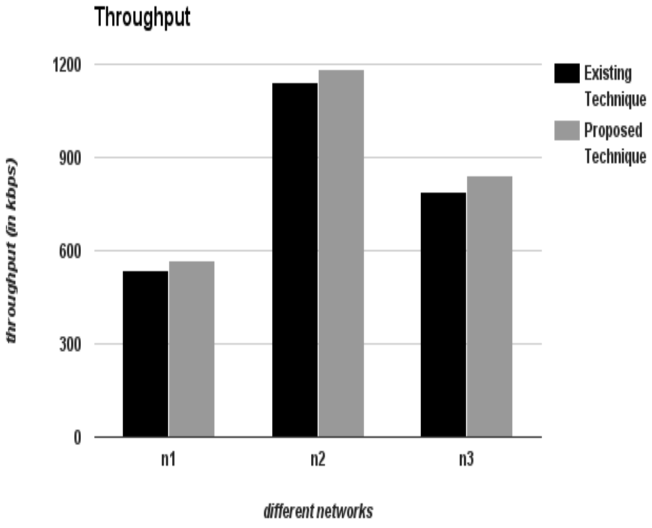

Figure 3 Comparison between Existing Technique and Proposed Technique based on Throughput

4.3.2 End to End Delay (in ms)

The graph represents the end to end delay analysis with respect to number of nodes. In figure 4, black bars are for packet delivery ratio of existing technique and gray bars for packet delivery ratio of new proposed technique. From the figure 4, it is clear that end to end delay has been reduced in proposed technique as compared to existing technique. The delay has been improved by the 1.23% as compared to existing technique as can be described from table 4. This is due the proposed technique because of that less number of retransmission of packets needs to be done and no fake path is created between the source and destination.

Table4: Comparison between Existing Technique and Proposed Technique in terms of end to end delay

Simulation Scenario	End to End Delay (Existing Technique)	End to End Delay (Proposed Technique)
N1 (10 nodes)	0.0044864	0.00446408
N2 (20 nodes)	0.00449729	0.00445913
N3 (40 nodes)	0.004516	0.00446037

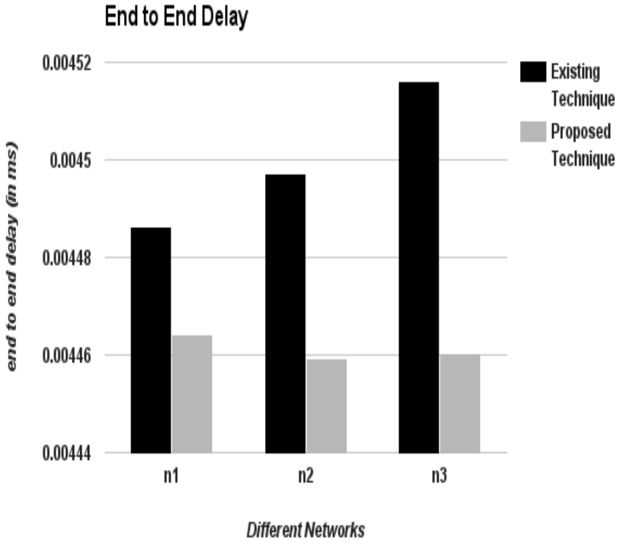

Figure 4 Comparison between Existing Technique and Proposed Technique based on End to End Delay

4.3.3 Packet Delivery Ratio (in %)

The graph represents the packet delivery ratio with respect to number of nodes. In figure 5, black bars are for packet delivery ratio of existing technique and gray bars for packet delivery ratio of new proposed technique. The figure 5 clearly shows that packet delivery ratio (PDR) is improved in case of proposed technique then the existing algorithm. Packet delivery ratio has been improved by 1.89% as can be calculated from table 5. The reason behind this is that malicious nodes are found by the algorithm and that node is considered for transmission of packets and hence packet drop decreases.

Table5: Comparison between Existing Technique and Proposed Technique in terms of Packet Delivery Ratio

Simulation Scenario	Packet Delivery Ratio (Existing Technique)	Packet Delivery Ratio (Proposed Technique)
N1 (10 nodes)	95.8546	97.4036
N2 (20 nodes)	96.4614	97.4315
N3 (40 nodes)	95.3493	97.158

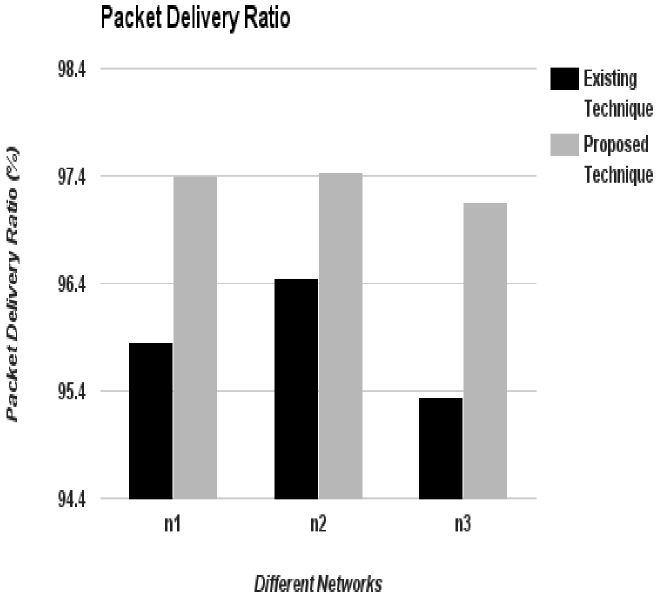

Figure5 Comparison between Existing Technique and Proposed Technique based on Packet Delivery Ratio

5. CONCLUSION

Security is one of the main issues for any network like mobile ad-hoc networks. But because of some attacks such as Gray Hole attack, security of the network gets affected. This causes the degradation in the performance of the network. In this paper, Gray Hole attacker nodes are identified and eliminated using the new proposed technique in which data routing information table is redefined over the mobile ad-hoc network. Simulation of the Gray Hole attack is carried out using ns-2. The new proposed technique uses the sequence number of the packets sent over the network to find the malicious nodes along with other information about the neighboring nodes. The source node asks about sequence number of last packet sent to the intermediate node and compares it with its table, if node specifies the fake number, the node is said to be malicious and is not used for routing the packet. The RM_EDRI table maintains the history of routing information of previous malicious nodes and uses them for future transmission and communication over the network. It is clear from the data and results that the proposed technique has improved the performance of the network by increasing throughput and packet delivery ratio and decreasing end to end delay. In future, the proposed technique can be applied to other ad-hoc networks like WMN (wireless mesh network). WMN's are emerging technology and there should be a secure technique for routing the packets over the network. So that potential performance of network can be increased.

6. ACKNOWLEDGMENTS

I would like to thank my guides Prof (Dr.) Paramjeet Singh and Prof (Dr.) Shaveta Rani for their consistent guidance and support in the accomplishment of this research work entitled "Performance Improvement by Identification and Elimination of Gray Hole Nodes in MANETs". I am also thankful to my family and friends who keep encouraging me to complete my work in time. My acknowledgements would not be complete without expressing my personal belief in and gratitude towards God, our creator. None of this would have been possible without His blessings.

7. REFERENCES

[1] Shrishti Jain, Raghuwanshi, Sandeep K,"Behavioural and node performance based Gray hole attack Detection and Amputation in AODV protocol", *IEEE International Conference on Advances in Engineering & Technology Research (ICAETR),* August 2014.

[2] V. Shanmuganathan, Mr.T.Anand, "A Survey on Gray Hole Attack in MANET", *International Journal of Computer Networks and Wireless Communication (IJCNWC),* Vol.2, No6, ISSN: 2250-3501 December 2012.

[3] V.A Hiremani. , M.M Jadhao, "Eliminating co-operative black hole and gray hole attacks using modified EDRI table in MANET", *IEEE International Conference on Green Computing, Communication and Conservation of Energy (ICGCE),* December 2013.

[4] Jasleen Arora , Paramjeet Singh and Shaveta Rani, "Detecting and Preventing Attacks in MANET" *International Journal of Computer Applications Vol.81 No5, ISSN: 0975 – 8887, November 2013*

[5] Harsh Pratap Singh, Virendra Pal Singh, Rashmi Singh, "Cooperative Black hole/ Gray hole Attack Detection and Prevention in Mobile Ad hoc Network: A Review", *International Journal of Computer Applications*, Vol. 64, No.3, ISSN: (0975 – 8887), February 2013.

[6] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs" *IEEE International Conference on System Engineering and Technology*, September 11-12, 2012, Bandung, Indonesia.

[7] Robinpreet Kaur and Mritunjay Kumar Rai, "A Novel Review on Routing Protocols in MANETs", *Undergraduate Academic Research Journal*, Vol. 1, ISSN: 2278-1129, 2012.

[8] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", *International Journal of Engineering and Advanced Technology (IJEAT),* ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[9] Onkar V. Chandure and V.T. Gaikwad, "Detection and Prevention of Gray Hole Attack in Mobile Ad- Hoc Network using AODV Routing Protocol", *International Journal of Computer Applications*, Vol. 41, No.5, ISSN: 0975- 8887, March 2012.

[10] Priyanka Goyal, Vinti Parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", *IJCEM International Journal of Computational Engineering & Management*, Vol. 11, ISSN: 2230-7893, January 2011.

[11] Vishnu K and Amos J Paul, "Detection and removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks" *IJCA* Vol.1, No.22 Jan 2010.

[12] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy and P. Balamuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", *Information, Communication and Signal Processing 2007, 6th International Conference*, December 2007.

[13] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". *In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03),* Las Vegas, Nevada, USA, pp. 570-575.