Scientific Journal Impact Factor (SJIF) : 4.364
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

TRUSTED DSR ROUTING PROTOCOL TO WITHSTAND AGAINST GRAY HOLE ATTACK IN MANET USING Q-LEARNING

A.Thirumavalavan[1] and K.Selvaraj[2]
[1,2]*Department of Computer Science, Arignar Anna Government Arts College, Attur, Tamilnadu, India*

Abstract - Routing is one of the required tasks in MANET to exchange packets among the mobile nodes that is accomplished by routing protocols. Traditionally routing protocols are designed to cope with routing operation but in practice they may be affected by misbehaving nodes in the form of attacks. Gray hole attack is one of the notable attack since they are launched internally and cannot be identified easily. It aims to disrupt the normal routing operation and try to minimize or collapse the overall network performance. Therefore, detecting Gray node and secure routing in MANET environment is always a challenging problem due to its distinct characteristics. In this paper, we have proposed a trusted DSR Routing protocol to detect the Gray hole attack over DSR routing protocol. Here we avoid the Gray hole nodes by calculating an overall trust of each node based on metrics such as direct and indirect trusts. In addition Q-learning algorithm is used to enrich the proposed work by assigning reward. This model is the extension of our earlier work [1] that overcomes the black hole attack over AODV Routing protocol.

Keywords – MANET, routing, Security, Gray hole attack and DSR

I. INTRODUCTION

Mobile Ad hoc Network also known as MANET is a group of autonomous mobile nodes that are connecting together in a self-organized manner over a wireless medium. In this network each node plays a dual role such as ordinary node; to perform network operations and router; to forward hence there is no specialized router for forwarding the packet. Nodes in the network can join and leave at any time leading to dynamic topology. Due to limited wireless range, it is multi-hop in nature so that it follows the peer to peer communication mechanism. Due to distributed nature there is no central control; therefore every node depends on other nodes for forwarding and act as routers. Such distinct characters make MANET differ from other networks and support many applications that run on top of it. As mobile communication plays a vital role, their security is also in focus. Such special characteristic makes the network for various applications. MANET has weakness in terms of security due to its unique nature so deploying application in MANET becomes highly insecure. Moreover the restriction of adversary in application is very low due to many factors such as weakness of technology, unexpected operational conditions, and lack of cooperation among the nodes, lack of communication and so on.

In general in a MANET environment, nodes are working together to achieve a task and they assume that all are performing well. But in practice it is not true due to attacks. The attacks are launched due to poor physical protection in MANET environment, open and lack of centralized control, due to resource constrained equipment, limited bandwidth of wireless devices and so on. The notable and most dangerous attack is Gray hole attack [2][3] since they are harder to detect and launched internally because of overload, congestion and selfish nature of nodes in the network Gray hole attack is a variation of black hole attack [4][5] where an opponent behave just like an authentic node during the initial route discovery process thereafter it drops the packets which is intended to forward even if there is no congestion. Moreover the detection of such attack is harder because an attacker behaves just like a normal node so that we can't distinguish. Simply we can say those nodes participate in route discovery process and thereafter simply drop all the incoming packets that are intended to be forward [6].

This work is the extensions of our earlier work [1] where we ensure the security by identifying the black attack over AODV routing protocol. In this work, we investigate our proposed work against Gray hole attacks over Dynamic Source Routing protocol (DSR) [7] so that Gray hole nodes will be identified and isolated from the network hence security can be achieved.

The remainder of this paper is organized as follows; section 2 discussed impact of Gray hole attack in MANET over DSR routing protocol, the need for trust, section 3 discusses the authentication and trust, section 4 deals with the related work, section 5 discusses the proposed work, section 6 discusses the results and discussion and finally section 7 discuss the conclusion.

II. IMPACT OF GRAY HOLE ATTACK OVER DSR ROUTING PROTOCOL

Information which is sharing in MANET environment is, highly confidential so high level of security is always requirement but achieving such security level in MANET is still complicated task due to its unique nature. This section deals with the impact of Gray hole attack. Attack is nothing but an assault on system security that is derived from an intelligent threat [8]. In general two types of attacks are possible in MANET such as internal attack and external Attack. Internal Attacks are very difficult to predict and detect because it may be launched by any compromised or malicious node from inside the network whereas external attack arises from outside the network. It causes more additional overhead on packets and tries to prevent the normal communication among the nodes. It is further classified into two categories such as passive attack and active attack.

Passive attack obtains information from the system that is being transferred and does not affect the system resources at any way and active attack aim is to alter the system resources and affect their performance. It makes some modification of data streams and creation of false streams routing by the way it affects the network.

In our proposed work we deals with internal attack such as Gray hole attacks. Before discussing the impact of such attack, it is necessary to know the working principal of DSR routing protocol.

2.1.DSR Protocol Description and its Implications

DSR is based on the concept of source routing that is the entire path is explicitly mentioned in the packet header of source. Hence intermediate nodes do not require keeping the routing information also need not updates periodically like *Hello* message in AODV. It supports both unidirectional and asymmetric links. Route Discovery and Route Maintenance phases are used to achieve reliable routing in DSR.

2.1.1. Route Discovery in DSR.

Every node in MANET maintains route cache that is used to store all available route information. The main advantages of route cache are used to speed up the route discovery process and reduce the propagation of route request. When a node wants to transmit a packet to another node, first it will check the route for a source to the destination in its route cache. If any route is found to a destination, it forwards the packets otherwise it initiates a route discovery process by propagating *RREQ* packet to its neighbouring nodes. In the meantime of *RREQ*, a node will do some other process like sending and receiving of packets from other nodes in the network. Typically the destination node does not forward any *RREQ* because it is the intended destination. *RREG* packet contains Sender's Address, Destination Address and Unique Request ID determined by the sender. While transmitting each node appends its own identifier to the forwarding node. Duplication of *RREQ* is avoided by <*initiator address and request id* > pair. Figure.1 illustrates route discovery process in DSR. There are two probabilities that will arise when a node receives a *RREG* that is a node may be an intermediate node or it may be a destination node. If it is an intermediate node, the node will perform the following actions, finding of its own address in the *RREQ* packet or if same ID of *RREQ*. In that case a node simply discards the packet otherwise the node appends its own address to the route record of the *RREG* packet and propagates to next hop neighbors. If it is a destination

node, it will return a route reply message to the sender with the path where it is stored in its route cache.

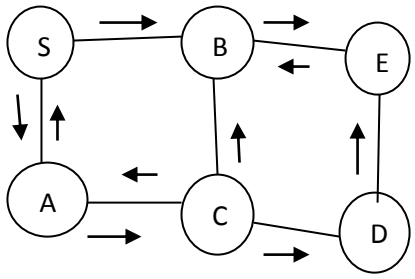

Figure 1. Route Discovery Process

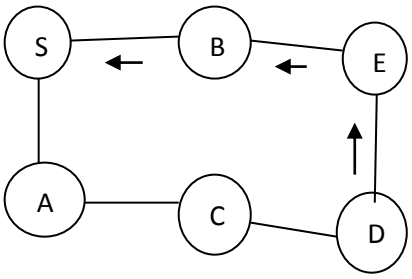

Figure 2. Route Reply Process

On receiving *RREP* the sender receives the route in route cache for subsequent uses as well as copy the accumulated route record from *RREQ* into *RPLY* here route reply is done by unicast not by multicast. Once the *RPLY* reaches the source node, the source node the actual data packet along the way to the destination. Figure.2 illustrates route reply process. When discovering a route, due to lack of route some packets may not be transmitted, those packets will be stored in the send buffer. Each packet which is stored in the send buffer will spend some specific time out period, if the packet is not delivered within that time, it will be discarded.

2.1.2. Route Maintenance in DSR.

Route maintenance is achieved by Route Error packet (*RERR*) and acknowledgement from the receiving nodes. When error packet is received from a particular node, the entire routes of the affected node are removed from the route cache of the rest of the nodes. Acknowledgement is achieved by listening to the transmission of active nodes within the network. To ensure this appending a acknowledge bit explicitly is done. If a node fails to receive the bit, it invokes a route discovery process again by sending a route error packet to the sender.

2.2 Gray hole attack on DSR Routing Protocol

In DSR protocol, a node wants to send a packet to a particular destination, first it checks whether it has route to the destination in its route cache. If it has, simply uses that route for relaying the packet. Otherwise it initiates the route discovery process by using *RREQ* packet (Arrow Line). Upon receiving the route request packet *RREQ* the intermediate nodes give response by the *RPLY* (Dotted Arrow line) packet back to the source if they have desired route to the requested Destination. According to the protocol specification, DSR protocol gives response and sends data packet to the first route reply from the neighbouring nodes though it receives multiple route replies. Here Gray hole node will occupy between the source and the destination and claim itself that has the shortest path by the way it is getting attention from then the source and it simply drops the incoming packets that is intended to be forwarded to others. The Figure.3 shows the Gray hole attack where GH is a Gray hole node it drops the route reply (RPLY) that is forwarded by destination node D to the source node A so that all the packets that are intended to be forwarded are dropped.

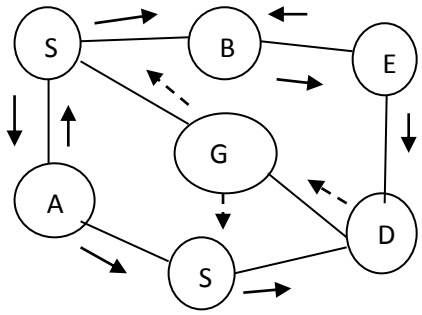

Figure 3. Gray hole attack

III. AUTHENTICATION AND TRUSTS

Authentication is one of the important security requirements in MANET and it is defined as *"the ability of a node to ensure the identity to the receiver [8]"*. Typically authentication is carried out in two ways. The first one is initial authentication, which means all the participating devices in the network are authentic at the time of initial network deployment so that such authentication mechanism is called pre-authentication. The next one is called post- authentication; means over a period of time; every node in the network should ensure the identity of participating nodes [9]. In this work we concentrate on post-authentication mechanism. Once authentication is achieved, remaining security requirements such as confidentiality, integrity and non-reputation [8] can be achieved easily. To achieve authentication, shared secret, Public Key Infrastructure [PKI], digital signature, digital certificate[10] are used but these techniques are centralized, pre-determined and depend on trusted third party, thereby increasing computation power, memory and consumption of communication bandwidth and battery power but MANET has limited resource constrains. To provide security with limited computational capabilities trust comes into existence because it offers less memory overhead, less transmission overhead and less bandwidth consumption[11].

Trust is a word which is originally derived from the social sciences. Trust is defined as "one entity (trustor) is willing to depend on another entity (trustee) [12]" or "the trustor abandons control over the actions performed by the trustee[13]". According to ad hoc networks, trust could be defined as "the reliability, timeliness, and integrity of message delivery to a node's intended next hop[14]. Typically trust can be evaluated based on direct and indirect means recommendation of others [15-17]. Direct means information gathering from one hop neighbours and indirect trust means information gathering from other than one hop neighbours. But both trust information exhibit the historical interactions of nodes with respect to each other.

Q-Learning algorithm is proposed by Watkins in the year 1989. The algorithm involves with an agent, states *s* and a set of actions per state *a*. The state of environment will change after receiving the action *a*. After executing an action in a specific state, the agent gets reward. The goal is to try to find an optimal policy that encourages the agent to obtain the total reward during the whole operation [18-20] and based on the total reward decision will be taken. The algorithm is defined as, Q(s, a) = r (s, a) +MAXa' _ (Q(s', a')) where *r(s, a)* is an immediate reward, _ is a discount factor that determines the importance of future rewards. The value of discount between *0* and *1* range, *s'* represents the new state after action *a*, *a'* represents the action in state *s'* and *a* and *s* represent the current state and action respectively.

IV. REVIEW OF LITERATUE

The author [21] proposed prevention and elimination of gray hole attack by packet update scheme where information about the suspected nodes is fetched from neighbors. Next the author [22] proposed a mechanism to detect collaborative Gray hole attacks based on destination based scheme with consist of three phases such as store the route reply packets in pervious nodes, check the neighbours those who are all 2 hop distances of suspected node and eliminate the route reply packets from the suspected node. Other than there are so many authors [23-27] deals with the Gray hole attack. Next the author [28] proposed a mechanism which is based on the threshold cryptography. Another author [29] used voting technique to eliminate the Gray hole attack. The author [2] proposed a detection of both black hole and Gray hole attacks.

V. PROPOSED MODEL

5.1 Assumptions

The proposed model is based on the following assumptions. As this work is the extension of earlier work (Sivagurunathan et al., 2016) [1] the assumption is used for (Sivagurunathan et al., 2016) [1] is also applied for this work. So for simplicity we assume the network is small in size. All the nodes are behaving well at the time of initial network deployment since all the nodes are authentic and all the nodes are having well defined resources such as battery power, bandwidth and

memory. Over the period of time, they may change their behaviour and become Gray hole. We represent the misbehaving nodes as Gray hole nodes where nodes try to drop every route request packets. Every node in the network maintains a table called ET table where trust values of their neighbour nodes can be stored. The structure of ET table is shown in table 1. We also assumed that node's trust value as a continuous real numbers in the range 0 to 1 with representation of 1 means completely trusted node, 0.5 means partially trusted node and 0 means untrusted or Gray hole node.

Table 1. ET Table

Node ID	DT	INDT	FT	IR	AT

Node ID – Node Identity, DT – Direct trust, INDT- Indirect Trust, FT-Final Trust, Ir- Immediate reward, AT-Aggregated Trust

5.2 Trust Computation phase

As mentioned earlier, initially all the nodes are cooperating well. Over the period of time, a node wants to send a packet to a particular destination. According to our proposed model, initially all the nodes broadcast the *HELLO* packets instead of initiating route discovery process or checking their own routing table for desired route. So that every node ensures it's one hop neighbouring nodes ultimately only one hop neighbours respond to the hello packets because they are in same communication range. From that every node can conclude how many nodes are staying as one hop neighbours. After that every node executes the trust evaluation mechanism on each of its neighbouring nodes based on the following equation 1.

$$DT_{AB} = \omega_1 * CP_{AB} + \omega_2 * DP_{AB} \quad (1)$$

Where ω denotes weighting factor and $\omega_1 + \omega_2 = 1$. CP_{AB} denotes control packet (forwarding or responding ratio) of node B with respect to node A. DP_{AB} denotes data packets forwarding ratio of node B with respect to node A over time with *n* number of interactions. In AODV the following control packets are used. In route discovery, route request *(RREQ)*, route reply *(RPLY)* packets are used. Route error *(RERR)* and *HELLO* packets are used in route maintenance process. Similarly, every node will evaluate the direct trust of its neighbour's nodes.

Control Packet forwarding (CP) or responding is calculated over the period of time based on the equation 2 with *n* interaction with the one hop neighbouring nodes.

$$CP_{AB} = \omega_1 * RREQ_{AB} + \omega_2 * RPLY_{AB} + \omega_3 * RERR_{AB} + \omega_4 * HELLO_{AB} \quad (2)$$

Where ω denotes weighting factor and $\omega_1 + \omega_2 + \omega_3 + \omega_4 = 1$. $RREQ_{AB}$ denotes route request forwarding ratio of node B with respect to node A. $RPLY_{AB}$ denotes route reply forwarding ratio of node B with respect to node A. $RERR_{AB}$ denotes route error forwarding ratio of node B with respect to node A. $HELLO_{AB}$ denotes route Hello packet forwarding ratio of node B with respect to node A.

The Data Packet (DP) forwarding ratio of each node is calculated based on the equation 3.

$$DP_{AB} = \frac{NDF_{AB}}{NDR_{AB}} \quad (3)$$

where *NDF* denotes number of data packets actually forwarded by node B evaluated by node A and *NDR* denotes number of data packets actually received over time with n number of interactions. The equation 2 and equation 3 will substitute to equation 1.Likewise every node could calculate the direct trust value of all its one hop neighbours and update its ETtable. Each node can monitor its neighbouring nodes' forwarding behaviour by using passive acknowledgment.

Sometimes direct trust is not enough to ensure the trustworthiness of a particular node hence second hand information such as opinion about others of a particular target node also known as indirect trust. The indirect trust is calculated based on the following equation 4.

$$IDT_{AB} = \omega_1 * DT_{AB} + \omega_2 * DT_{CB} \quad (4)$$

Where ω denotes weighting factor and $\omega_1 + \omega_2 = 1$. IDT denoted by indirect trust, A and C are evaluating node and B is evaluated node and DT denotes direct trust. In the above equation C denotes one hop neighbours who had interactions with B already.
Now a node can calculate the final trust from equation 1 and equation 4.

$$FT_{AB} = \omega_1 * DT_{AB} + \omega_2 * IDT_{AB} \quad (5)$$

In the above equation FT_{AB} denotes final trust of node B with respect to node A and ω denotes weighting factor and$\omega_1 + \omega_2 = 1$.

After the final trust computation phase, by using final trust values obtained for every node, an evaluating node assigns a reward for each interaction that had with one hop neighbouring nodes based on the threshold values. These threshold values can be changed according to the user specification. The reward value ranges between 0 and 1. 1 specifying the maximum, 0 specifying no reward and 0.5 specifying intermediate reward. The specification is given below.

$$\begin{gathered} R = 1 \; when \; FT_{AB} >= TH1 \\ R = 0.5 \; when \; FT_{AB} <= TH1 \; and \; FT_{AB} >= TH2 \\ R = 0 \; when \; FT_{AB} <= TH3 \end{gathered} \quad (6)$$

Thereafter evaluating node utilizes the Q-Learning algorithm to evaluate the overall performance of its neighbour nodes because a node can get high reward for some action and vice versa hence based on the equation 6 an evaluating node can get an aggregated reward means overall performance of its neighbours.

$$AT_{AB} = [\,(IR)_{AB} + \gamma \, MAX(R)_{AB}(n)]/2\,)/n \quad (7)$$

where R represents the reward, IR denotes the immediate reward over time and AT denotes the aggregated trust. γ is a relative value and always>0. Immediate reward for all the neighbours is calculated based on its battery capacity, memory and bandwidth due to processing capabilities of each node these factors can change and also affect the overall network performance. Hence we consider each node's recent battery power, bandwidth and memory as immediate reward because they may change over time. So immediate reward can be calculated as,

$$(IR_{AB}) = \omega_1 * \text{Battery Capacity}_{AB} + \omega_2 * \text{Memory}_{AB} + \omega_3 * \text{Bandwidth}_{AB} \quad (8)$$

In the above equation IR_{AB} denotes immediate reward of node B with respect to node A.

5.3 Identifying Gray hole nodes

Once aggregated trust is calculated, now node A can take decision on node B. This aggregated trust will be checked against the predetermined threshold value which is mentioned in table 2. Here the threshold values (TH) can also be changed according to the user specification.

Table 2. Threshold table

Level	Threshold	Classification of nodes
1	>= TH_1	Trusted node
2	<=TH_1 and >=TH_2	Partially Trusted node
3	<=TH_3	Gray hole node

VI. SIMULATION RESULTS AND DISCUSSION

The proposed model is implemented in Network Simulator 3(NS3). The study area is 500mx1000m for simulation with random way point mobility model. The number of nodes involved

for simulation is 100. The following table 3 gives illustrate the simulation parameters. The aim of the simulation experiment is to identify and isolate the misbehaving nodes hence we chose the black hole nodes in a random fashion and include in the network to validate the performance of proposed model. We also set source and destination in a random fashion. We increase the number of Gray hole nodes step by step and run the experiment. According to the algorithm specification, we have taken four numbers of interactions; hence we run the simulation for four times with varying number of malicious nodes for analysis over the period of time. We have done the following experiments,

- Our aim is to identify the Gray hole nodes, so that it is necessary to know the impact of Gray hole nodes. In this regard, we include the Gray hole nodes by increasing percentage and observed the packet dropping ratio.
- Include the Gray hole nodes with increasing number in normal DSR routing protocol and identify them by using proposed model and Sukla model [2].
- Comparing the packet delivery ratio, packet dropped ratio and end to end delay of proposed model, Sukla model[2] and DSR routing protocol.

6.1 Experiment 1

Observe the packet dropping ratio by increasing the number of Gray hole nodes. The Figure. 4 shows when number of Gray hole nodes increases, packet dropping ratio is also increased proportionally.

Table 3. Simulation Parameter

System Parameters	Values Utilized
No. of Mobile Nodes	100
% of Gray hole	Increasing from 10% to 80%
Mobility Model	RWPM
Simulation Duration	100 Sec
Time interval	.5 Sec
Simulation Size	500mx1000m
Routing Protocol	DSR
Data rate	3072bps
Packet Size	64 Bytes
Wi-Fi Ad Hoc	802.11b
Data Traffic	UDP
MaxNode Speed	20m/s
Node Pause	0s
Transmission Range	7.5dbm
Threshold Value1	6.0
Threshold Value2	4.0

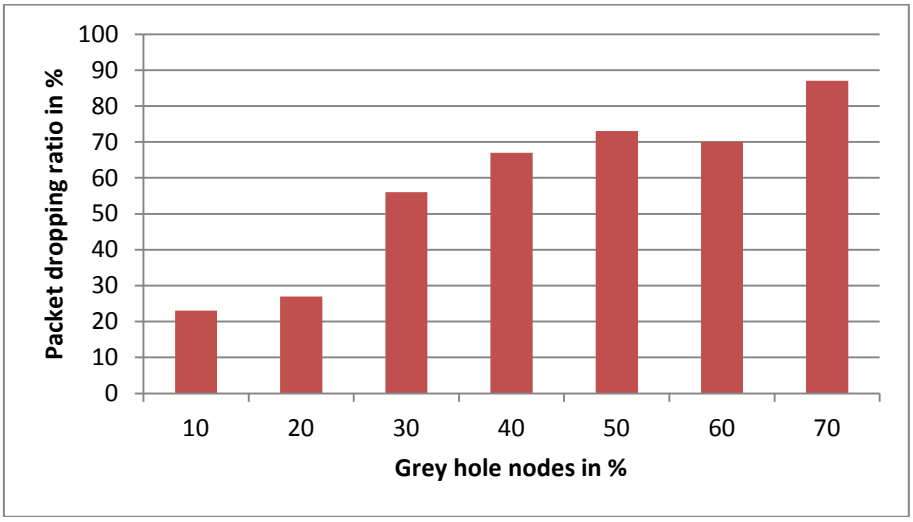

Figure 4. Packet Dropping Ratio

6.2 Experiment 2

The ultimate aim of this experiment is to identify the misbehaving nodes. Hence we increase the Gray hole nodes by 10%, 20%, 30%, 40%, 50%, 60% and 70% respectively to assess the performance of proposed model against Sukla model. According to the aggregated trust from the proposed model, the detection of misbehaving nodes i.e Gray hole can be executed. We observe that as the number of Gray hole nodes has increased, the detection ratio of proposed model is also increased proportionally. In addition, the detection ratio is also high compare with Sukla model. The detection ratio is 11.73% is high compared with Sukla model. Figure 5. Shows the Detection Ratio.

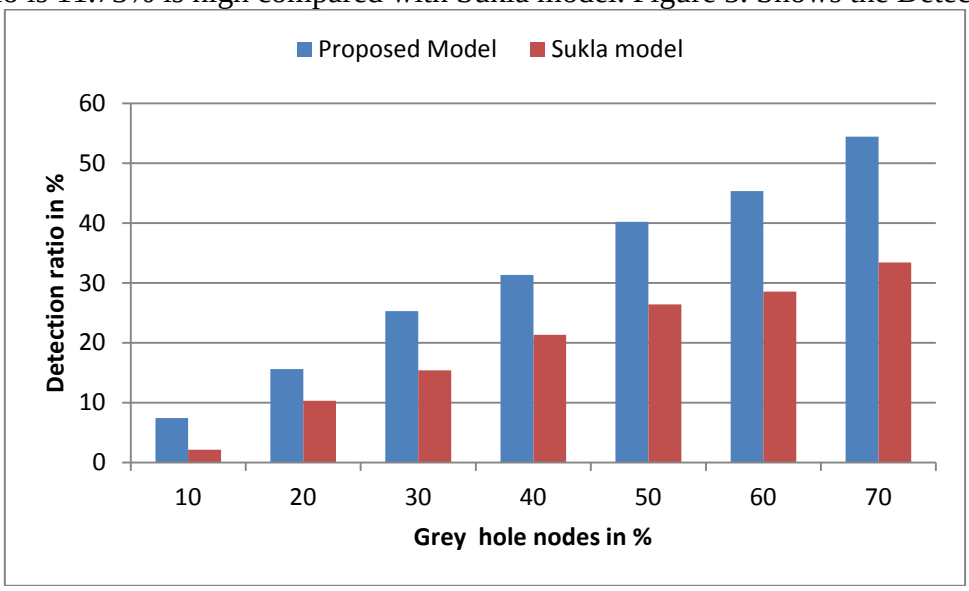

Figure 5. Detection Ratio

Experiment 3: The following performance like metrics packet delivery ratio and end to end delay evaluated.

Packet delivery ratio: This metric analyses the packet delivery ratio of each node as well as overall network. It is measured by number of packets actually received divided by number of packets actually sent. Figure 6 depicts the packet delivery ratio of proposed model is very high over sukla model because, Gray hole nodes are isolated from the network. Since they will not be involved in routing operation. The packet delivery ratio is 17.45% high compared with sukla model.

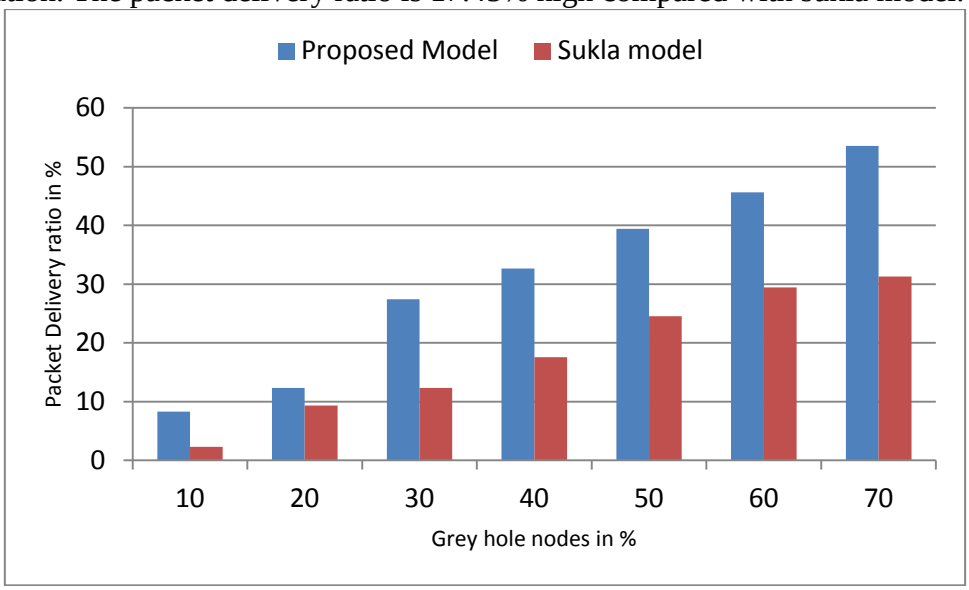

Figure 6. Packet Delivery ratio

End to End delay: It is measured by the average time taken by a packet from the source to the destination. Hence it is calculated by difference between the arrival times and sending time of packets from the source to the destination and the results will be divided by total number of

connections between the sources to the destinations. The Figure 7 shows the end to end delay of proposed model is low compared with sukla model. The end to end delay is 15.45% low compared with sukla model.

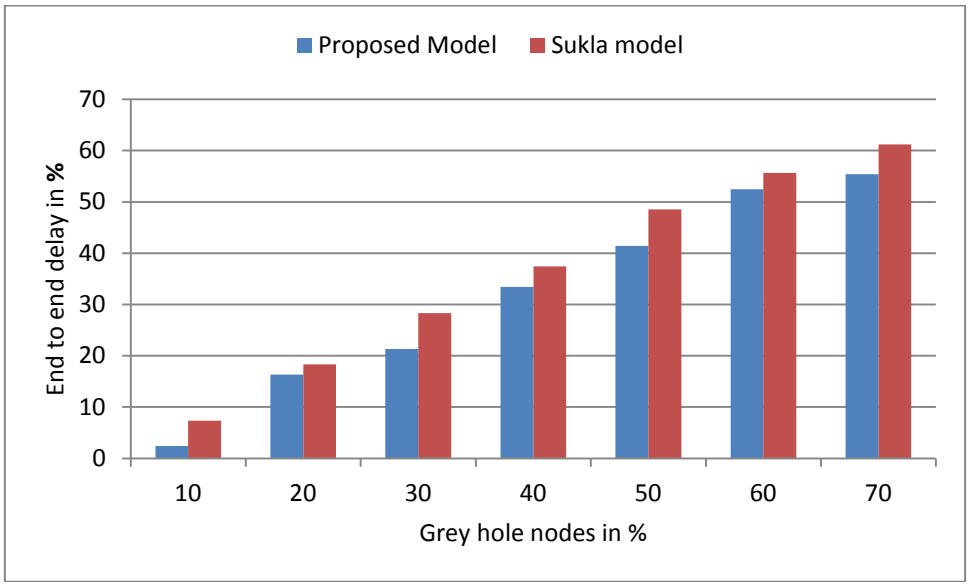

Figure 7. End to end delay

VII. CONCLUSION

In this paper a Trusted DSR Routing Protocol to withstand against Gray Hole attack in MANET using Q-Learning is proposed. The trustworthiness of node is assessed by aggregated trust which is evaluated based on the direct, indirect trusts and immediate trusts. In addition Q-learning algorithm is used to enrich the proposed model. The simulation results shows better results compared with the existing one. In this model we do not make use of any complex algorithms so that it is suitable for resource constrained MANET devices.

REFERENCES

[1] S.Sivagurunathan, K.Prathapchandran and A.Thirumavalavan, "Authentication using trust to detect Misbehaving nodes in Mobile Ad Hoc Networks using Q-Learning", International Journal of Network Security & Its Applications (IJNSA), Vol.8, No.3, May 2016

[2] Sukla Banerjee, (2008) "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008, WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[3] V. Shanmuganathan & T.Aanand, (2012) "A Survey on Gray Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.2, No.6.

[4] Deng H, Li W & Agrawal DP, (2002) Routing Security in Wireless Ad-hoc Networks. IEEE Communications Magazine, Vol.40, No.10, pp70–75.

[5] Fan-Hsun Tseng , Li-Der Chou1 & Han-Chieh Chao, (2011) "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences 2011, Vol.1, No.4.

[6] Michael Weeks & Gulsah Altun1, (2006), "Efficient, Secure, Dynamic Source Routing for Ad-hoc Networks", Journal of Network and Systems Management, Vol. 14, No. 4.

[7] Charles E.Perkins, (2001) "Ad hoc networking", Addision Wesley.

[8] William Stallings, (2003) "Cryptography and Network Security", Pearson Education

[9] Y.Xiao, X.Shen & D.Z.Du, (2007) "Wireless Network Security", Springer.

[10] Sivagurunthan .S & Prathapchandran. K, (2014) "Trust based Security schemes in Mobile Ad Hoc Networks – A Review" 978-1-4799-3966-4/14, DOI 10.1109/ICICA.2014.67, IEEE.

[11] Xiaoyong Li, Feng Zhou & Junping Du,v(2013) "LDTS: A Lightweight and Dependable trust system for Clustered Wireless Sensor System", IEEE Transactions on information forensics and security, Vol.8, No.6.

[12] R C Mayer, J H Davis & F D Schoorman, (1995) "An Integrative Model of Organizational Trust- Academy of Management Review", vol. 20 (3), pp. 709-734.

[13] Bamberger and Walter, (2010) "Interpersonal Trust – Attempt of a Definition", Scientific Report.

[14] Liu z, JoyA.W & Thompson R A, (2004) "A dynamic trust model for mobile ad hoc networks", Proceeding of the 10 th IEEE International Workshop on Future trends of distributes computing systems, pp-80-85.

[15] A.Boukerch & K.EL-Khatib, (2007) "Trust based Security for Wireless ad hoc and Sensor networks", Computer Communications, vol.30, pp.2413-2424.
[16] Feng Zhang, Zhi-Ping Jia, Hui Xia, Xin Li & H.M. Sha Edwin, (2010) "Node trust evaluation in mobile ad hoc networks based on multi-dimensional fuzzy and Markov SCGM(1,1) model", Computer Communications, vol.35, pp.589-596.
[17] Mentari Djatmiko, Roksana Boreli, Aruna Seneviratne & Sebastian Ries, (2013) "Resources aware trusted node selection for content distribution in mobile ad hoc networks", Wireless networks, vol.19, pp.843-856.
[18] Q-Learning Algorithm, Retrieved on January, 12, 2015 from http://www.wikipedia.com
[19] Li X & Wu J, (2006) "Improve searching by reinforcement learning in unstructured P2Ps," International Conference on Distributed Computing Systems Workshops, pp.1-6.
[20] Wang Q & Zhan Z, (2011) "Reinforcement Learning Model, algorithms and its Applications", International Conference on Mechatronic Science, Electric Engineering and Computer, pp.1143-1146.
[21] Jin-Hee Cho, Ananthram swamia & Ing-Ray Chen, (2012) "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks", Journal of networks and computer applications, Vol.35, pp 1002-1012.
[22] Vaishali Mittal, (2011), "Prevention and Elimination of Gray Hole Attack in Mobile Ad-Hoc Networks by Enhanced Multipath Approach", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol.4 No. 5.
[23] Avenash Kumar & Meenu Chawla , (2012) " Destination based group Gray hole attack detection in MANET through AODV", International Journal of Computer Science Issues, Vol. 9, No.1.
[24] Onkar V. Chandure& V. T. Gaikwad, (2011), "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV routing protocol in MANET", International Journal of Computer Science and Information Technologies, Vol. 2, No.6, pp 2607-2613.
[25] Maha Abdelhaq, (2011) "A Local Intrusion Detection Routing Security over MANET Network", International Conference on Electrical Engineering and Informatics, IEEE.
[26] R. H. Jhaveri, (2013) "MR-AODV: A Solution to Mitigate Black-hole and Gray-hole Attacks in AODV Based MANETs" Third International Conference on Advanced Computing & Communication Technologies, IEEE, pp. 254-260.
[27] S. J. Patel, (2012) "A Novel Approach to Gray-hole and Black-hole Attacks in Mobile Ad-hoc Networks" Second International Conference on Advanced Computing & Communication Technologies, 2012 IEEE, pp 556-560.
[28] Jaydip Sen, M.Grish Chandra and Harihara, "A Mechanism of detection of Gray hole attack", IEEE Digital library, 2007.
[29] S.Marti, T.Guili, K.Lai and M.Baskar, "Mitigating routing misbehavior in mobile ad hoc networks", in proceedings of MOBICOM 2000