Trust Based Routing to Mitigate Black Hole Attack in MANET

[1]S. P. Manikandan, [2]R. Manimegalai

[1]Research Scholar, Department of Computer Science and Engineering
Anna University, Regional Centre, Coimbatore, India
[2]Professor, Department of Computer Science and Engineering
Park College of Engineering and Technology, Coimbatore, India
mkandan_2000@yahoo.com

Abstract: This paper proposes a novel trust based routing mechanism to mitigate black hole attack in Mobile ad hoc Networks (MANETs). The proposed model is based on Trust Correlation Service (TCS) mechanism. This aggregates and distributes the trust among nodes that are participating in the wireless network. The trust for a node and the correlation score for various pairs of nodes is computed before establishing the route for communication between the source and destination. The Trust for a node is computed based on various factors such as node reputation, its ability to defend against various attacks and unauthorized resource utilization. A correlation score for a pair of nodes is computed based on their internal trust, required level of trust, number of packet sent and delivered to the destination. It is computed for every pair of intermediate nodes along the path from source to destination. In this paper, the Dynamic Source Routing (DSR) Protocol is modified to find a trusted route rather than the shortest route between source and destination. The proposed trust based model yields reduced data drop rate and end-to-end delay. The simulation results achieved are promising with improved throughput.
[S. P. Manikandan, R. Manimegalai. **Trust Based Routing to Mitigate Black Hole Attack in MANET.** *Life Sci J* 2013;10(4s):490-498] (ISSN: 1097-8135). http://www.lifesciencesite.com. 75

Keywords: Mobile ad hoc networks (MANET), Dynamic Source Routing (DSR), MANET Security, Trust and Reputation

1. Introduction

With the advent of internet technologies, there is a paradigm shift towards distributed computing such as grid and cloud technologies in recent years. From current static networking systems with client-server architectures, it can be seen that the trend is moving more towards peer-to-peer or ad hoc networking systems. Peer-to-peer and ad hoc networks have totally different and decentralized architecture. A Mobile Ad hoc Network (MANET) is a system which consists of small devices communicating spontaneously through wireless communication medium. With devices being mobile, interconnections between them change frequently. Also, instead of the usual dedicated fixed routers, nodes in the network relay network traffic for other peers [1]. Thus, the dynamic and open nature of mobile ad hoc networks threw up many challenges especially in secured communication. The security in MANET depends on many factors such as availability, confidentiality, integrity, authentication, non-repudiation, access control and usage control [2, 3]. It should be understood that, in real life settings, nodes would necessarily not cooperate with each other. Such selfishness leads to malicious acts such as retaining its own resources and harming others. Hence, the aim is to establish trust relationships with nodes that behave correctly and exclude those nodes from the system which do not cooperate.

There is every possibility of malicious nodes attempting Passive and Active attacks against the network [4]. In the former type of attacks a malicious node, only listen in or eavesdrops upon packet contents, whereas, in active attacks, it could imitate drop or modify legitimate packets. The severity of such attacks increased manifold when these were performed in collusion. For example, blackhole attack is an active attack. It is a Denial of Service (DoS) attack in which a malicious node absorbs data packets without forwarding to the destination [5]. The malicious nodes also attract data packets by wrongly informing the availability of the route to the destination. The consequences of such a black hole attack on the network could be catastrophic.

Secured routing protocols [6, 7, 8] are developed using authentication and encryption mechanism, to ensure confidentiality and integrity during communication. But such protocols need a centralized, trusted third party, which in turn made them ineligible for MANETs [9]. Moreover, these secured routing protocols do not completely prevent malicious or compromised nodes that act as authorized participants and try to misbehave. As in real time society, one would trust another to fulfill

an action, though the former could not guarantee the latter's behavior [10]. Hence the concept of trust was introduced into computing networks, to measure expectations or uncertainties that an entity had about another's behavior for a certain action in the future.

The concept "trust" is taken from social sciences and described as a measure of subjective belief about behaviors of an entity. The term "Trust Management" was coined by Blaze, et al., [11], categorizing it as a separate factor for network security services. Trust management is essential, particularly when several nodes combine to start a network without earlier interactions. The participating nodes must build trust relationships among themselves. Methods like bootstrapping, coalition operation, and third party certificate authentication are used for building initial trust in the network [12]. Trust management also includes trust establishment, trust update, and trust revocation. Collecting trust information for evaluating trustworthiness is difficult because of MANET's dynamic topology.

Trust could be derived from direct interactions or recommendations. The trust management in MANET has the following two advantages: (i) The evaluation of trust for every node help in discriminating good and malicious entities. Every entity maintains a trust history which records the behavior of the other entity. This trust history is helpful in avoiding the malicious or suspected entity. (ii) The trust management predicts future behavior of all entities in the network and improves the network performance. Based on the trust evaluated dynamically in the network, an incentive for good/honest behavior for the participating node can be given. Similarly, a penalty for selfish or malicious behaviors in the network can be implemented.

Broch, et al., have developed the Dynamic Source Routing protocol (DSR) for MANET [13]. In DSR, when a node sends out a ROUTE REQUEST message, all other nodes that receive the message include their identity in the route and forward it to neighbors. This request message is forwarded till either the message reaches the destination or an intermediate node which has the route to the destination. Then the destination node or the intermediate node sends back a REPLY message with the full route details to the source node. After receiving replies from many paths, the source selects the best route (shortest route by default) stores it and send a message along that path. The better the route metrics (number of hops, delays, bandwidth, or other criteria) the earlier the REPLY reaches at the source, the higher the preference given to that route, and longer it would stay in the cache. When a ROUTE REPLY reaches very quickly after a ROUTE REQUEST was sent out, it is an indication of a short path, since it's mandatory for the nodes to wait for a time equal to the length of the route they could advertise, before sending it. This is done to avoid a storm of replies. If there is a link failure, the node could not forward the packet to its neighbor; it sends an error message to the source. Routes that have a failed link could be `salvaged' by taking an alternate partial route.

In this paper, a Trust Correlation Service (TCS) mechanism is proposed. The proposed model aggregates and distributes current trust of nodes participating in the wireless network. A correlation score is proposed to find the correlation between the source node and intermediate node or intermediate - intermediate node. The proposed correlation score is incorporated in DSR. The routing protocol is modified to find a trusted route rather than the shortest route between source and destination.

2. Related Works

Hu et al., [14] introduced ''packet leash'' to defend against wormhole attacks through the addition of information about geography or time to a packet to restrict its maximum permitted transmission distance. This requires time synchronization and Global Positioning System (GPS). The proposed method used two types of leashes: geographical leashes and temporal leashes. Geographical leashes restricted the distance the packet can travel from the sender to the destination and the temporal leash specified the upper bound of the lifetime of the packet. These leashes help prevent wormhole attacks as it allows the destination node to detect if the packet has travelled further than the leash specifications. The proposed method also introduced a protocol, TIK, which provides instant authentication of received packets.

Secured tracking of node encounters (SECTOR) is proposed by Capkun et al. in [15] which apply similar principles as packet leashes, the only difference being that it measures distance in a single hop. SECTOR needs special hardware at each node to respond to a one-bit challenge with an immediate one-bit response using a MAD protocol.

Wang et al., [16] have proposed the idea of using an end-to-end mechanism with each node appending its time and location information to a detection request, and then the destination checks claimed time and locations to identify wormhole attacks. To lower the overhead, Cell-based Open Tunnel Avoidance (COTA) is proposed for

distributed processing.

Zhen, et al., [17] have used round-trip time (RTT) to verify whether a node is a real neighbor or not. When a node receives a RREQ, it checks the RTT. If RTT exceeds a threshold, the RREQ is dropped. Otherwise, the RREQ is a legal request. This mechanism can detect replay attacks/sort out wormhole attacks in AODV, but it implies that routing messages cannot be altered, and all nodes are time synchronized with a key that exist between a node pair.

A graph theoretic framework is presented by Poovendran et al. in [18] for characterization of the wormhole attack. The proposed graph showed that a communication graph is a connected subgraph of the geometric graph of the network. Local broadcast key based cryptographic solution is provided to prevent the wormhole attacks. A distributed mechanism was established to provide local broadcast keys. Analytical evaluation based on spatial statistics theory was presented for detection of wormhole attacks.

Panaousis et al. have [19] proposed a novel routing mechanism called AODV-Wormhole Attack Detection Reaction AODV-WADR. The AODV-WADR, help in determining whether a neighbor node has created a wormhole tunnel in the MANET or not. A combination of timing and cryptography is used to ensure that the neighboring nodes are not tunneled. When a wormhole attack is detected by the source node while sending packets to a destination, it deletes the route containing the malicious wormhole node and adds it to the blacklist. Simulations were carried out using the network simulator NS-2. The simulation results showed that the performance of AODV-WADR is more efficient than AODV in terms of packet loss in all cases.

Vaidya, et al., [20] have proposed a robust, secure, multipath routing protocol, SAODV-MAP, based on AODV. The proposed protocol is robust against communication failures and malicious threats. The approach discovers multiple paths by computing node-disjoints and fail-safe paths. Security is incorporated in the proposed protocol by secure neighbor discovery and secure route discovery. The routing control messages are protected by keyed message authentication code.

3. Methodology

In ad hoc networks, as there is no centralized authority, most of the designed protocols rely on co-operation and trust among nodes in the network. A malicious user can easily exploit this trust to compromise all participating nodes. While doing the transaction, nodes can enter and leave the network at any time. In such scenario, transactions can break and restore without proper authentication. If some of the nodes are compromised, it is possible that few nodes are routed to malicious servers. This infrastructure has a very high tendency to lead the "innocent" user towards the malicious node. Traditionally, authentication in any network depends on reliable key management, to produce original credentials, which cannot be falsified. In such network configurations, integration of public key infrastructure, certification authorities, and private key mechanisms are very difficult. Two concepts are introduced in this paper, which are also implemented over the existing DSR routing protocol.

Definition I: The Internal Trust (IT) of the node is computed based on its ability to defend against virus attacks, network attacks and unauthorized resource utilization.

$$IT = \sum \varphi_{Av} + \varphi_{Fw} + \varphi_{Aut} \qquad (1)$$

where

$$\varphi_{Av} = \begin{bmatrix} 0, \text{ if antivirus product is not present} \\ 0.5, \text{ if antivirus product is present but not updated} \\ 1, \text{ if antivirus is product is present and up to date} \end{bmatrix}$$

$$\varphi_{Fw} = \begin{bmatrix} 0, \text{ if firewall not present} \\ 2, \text{ if firewall is present and not upto date} \\ 4, \text{ if firewall is present and upto date} \end{bmatrix}$$

$$\varphi_{Aut} = \begin{bmatrix} 0, \text{ if authorization mechanism of any type, not present} \\ 1, \text{ if password based authorization mechanism present} \\ 2, \text{ if alternative authorization mechanism such} \\ \quad \text{as biometrics is present} \end{bmatrix}$$

Definition II: The proposed Trust correlation score (TCS) between two nodes U and V is given by

$$TCS_{uv} = \alpha . \sum \frac{(u_{IT} - v_{IT})}{\sqrt{(u_{IT} - v_{IT})^2}} + \frac{P_{dv}}{P_{sv}}$$

where

u_{IT} *and* v_{IT} internal trust of nodes U and V (2)

α is the trust level required

P_{dv} is the total packet delivered by v

P_{sv} is the total packet sent to v

where U originates a request and V forwards the request.

The formats of Route Request (RREQ) and the Route Reply (RREP) of the DSR protocol are modified to accommodate the trust value of a node's neighbor. The optional header feature of

DSR protocol supports the modification of the header to store the TCS values. The RREQ and the RREP of the modified DSR routing protocol are shown in Figure 1 and Figure 2.

IP Header	DSR Fixed Header	DSR Route Request Header	Intermediate Addresses Address1 Address2, AddressN	TCS values

Figure 1: The modified RREQ

IP Header Reply	DSR Fixed Header	DSR Route Reply Header	Addresses Addr Src Addr1.. AddrN Addr Dst
Reply TCS Between src and dest	DSR Source Route Header	DSR Source Route Addr1... AddrN	DSR Source Route TCS

Figure 2: The modified RREP

Consider the network scenario shown in Figure 3. The malicious nodes are indicated by red. The shortest path between the source and destination is given by S – 8 - D. This route is taken by normal routing protocols and hence involved in a lot of packet drops. Possible routes from source to destination are given in Table I.

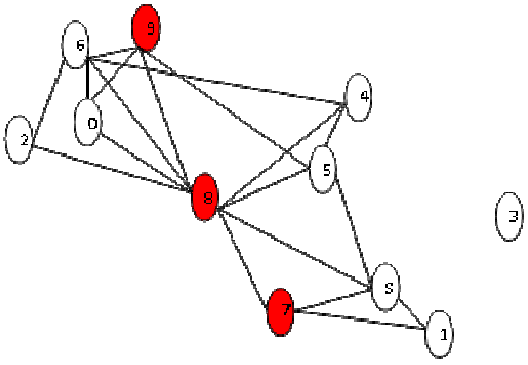

Figure 3: A Simple MANET

TABLE I: Possible Routes between S and D

Route	Path
R1	S – 8 – D
R2	S – 7 – 8 – D
R3	S – 5 – 9 – D
R4	S – 8 – 2 – D
R5	S – 8 – 9 – D
R6	S – 5 – 4 – 6 – D

From Table I it can be seen that the route R6 is the safest route in the given scenario, though it has the maximum number of hops compared to all other routes. The internal trust parameter for a given scenario is shown in Table II. The maximum internal trust that can be obtained as per rule is 7 and *node 2* achieves the highest level of internal trust. However nodes *7, 8, 9* have the minimum internal trust with trust scores of less than 2.5.

TABLE II: Internal Trust Parameters

Security Type	S	n1	n2	n3	n4	n5	n6	n7	n8	n9	D
Antivirus	0.5	2	1	0	1	1	1	1	0	0	1
Firewall	2	2	4	4	2	4	4	0	1	0	2
Authorization	2	2	2	0	2	0	1	1	0	2	2
Total	**4.5**	**6**	**7**	**4**	**5**	**5**	**6**	**2**	**1**	**2**	**5**

It can be observed from Table II that nodes *N1*, *N2* and *N6* have very high trust values, hence from these nodes through which communication takes place. The correlation between every pair of nodes is computed. The correlation of two nodes shows the degree to which the nodes are related. Pearson Product Moment Correlation is used for measuring the correlation; it is designated ρ or "*r*" when computed in a sample. Pearson's correlation reflects the linear relationship between two entities and ranges from +1 to -1 where +1 reflects perfect positive linear relationship. Table III shows the correlation between possible pair of nodes. It can be seen that correlation among itself is 1 whereas relationship between node S and node 6 is strongly negative which implies that the trust level of S is very high compared to trust levels of node 7. Similarly, trust levels between node N1 and node N2 are independent and hence have almost 0 correlations.

TABLE III: Correlation between Nodes

	S	N1	N2	N4	N5	N6	N7	N8	N9	D
S	1	0.09	-0.33	0.49	0.65	-0.3	-0.46	0.56	-0.29	-0.39
N1	0.09	1	-0.01	0.02	0.03	0.19	-0.1	-0.04	0.13	-0.35
N2	-0.33	-0.01	1	0.04	-0.24	-0.08	0.14	0.06	0.11	-0.05
N4	0.49	0.02	0.04	1	0.17	0.42	-0.16	0.55	0.51	-0.35
N5	0.65	0.03	-0.24	0.17	1	-0.34	-0.47	0.19	-0.28	-0.36
N6	-0.3	0.19	-0.08	0.42	-0.34	1	0.66	-0.06	0.01	-0.02
N7	-0.46	-0.1	0.14	-0.16	-0.47	0.66	1	0.09	0.18	-0.05
N8	0.56	-0.04	0.06	0.55	0.19	-0.06	0.09	1	-0.29	0.08
N9	-0.29	0.13	0.11	0.51	-0.28	0.01	0.18	-0.29	1	-0.39
D	-0.39	-0.35	-0.05	-0.35	-0.36	-0.02	-0.05	0.08	-0.39	1

The packet delivery ratio between the nodes is computed to understand the packet drops across the malicious nodes. Table IV shows the packet delivery ratio between the nodes at the instance of the node formation shown in Figure 3. The PDR is between 65% to 95%.

TABLE IV: Packet Delivery Ratio between Nodes

S	N1	N2	N4	N5	N6	N7	N8	N9	D
0.6942	0.9227	0.7053	0.6719	0.7632	0.8819	0.684	0.841	0.8011	0.7994
0.9249	0.6481	0.9626	0.7587	0.8498	0.7501	0.7589	0.9259	0.7199	0.8474
0.9063	0.9013	0.7693	0.9517	0.6478	0.959	0.8362	0.7167	0.9097	0.879
0.8699	0.9706	0.862	0.9756	0.624	0.669	0.8181	0.6161	0.7773	0.7817
0.6109	0.853	0.951	0.7973	0.8932	0.6508	0.641	0.7529	0.9479	0.8529
0.7008	0.6395	0.9043	0.845	0.8043	0.6538	0.8014	0.843	0.6556	0.7244
0.9526	0.7676	0.7352	0.8007	0.699	0.7727	0.9492	0.9046	0.9814	0.6817
0.7037	0.6483	0.8905	0.9448	0.7579	0.8272	0.8654	0.6843	0.9527	0.7685
0.9896	0.9841	0.9304	0.7274	0.8471	0.9813	0.8946	0.7716	0.6892	0.6964
0.6646	0.8958	0.7905	0.7907	0.7522	0.9886	0.8935	0.6005	0.6654	0.7914

The trust correlation score computed using Table III, and Table IV is shown in table V without multiplying the output with alpha value and the TCS with alpha value = 0.5 is shown in Table VI.

TABLE V: Trust Correlation

S	N1	N2	N4	N5	N6	N7	N8	N9	D
2	0.18	-0.66	0.98	1.3	-0.6	-0.92	1.12	-0.58	-0.78
0.18	2	-0.02	0.04	0.06	0.38	-0.2	-0.08	0.26	-0.7
-0.66	-0.02	2	0.08	-0.48	-0.16	0.28	0.12	0.22	-0.1
0.98	0.04	0.08	2	0.34	0.84	-0.32	1.1	1.02	-0.7
1.3	0.06	-0.48	0.34	2	-0.68	-0.94	0.38	-0.56	-0.72
-0.6	0.38	-0.16	0.84	-0.68	2	1.32	-0.12	0.02	-0.04
-0.92	-0.2	0.28	-0.32	-0.94	1.32	2	0.18	0.36	-0.1
1.12	-0.08	0.12	1.1	0.38	-0.12	0.18	2	-0.58	0.16
-0.58	0.26	0.22	1.02	-0.56	0.02	0.36	-0.58	2	-0.78
-0.78	-0.7	-0.1	-0.7	-0.72	-0.04	-0.1	0.16	-0.78	2

TABLE VI: Trust Correlation with alpha = 0.5

	S	N1	N2	N4	N5	N6	N7	N8	N9	D
S	1	0.09	-0.33	0.49	0.65	-0.3	-0.46	0.56	-0.29	-0.39
N1	0.09	1	-0.01	0.02	0.03	0.19	-0.1	-0.04	0.13	-0.35
N2	-0.33	-0.01	1	0.04	-0.24	-0.08	0.14	0.06	0.11	-0.05
N4	0.49	0.02	0.04	1	0.17	**0.42**	-0.16	0.55	0.51	-0.35
N5	**0.65**	0.03	-0.24	**0.17**	1	-0.34	-0.47	0.19	-0.28	-0.36
N6	-0.3	0.19	-0.08	0.42	-0.34	1	0.66	-0.06	0.01	**-0.42**
N7	-0.46	-0.1	0.14	-0.16	-0.47	0.66	1	0.09	0.18	-0.05
N8	0.56	-0.04	0.06	0.55	0.19	-0.06	0.09	1	-0.29	0.08
N9	-0.29	0.13	0.11	0.51	-0.28	0.01	0.18	-0.29	1	-0.39
D	-0.39	-0.35	-0.05	-0.35	-0.36	-0.02	-0.05	0.08	-0.39	1

The ideal source to destination path is shown in using red colored arrows.

4. Experimental Results

The OPNET Modeler is used to construct models for two different purposes: to study system behavior and performance; and to deliver a modeling environment to end users. A network model contains communicating entities called nodes and developed using the Node Editor. Network models consist of nodes and links that can be deployed within a geographical context. Node models consist of modules and connections. For simulation the network is configured with the parameters shown in Table VII. The following three scenarios are considered for simulation:

- DSR protocol without Black hole attack.
- DSR protocol with Black hole attack
- Trust based DSR with Black hole attack.

TABLE VII: Simulation Parameters

Number of Nodes	50
Number of Malicious Nodes	4
Malicious Activity	Black Hole
Routing Protocol Used	DSR
Trajectory of Nodes	Random waypoint
Data Rate of Node	11Mbps
Transmit Power of Nodes	0.005 Watt

The simulation results are shown in Figures 4, 5, 6, 7 and 8, when simulated with random traffic. In Figure 4, it can be seen that the average number of hops increases by 5% in the proposed method which is indicated using green color when compared to regular DSR which is indicated using blue color. This is due to node selection based on trust which results in additional hops that need to be taken from source to destination.

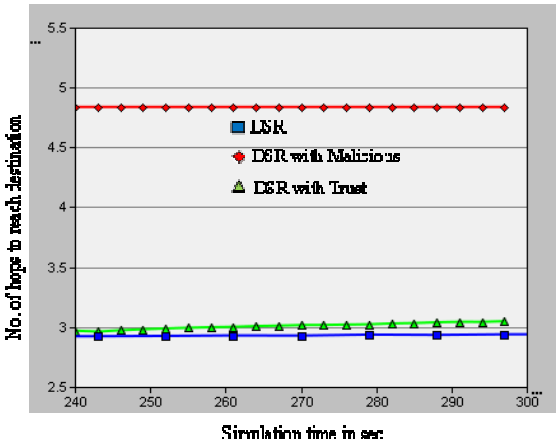

Figure 4: Number of hops to reach destination

The average routing traffic received by the nodes in the network is shown in Figure 5. It can be seen that due to swallowing of packets by malicious nodes, many nodes do not receive requests to participate in the network, which is indicated in red color, resulting in very low overall routing traffic. Routing traffic is 8% more in proposed algorithm compared to regular DSR protocol.

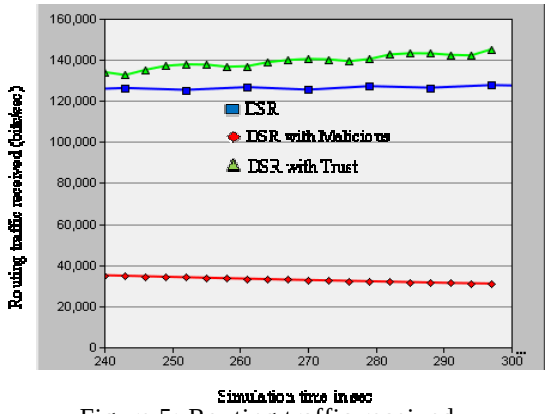

Figure 5: Routing traffic received.

The data dropped (bits/sec) and average end to end delay (sec) for the packets to reach from source to destination is shown in Figure 6 and Figure 7. It is seen the end to end delay due to malicious node in the network is roughly three times more than regular network without attack. The end to end delay in the proposed trust based protocol is higher than the regular DSR network due to the longer route taken by the packets. However, the difference is negligible and will not affect even streaming data packets.

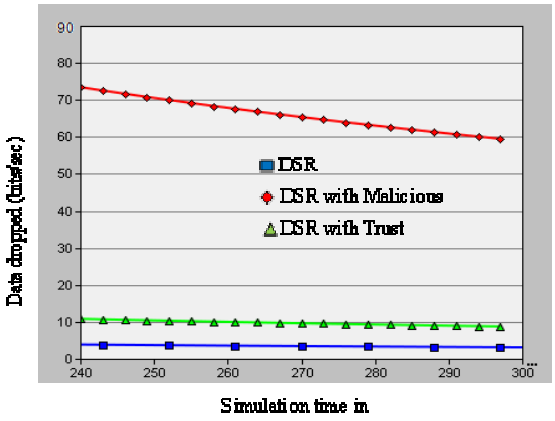

Figure 6: Data dropped due to retry threshold exceeding

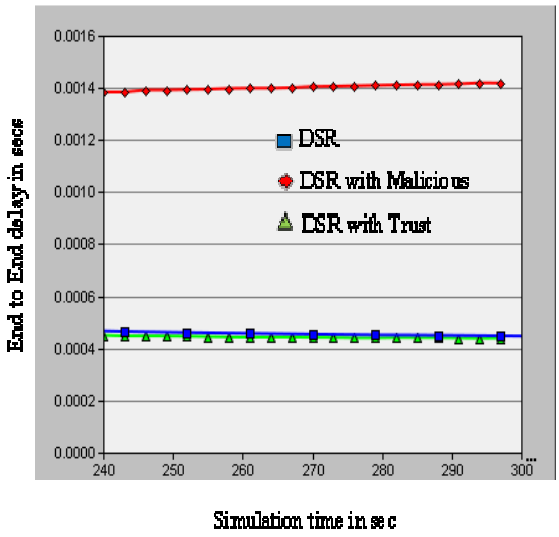

Figure 7: End to End delay (All three scenarios)

Figure 8 shows the throughput of the simulation. It can be seen that the proposed model performs better than DSR though it takes a longer path to reach the destination. The proposed network not only increases the security of the network but is also found to improve the overall throughput. Network simulated with malicious node displays very low throughput due to the large amount of data drop. Table VIII, tabulates the values hop count, end to end delay, throughput and data dropped for all scenarios.

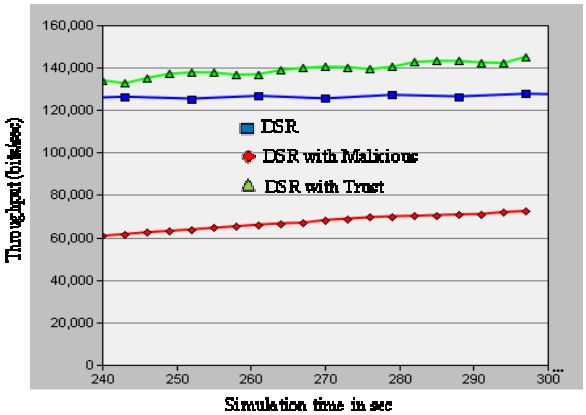

Figure 8: Throughput of the network

TABLE VIII: Quality of Service Parameters Measured Under Various Experimental Setup

Parameters	Mechanism	Measured Value
Num. of HOPs to reach Destination	Dynamic Source Routing (DSR)	2.890162
	DSR with Malicious Nodes	4.837681104
	DSR with Trust Based Mechanism	3.010154262
Data Dropped (Bits / sec)	DSR	3.550372
	DSR with Malicious Nodes	65.97774297
	DSR with Trust Based Mechanism	9.70435
End to End Delay (sec)	DSR	0.000437
	DSR with Malicious Nodes	0.001402751
	DSR with Trust Based Mechanism	0.000443
Throughput (Bits / sec)	DSR	126168.2
	DSR with Malicious Nodes	67255.22545
	DSR with Trust Based Mechanism	139293.2

It can be seen from Table VIII that since many of the packets did not reach the destination due to malicious nodes, the number of hops to the destination increases leading to increased end to end delay. The proposed trust based system mitigates this issue by avoiding malicious nodes and in the process the average number of hops increases by 4.15 % compared to DSR network without any malicious nodes. Similarly, it can be seen that end to end delay increases by 220% when malicious nodes are present in the network. The proposed trust based model decreases this with the end to end delay increasing by 1.37% compared to DSR model without malicious node. The increase in the end to end delay is due to the control packet overheads in finding the trusted nodes. With the packet drop and end to end delay decreasing, the throughput of the system of the proposed system is in par with DSR based model.

4. Conclusion

In this paper, the behavior of DSR protocol with and without the black hole attack is investigated. As ad hoc networks are formed by cooperative dynamic nodes, i.e. nodes joining and leaving the network any time, it is difficult to maintain security mechanisms centrally. In this work, a novel mechanism based on trust is proposed to mitigate black hole attacks. The DSR header is modified to carry an additional payload to measure trust within the network. The proposed scheme mitigates black hole attacks by avoiding the malicious nodes. The proposed model though increases the hop count performs better than DSR by roughly 13% without compromising on security. The end to end delay remains almost the same as compared to DSR even during an attack. The proposed model can be extended to study the behavior of DSR protocol with other types of attacks including wormhole and grey hole attack.

References

[1] S. Corson, J. Macker, (1999) " Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF RFC2501.

[2] L. Zhou, and Z. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24–30. 1999.

[3] Y.Zhang, W. Lee, " Intrusion Detection in Wireless Ad-Hoc Networks", Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Aug 2000.

[4] H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, pp. 70-75, October 2002.

[5] P. Papadimitratos, and Z.J. Haas, "Securing the Internet Routing Infrastructure," IEEE Communications, vol. 10, no. 40, pp. 60-68 October 2002.

[6] Y. C. Hu, A. Perrig, D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks". ACM MOBICOM Wireless Networks, Volume11, pp. 21-38, 2005.

[7] Y. C. Hu, and A. Perrig, "A survey of Secure

Wireless Ad Hoc Routing", IEEE Security and Privacy, special issue on Making Wireless Work. Volume 2, Issue 3, pp. 28-39, 2004.

[8] M. G. Zapata, "Secure ad hoc on-demand distance vector routing", ACM Mobile Computing and Communications Review, Volume 6, Issue 3, pp. 106-107,2002.

[9] N. Griffiths, A. Jhumka, A. Dawson, and R. Myers, " A Simple Trust model for On-Demand Routing in Mobile Ad-hoc Networks", Intelligent Distributed Computing, Systems And Applications Studies in Computational Intelligence, Volume 162, pp.105-114, 2008.

[10] D. Gambetta, "Can We Trust Trust? Trust: Making and Breaking Cooperative Relations", electronic edition, Department of Sociology, University of Oxford, chapter 13, pp. 213-237, 2000.

[11] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," Proc. IEEE Symposium on Security and Privacy, pp. 164 – 173, May 1996.

[12] L. Eschenauer, V. D. Gligor, and J. Baras, "On Trust Establishment in Mobile Ad Hoc Networks," Proc. 10th Int'l Security Protocols Workshop, Cambridge, vol. 2845, pp. 47-66, Apr 2002.

[13] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", in Ad Hoc Networking, Chapter 5, Addison-Wesley, pp. 139-172, 2001.

[14] Y. C. Hu, A. Perrig, and D. B. Johnson, " Packet Leashes: A Defense against Wormhole attacks in Wireless Ad Hoc Networks In Proceedings of the IEEE 22nd Annual Joint Conference of the IEEE Computer and Communications", pp. 1976-1986, Apr 2003.

[15] S.Capkun, L.Buttyan, and J. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks", ACM workshop on security of ad hoc and sensor networks (SASN), pp. 1–12, October 2003.

[16] W. Wang, B.Bhargava, Y,Lu, and X.Wu, "Defending against wormhole attacks in mobile ad hoc networks", Vol 6, Issue 4, pp. 483-503,2006.

[17] J. Zhen, S. Srinivas, "Preventing replay attacks for secure routing in ad hoc networks", ADHOC-NOW 2003, Lecture Notes in Computer Science, vol. 2865, pp. 140–50, 2003.

[18] R. Poovendran and L. Lazos, "A Graph Theoretic Framework for Preventing the Wormhole Attack in Wireless Ad Hoc Networks", Journal of Wireless Networks, Volume 13, Issue 1, pp. 27-59, 2007.

[19] E. A. Panaousis, L. Nazaryan, C. Politis, "Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications In Proceedings of the 5th International ICST Mobile Multimedia Communications Conference", 2009.

[20] B. Vaidya, S. S. Yeo, D. Y. Choi, and S. J. Han, "Robust and Secure Routing Scheme for Wireless Multihop Network", Springer Personal and Ubiquitous Computing, 13: pp. 457-469, 2009.

1/29/2013