Performance Analysis of AODV and DSR Routing Protocols of MANET Under Wormhole Attack and a Suggested Trust Based Routing Algorithm for DSR

Shripriya Tripathi

October 9, 2019

PERFORMANCE ANALYSIS OF AODV AND DSR ROUTING PROTOCOLS OF MANET UNDER WORMHOLE ATTACK AND A SUGGESTED TRUST BASED ROUTING ALGORITHM FOR DSR

Abstract**—**Mobile adhoc network (MANET) is a network where the nodes can move freely in the network, self-assemble themselves and can interact with each other without any help from any centralized authority or fixed infrastructure. Due to its' highly dynamic and self-configuring nature MANET is susceptible various types of attacks like blackhole attack, wormhole attack, rushing attack, spoofing attack etc. Here, in this paper the effect of wormhole attack on MANET's two main reactive routing protocols namely Ad-hoc On Demand Distance Vector (AODV) and Dynamic source Routing (DSR) is analyzed and compared by increasing the number wormhole tunnels in MANET. Here, we will see that DSR is greatly affected by this attack, so, as a solution a trust based routing algorithm for DSR is proposed to prevent the caching of attacked routes.

Index Terms**— MANET, AODV, DSR, wormhole attack, trust**

I. Introduction

Mobile ad-hoc network (MANET) is created by some mobile nodes that communicate with each other without any help of any centralized management/coordination/administration or fixed/stand-alone infrastructure. Main features of MANET are: (a) Dynamic topology (b) limited energy resource (c) energy constrained operations (d) limited bandwidth links. MANET has got many applications in various areas like battle-field communications/application, law-enforcement, virtual classrooms, emergency relief cases, public meeting etc. Every node in MANET behaves as a router and make use of multi-hop communication in order to route packets in a network where the topology changes so frequently. The routing protocols in MANET are designed in such a way that they can easily deal with frequently changing network topology which causes many security problems in ad-hoc network when

compared to wired network. As when routing protocols were designed security aspects were not taken into account. Due to this malicious nodes can affect the routing of packets properly in network by different ways like altering current routing information, spoofing, and fabrication of correct information. In wormhole attack two or more malicious nodes collaborate with each other and form a tunnel in the network through which the attackers can pass the packets and disrupt the routing information in the network by providing a shortest route in the network. This paper is organized as follows. Firstly a short overview of MANET routing protocols is discussed and then the wormhole attack has been described. After that the effect of wormhole attack on AODV and DSR routing protocols is analyzed by taking into account various network performance metrics like throughput, average jitter and average end to end delay by varying the number of wormhole tunnels in the network. After that a trust based routing algorithm for DSR is being discussed to prevent DSR from storing attacked routes

A. MANET Routing Protocols

The main goal of routing in MANET is to establish a path with minimum number of hops between source and destination. Routing protocols in MANET can be classified into the following categories: proactive routing protocols, reactive routing protocols and hybrid routing protocols. The network incorporating proactive routing protocol, nodes always search for routing information inside the network and when any route is needed, the route is already there. Each node contains one or more than one table which represents the whole topology of the network. These tables are kept up-to-date whenever there is any topology change (e.g., OLSR).

The second category is reactive routing protocols in which the route is found only when there is a need of route from source to destination. Since nodes don't have any overhead of keeping routing tables so there is a significant amount of route discovery delay in network.

Ad-hoc On-Demand Distance Vector (AODV) is an advancement of Destination Sequence Distance Vector (DSDV) routing algorithm. Route to the destination is found only when required. Routing in AODV is done in two phases: Route Discovery and Route Maintenance. In route discovery phase RREQ packet is broadcasted in network. Every node in the network has a routing table to route packets at a particular destination. Route discovery is done by broadcasting the RREQ packets to the neighbors and then getting a unicyclist RREP packet to the source as the acknowledgement. Whenever there is any route break in the active path occurs, the neighboring node of the broken link node starts broadcasting RERR packet to it's neighboring nodes.

Dynamic Source Routing (DSR) depends on source routing and route caching. Source routing means the sender is having the information of complete route in a hop by hop manner and the packets while traveling in the network carry this information with them. Every node in the network has a route cache which is used to provide routing information to the destination. Before transmitting any packet the sender checks it's route cache as to know whether the route is already available. If there is a route to the destination ,the packet will follow that specified path but if there is no path available then the route discovery phase starts like that of AODV. In the same way if there is any link break in the network then this information is broadcasted in the network by the neighboring nodes.

B. WORMHOLE ATTACK

This attack can be launched with the collaboration of two or more attackers which form a tunnel in the network. The attacker at one end receives the packets and tunnel these packets to another attacker present at the other end of the tunnel. The attacker need not have any knowledge of cryptographic keys. By this attack the attackers can disrupt the normal flow of packets in the network. This tunnel provides a shortest path to the destination as compared to the multi-hop route. In this way the attackers get advantage of transmitting the packets through them and hence can give birth to many attacks like blackhole and greyhole attacks.

II. RELATED WORK

Rutvij H. Jhaveri et al.[4] said that AODV is prone to attacks like modification of sequence numbers, modification of hop counts, source route tunneling, spoofing and fabrication of error messages. Even though modification of source-routes by cache poisoning is not possible in AODV while DSR is vulnerable to it. Wormhole attack is an actual threat for AODV routing protocol. G.K.Singh et al [2] concluded that in Random waypoint mobility model with CBR traffic sources, AODV performs better than the other protocol DSR when node density is kept low. When node density is kept high, AODV protocol's performance is better in low Traffic load. But when node density and traffic load is high, DSR performs better than AODV. AODV always give low jitter irrespective of traffic load and node density also AODV is gives better performance then DSR for Average End to End delay. Average End to end delay for DSR increases fastly when traffic load is increased and hence, it is not affected by the node density. S.Tiwari et al.[1] said that for small number of nodes

Performance of AODV is better. As node increases, for AODV protocol, routing overhead in the network increase in large amount. Hence performance for AODV decreases with large network. Thus for constant length of wormhole link there is no effect on the functioning, because the wormhole link behaves as high speed directional link for routing messages. As the length of colluding link increases, the performance for DSR degrades compared to AODV. Hence, the effect of wormhole attack is much severe for DSR than AODV protocol. Su Mon Bo,Hannon Xiao [3]compared three routing protocols, DSDV,

DSR, and AODV under security attack. Network performance is evaluated in terms of normalized throughput, average packet delay, routing overhead and normalized routing load, when a percentage of nodes behave selfishly. Although the performance of all three routing protocols degrades, DSDV is the most robust routing protocol under security attack. This reveals that a proactive routing protocol has the potential of excluding misbehaving nodes in advance and reducing the impact of security attacks. Shahjahan Ali et al.[6] When comparing the performances of AODV and DSR under wormhole attack, a general conclusion is that, under the wormhole nodes, DSR outperforms as compare to AODV because AODV is more vulnerable to attacks. This is because to the fact that redundant routes in DSR provide alternate paths for data delivery. Therefore, techniques that use trust for discovering and detection of wormhole attack should be used. It should keep in mind that some solutions may not work well in the presence of more than one malicious node, while some require special hardware and some solutions are very expensive. Poonam, K.Garg,M.Mishra [19] have presented a trust based routing algorithm for DSR. By calculating the amount for a given path, the routing is done according to it. Asad Amir Pirzada et al. [11] proposed a novel and pragmatic scheme for establishing and sustaining trustworthy routes in the network. Each node maintains trust levels for its immediate neighbors based upon their current actions. Nodes also share these trust levels (reputations) to get ancillary information about other nodes in the network.Guo Wei, Xiong Zhongwei, Li Zhitang [12] concluded that the trust value in routing protocol as the records linked with the behaviors of links to deliver message to the intended next node reliably, timely, and integrally. After using a trust graph theoretic model to evaluate dynamically, to maintain trust relationships, and to make trust-based routing decisions, _ve trust-based theoretic strategies have been presented for routing selection. N.Bhalaji, Dr.A.Shanmugam [13] analyzed the blackhole attack which is one of the possible and commonest attacks in adhoc networks. In the given attack, the malicious nodes advertise themselves to have the shortest path to the destination from source. In this approach they have classified nodes in to 3 categories based on their behavior. The extents of association between the nodes were used for the route selection. Zhaoyu Liu, AnthonyW. Joy, Robert A. Thompson [14] introduced a trust model for mobile ad hoc networks. Initially each node is assigned a trust level.Syed S. Rizvi, Saroj Poudyal, Varsha Edla, and Ravi[15] Nepal presented a Reputation-Trust (RT) system that can be used to stabilize the performance of the network for the working nodes when the malicious nodes are present, it intentionally do not route and forward packets send by others correctly. Seungtak Oh, Chilgee Lee, and Hyunseung Choo[16] proposed a comprehensive mechanism for discovering the most secure and shortest paths.JIE WU [17] generated two node-disjoint paths during the query phase of the discovery of route process by controlling the way the query packet is flooded. Several optimization options are also considered. Simulation is done to find out the success rate of finding node-disjoint paths. Cuirong Wang, Xiaozong Yang, and Yuan Gao [18] said that the trust level is used as knowledge for routing. The security rather than shortest path is the primary concern of the method.

III. Simulation Results and Discussion

The simulations were performed using EXata/Cyber 1.2 simulator. In this scenario the source destination pairs are spread randomly over the network. The model parameters that have been used in the following experiments are summarized here.

PARAMETERS	VALUES
Topological Area	2500*2500 sq. m.
Channel Type	Wireless Channel
Radio-propagation Model	Two Ray Ground
Antenna Type	Omni antenna
Interface Queue Type	Drop Tail/PriQueue
MAC Type	802.11,Wormhole
Routing Protocols	AODV, DSR
Node Density	20,40,60,80,100,120,140,160,180,200
Mobility Model	Random Waypoint
Number of tunnels	2, 3, 4
CBR Packet Size	512 Bytes
Simulation time	300 s

Here, the performance of two routing protocols namely AODV and DSR have been compared under different number of wormhole tunnels in the network. The network performance metrics taken are throughput, average end-to-end delay and average jitter which change their values with respect to varying number of nodes.

A. *Average End to End Delay*

The time taken by any packet to go from source to destination is called the end to end delay. The average of these end to end delays of all the received packets is called average end to end delay.

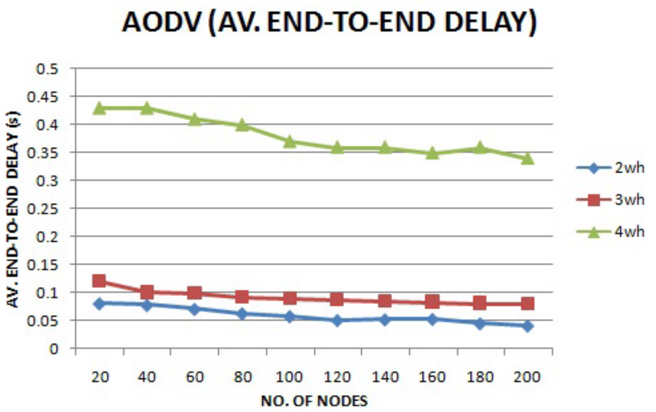

Fig 1: Average end to end delay Vs no. of nodes in AODV

The av. end-to-end delay of AODV is higher in case of four tunnels and afterwards it starts decreasing for three and then two tunnels in the network. The value of average end-to-end delay is decreasing with increase in number of nodes.

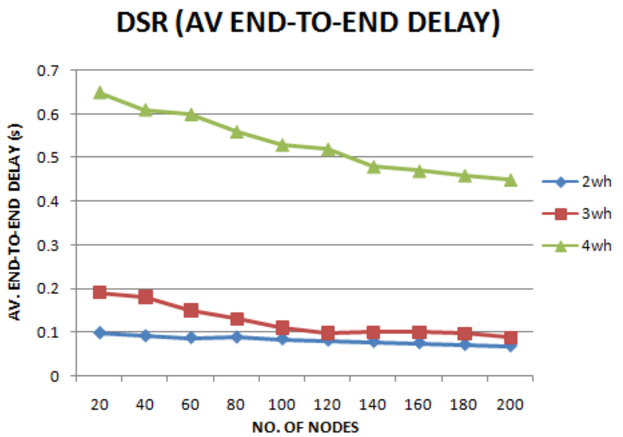

Fig 2: Average end to end delay Vs no. of nodes in DSR

The av. end-to-end delay of DSR is highest in case of four tunnels and it has lesser values for three and then two tunnels in the network. The value of average end-to-end delay is decreasing with increase in number of nodes.

B. THROUGHPUT

The throughput of a receiver is defined as the ratio of the number of bits received over the time difference between the first and the last received packets.

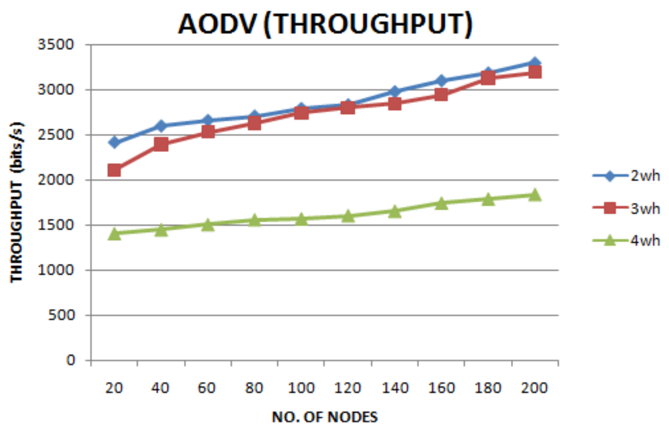

Fig 3: Throughput Vs no. of nodes in AODV

The throughput is highest in two tunnels and then it's value starts decreasing with increase in no. of tunnels. The value of throughput is increasing with increase in number of nodes.

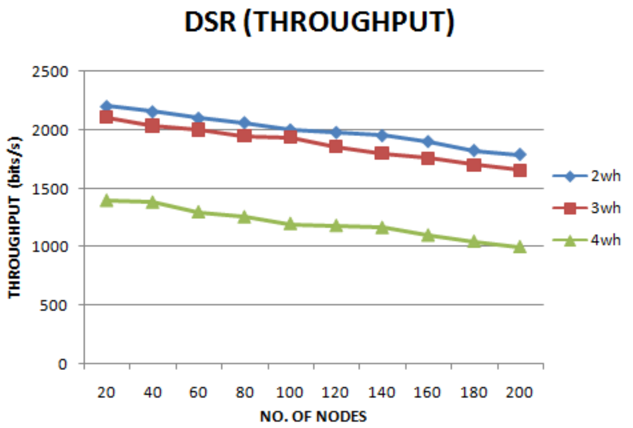

Fig 4: Throughput Vs no. of nodes in DSR

In DSR, the throughput is highest in case of two tunnels and then it's value show a decrease with increase in number of tunnels. Overall, the throughput is increasing with increase in no. of nodes.

C. AVERAGE JITTER

The jitter of the packet is defined as the deviation of the difference in packet spacing at the receiver compared to the sender, for a pair of packets.

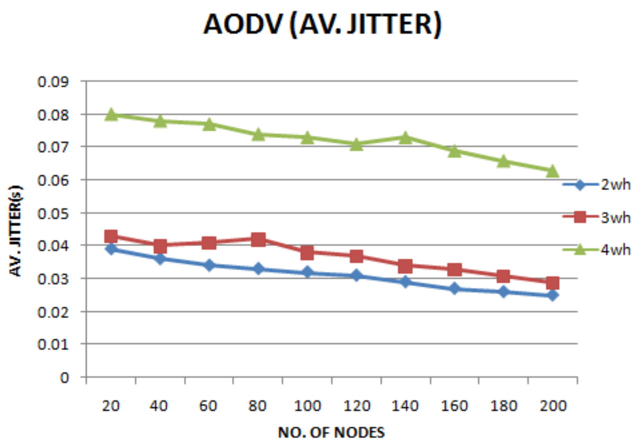

Fig 5: Average jitter Vs no. of nodes in AODV

The average jitter is increased with increase in number of tunnels. Overall, it's value is decreasing if number of nodes in the network are increased.

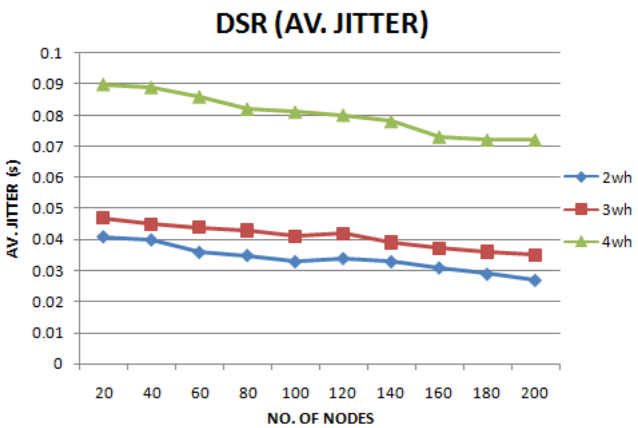

Fig 6: Average Jitter Vs No. of nodes in DSR

The values of avg. jitter is highest in case of four tunnels. Afterwards, it shows a decrease if number of tunnels in the network are increased. The value of average jitter is decreased if number of nodes are increased in the network.

A PROPOSED TRUST BASED ROUTING ALGORITHM FOR DSR

As it can be seen from the graphs that DSR suffers most when there is wormhole attack in the network as it caches the attacked route in the route cache. So for that a trust based routing algorithm is suggested here. This algorithm will help DSR in not caching the attacked routes but the trusted routes. The assumptions taken in this algorithm are as follows:

1. Initial value of forward trust and reverse trust is 0
2. Each node creates a trust table and stores the trust values of it's one hop neighbors.

A. *Algorithm : Routing of data packets in DSR via trusted paths*

```
if (routing cache is empty) then
  run route discovery algorithm
  source node S broadcast RREQ packet
  intermediate node A received the RREQ message in the form {SA, DA, Seqnum}
  if (intermediate node is not destination) then
    Re-broadcast the RREQ message with some modification as
    RREQ now becomes {SA,DA, Seqnum} U {forward trust}
    {forward trust} = {forward trust} U  T(AB)
    where T(AB) is the trust assigned by node A for node B
  else(intermediate node is destination)
      It returns route reply packet(RREP) modified as below
      RREP = {SA, DA, seqnum} U {forward trust} U {reverse trust}
    reverse trust = reverse trust U T(BA)
      where T(BA) is the trust assigned by node B for node A
  end if
  When intermediate node receives the RREP packet
  it unicasts it to the next node present in the route cache, back to sender
  Sender calculates the geometric mean of the forward trust and reverse trust
  for each route separately
  if (forward trust and reverse trust are same) then calculate
      path - $trust_i$ = {(forward trust + reverse trust) / 2} X  $w_i$
      where $w_i = 1/x_i$
    and $x_i$ is the number of nodes in the $path_i$
  else (forward trust and reverse trust are not same) calculate
    GM(forward trust, reverse trust) X $w_i$
  end if
  if (a path chosen for routing proves to be trustworthy) then
    the trust value of all the nodes in that path will be increased
    according to the given formula $T_u(E, T_e) = (1 - c) X E + (c X T_e)$
  else (a path chosen for routing does not prove to be trustworthy)
  the trust value of all the nodes in that path will be decreased
  according to the given formula $T_u(E, Te) = (1 - c) X E - (c X  T_e)$
  where $T_u$ is the upgraded trust
  $T_e$ is existing trust and X is multiply
  E is the experience value
  C is the constant to express the change in trust
  end if
end if
```

B. Testing the performance of the proposed algorithm

Here, some test cases will be provided to examine the performance of the algorithm. This algorithm is also compared with the algorithm given in the paper "Trust based Multipath DSR Protocol".

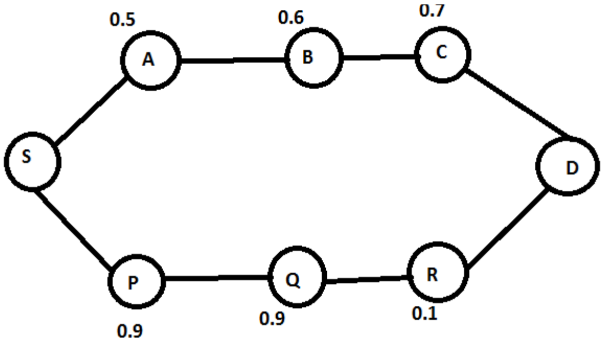

Fig 7: Ad-hoc Network

(a) $path_1$ consists of nodes namely S-A-B-C-D and path2 consists of nodes S-P-Q-R-D.

(b) forward trust = forward trust + T(AS) + T(BA) + T(CB) + T(DC)

(c) reverse trust = reverse trust + T(CD) + T(BC) + T(AB) + T(SA)

(d) path - $trust_i$ = {(forward trust + reverse trust) / 2} X (1/5)

(e) So, path - $trust_1$ = {((0.5 + 0.6 + 0.7) + (0.5 + 0.6 + 0.7)) / 2} X (1/5) = 0.36

(f) path - $trust_2$ = {((0.9 + 0.9 + 0.1) + (0.9 + 0.9 + 0.1))/ 2} X (1/5) = 0.38

According to [4] path chosen is S-P-Q-R-D. This paper has following drawbacks:

- It has taken just the total sum of the trusts and not considered the vulnerability of the weakest link.
- As security is the just the strength of the weakest link, any malicious node with lower trust will get a route through it if it comes in the path of higher trust valued Nodes.

The path chosen by the proposed Algorithm is S-A-B-C-D. As it considers the geometric mean of all the trust values. If any trust value goes lower then there will be lesser chances of choosing it.

- path - $trust_i$ = {GM(forward trust + GM(reverse trust)) / 2} X (1/5)
- path - $trust_1$ = {(0.594 + 0.594) / 2} X (1/5) =0.1188
- path - $trust_2$ = {(0.4326 + 0.4326) /2} X 1/5 = 0.086

Since, path - $trust_1$ > path - $trust_2$; $path_1$ will be chosen for routing.

C. Conclusion

From the given graphs it can be analyzed that the performance of AODV is better in case of average end-to-end delay and throughput. Since DSR maintains existing routes or secondary routes in their cache which increases the probability that an attack route is present in the cached route which increases the impact of wormhole attack on DSR.As far as average end-to-end delay is concerned DSR outperforms AODV due to availability of complete routes in DSR cache and large overhead in case of AODV. Once the number of wormhole tunnels are increased in the network, the effect of attack becomes severe but the impact of attack can be diminished in the network if we increase the number of nodes the network. In the proposed algorithm we have considered the geometric mean of the trusts in both the directions. So, if any node's trust goes lower, it loses the chance of being chosen in the network. .

References

[1] Djenouri, D.; Khelladi, L.; Badache, N., \A survey of security issues in mobile ad hoc and sensor networks," Communications Surveys Tutorials, IEEE , vol.7, no.4, pp.2,28, Fourth Quarter 2005

[2] Govindan, K.; Mohapatra, P., "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey," Communications Surveys Tutorials, IEEE , vol.14, no.2, pp.279,298, Second Quarter 2012

[3] Mon Bo Su, Xiao Hannan, A. Adereti, J. A. Malcolm, B. Christianson, "A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack", Proc. of Third International Symposium on Information Assurance and Security, 'IAS 2007', pp. 50-55, Aug. 2007.

[4] Rutvij H. Jhaveri, Narendra M. Patel, "A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks", Wireless Networks, vol. 21, pp. 2781, 2015.

[5] V.K.Taksande& Dr. K. D. Kulat "Performance Comparison of DSDV, DSR, AODV Protocol with IEEE 802.11 MAC for Chain Topology for Mobile Ad-hoc network using NS-2 " IJCA Special Issue on "2nd National Conference- Computing, Communication and Sensor Network"CCSN, 2011

[6] Shahjahan Ali and Abdul Wahid "Performance Evaluation of Routing Protocols under Wormhole Attack in Mobile Ad-Hoc Network"

[7] Erik Nordstr¨om, Per Gunningberg, Christian Rohner, and Oskar Wibling. "Evaluating wireless multi-hop networks using a combination of simulation, emulation, and real world experiments". In Proceedings of MobiEval'07, June 2007

[8] JosipLorincz, NenadUkic, DinkoBegsic, "Throughput Comparision of AODV-UU and DSR-UU Protocol Implementation in Multi-hop Static Environments". 9th International Conference on TelecommunicationsConTEL 2007

[9] Pissinou, N., Ghosh, T., Makki, K.: Collaborative Trust-Based Secure Routing in Multihop Ad Hoc Networks. In: Mitrou, N.M., Kontovasilis, K., Rouskas, G.N., Iliadis, I., Merakos, L. (eds.) NETWORKING 2004. LNCS, vol. 3042, pp. 1446–1451. Springer, Heidelberg (2004)

[10] Capkun, S., Buttyan, L., Hubaux, J.-P.: Self-Organized Public-Key Management for Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing 2(1), 52–64 (2003)

[11] Amir Pirzada, Asad & Datta, Amitava & Mcdonald, Chris. (2006). Incorporating trust and reputation in the DSR protocol for dependable routing. Computer Communications. 29. 2806-2821. 10.1016/j.comcom.2005.10.032.

[12] Wei, Guo & Zhongwei, Xiong & Zhitang, Li. (2005). Dynamic trust evaluation based routing model for ad hoc networks. 727 - 730. 10.1109/WCNM.2005.1544157.

[13] Natarajan, Bhalaji & Shanmugam, A. (2009). Association between nodes to combat blackhole attack in DSR based MANET. 1 - 5. 10.1109/WOCN.2009.5010579

[14] Zhaoyu Liu, A. W. Joy and R. A. Thompson, "A dynamic trust model for mobile ad hoc networks," Proceedings. 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2004. FTDCS 2004., Suzhou, China, 2004, pp. 80-85. doi: 10.1109/FTDCS.2004.1316597

[15] Reddy, Vijender & Negi, Atul & Venkataraman, S & Raghu Venkataraman, V. (2019). A Similarity based Trust Model to Mitigate Badmouthing Attacks in Internet of Things (IoT). 278-282. 10.1109/WF-IoT.2019.8767170.

[16] Oh, Seungtak & Lee, Chilgee & Choo, Hyunseung. (2006). Collaborative Trust-Based Shortest Secure Path Discovery in Mobile Ad Hoc Networks. 3992. 1089-1096. 10.1007/11758525_145.

[17] Shrivastava, Neha & Motwani, Anand. (2014). A Modification to DSR using Multipath Technique. International Journal of Computer Applications. 92. 10.5120/16053-5236.

[18] Jian Wang , Yiwen Xu , Jindong Zhang , Yanheng Liu , Weiwen Deng, SAV4AV: securing authentication and verification for ad hoc vehicles, Security and Communication Networks, v.8 n.4, p.626-636, March 2015 [doi>10.1002/sec.1011]

[19] Bansal, Mohit & DEVI, MUNESH & CHADRA SATI, DAYAL & KANT, RAVI. (2017). Design and Analysis of Trust Based Modified DSR Routing Protocol in Mobile Ad-Hoc Networks.