RESEARCH ARTICLE OPEN ACCESS

Trust Based Dynamic Source Routing Protocol by Exclusion of Black-Hole Attack for MANETs

K. Thamizhmaran [1], K. Prabu [2]
Department of ECE [1], Annamalai University, Annamalai Nagar
PG & Research Department of CS [2], Sudharsan College of Arts & Science, Pudukkottai
Tamil Nadu -India

ABSTRACT

Recent research develops scheme that permits the users to get right of entry to facts and techniques anywhere no matter their geographic location. Mobile ad-hoc community (MANET) is the giant designs amongst numerous wireless conversation technologies wherein us all of the nodes are mobile and which may be related to dynamically the usage of wi-fi hyperlink within the random manner. Maximum of the proposed protocols expect that each one nodes inside the network are cooperative, and where it does no longer deal with any security issues. Black hole assault is a commonplace safety issue encountered in mobile ad-hoc community routing protocol. In this technical research paper a trust value for each node has been obtained depending upon the packet forwarding ability of the node. A rank is generated primarily based on this consider price. Inside the course discovery step of the Dynamic source Routing (DSR) protocol a direction is chosen in this type of manner that more depended on nodes are worried also a node may be without which isn't always relied on from the course for that reason the packet is transferred via a more depended on path instead of the shortest route consequences of simulation via the use of NS2 software program that indicates higher packet deliver ratio and decrease packet drops presenting greater appropriate communication.

Keywords:- MANETS, Security, Black-hole Attack, Packet Delivery Ratio, Packet Drop.

I. INTRODUCTION

Because MANET is fixed infrastructure much less, it suffers from unique network assaults typically kinds of assaults are there namely inner assault and external attack show in discern. In inner assault the attacker silently listening to the communication medium to wager what conversation goes on in that channel. It does now not modify any technique inside the message packet. As a result the attacker may additionally come to know the name of the game records that are being sending via the air medium in the community on the other hand in lively assault the attacker can break, loss, and exchange the original facts. Black hollow attack is one of the most vital protection assaults which might be responsible for packet losing those results in packet loss. It gets the RREQ from its neighbour node and also send back path replay reaction message to the path request sender as a consequence according to the constant DSR routing protocol a maximize series range is likewise allotted to this node as a consequence this actively node takes part in route discovery process of DSR routing for that reason the direction is likewise set up via this node. The sender and the target appear that the actual course is mounted, in order that they start to send the facts however then these misbehaviour nodes deny forwarding the packet. This node swallows the packet thus the packets are loosed right here rather than forwarding it to its original goal. This corresponding node is known as black hole node and this impact is the black hole assault glaringly this black hollow assault degrades the great of carrier in terms of packet loss. There are numerous designs evolved by way of the researchers to handle this difficulty consider based routing is one of the extensively ordinary strategies. The relaxation of the paper is organized as follows.

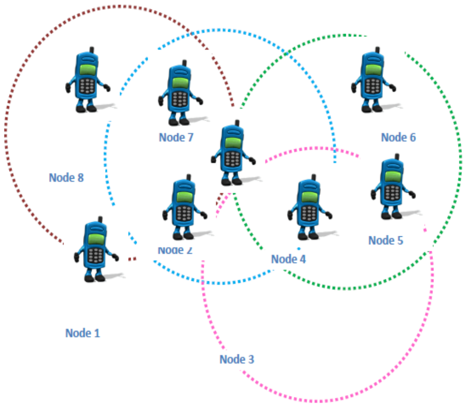

Figure 1 Mobile ad-hoc network

II. RELATED WORK

Dynamic source routing in ad-hoc wireless networks was done by Johnson and Maltz (1996). Optimized link state routing protocol for ad-hoc networks was done by Jacquet, et al (2001). Mobile ad-hoc networking: imperatives and challenges, Ad-hoc networks were done by Chlamtac, et al (2003). Performance analysis of reactive shortest path and multipath routing mechanism with load balance was done by Pham and Perreau (2003). Minimum energy disjoint path routing in wireless ad-hoc networks was done by Srinivas and Modiano (2003). Multipath routing in mobile ad-hoc networks: issues and challenges were done by Mueller, et al (2004). Q-OLSR multi-path routing for mobile ad-hoc networks based on multiple metrics: bandwidth and delay was done by Badis, et al (2004). Distributed construction of connected dominating set in wireless ad-hoc networks was done by Alzoubi and Frieder (2004). The research and simulation of multipath-OLSR for mobile ad-hoc network was done by Kun, et al (2005). Improving the perform ability of data transfer in mobile ad-hoc networks was done by Gregori and Maselli (2005). A novel routing protocol for ad-hoc sensor networks uses multiple disjoint paths was done by Zhou, et al (2005). Improving security and performance of an ad-hoc network through a multipath routing strategy was done by Aiache, et al “Tavernier (2008). Survey of multipath routing protocols for mobile ad-hoc networks was done by Tarique, et al (2009). Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MANET was done by Mangrulkar, et al (2010). Mitigation of topology control attacks in OLSR networks was done by Cervera, et al (2010). Security Issues in the Optimized Link State Routing Protocol version 2 (OLSRv2) was done by Clausen and Herberg (2010). Multipath optimized link state routing for mobile ad-hoc networks was done by Yi, et al (2011). Mitigation of flooding disruption attacks in HOLSR networks was done by Cervera, et al (2011). Supported reliable multipath multicast routing in MANETs was done by Biradar and Neighbor (2012). Multipath routing in spatial wireless ad-hoc networks was done by Guo, et al (2012). A novel acknowledgment-based approach against collude attacks in MANET was done by Chen and Ku (2012).

III. PROPOSED WORK

Inside the implementation approach a new parameter known as ‘trust price’ is degree in opposition to all of the intermediate nodes. These accept as true with cost is degree depending upon the capable of forward packets and the RREQ forwarding capability of a node. To obtain this ability the number of packets amassed and the wide variety of packet transmit is counted special weight elements W1 and W2 are brought. W1 is the ratio of number of packets transmits from a node to the quantity of packets accumulated to that node. A maximum price of this ratio shows that, the node has an extra capacity to forward the packets consequently the opportunity of drop of packets is decrease. The most price of W1 may be 1, where all the accrued packets are forwarded and no packet is loosed. From this fee we also can determine the untreated nodes within the network the opposite weight vector W2 is the ratio of wide variety of RREQ amassed to wide variety of RREP transmits. This ratio founds the nodes which constantly accumulate the RREQ from its neighbour nodes however never respond to that request via transmitting the respond. Then this weight aspect is elevated to get the trust cost of that node right here we check if any nodes have the W1 value greater than the edge price. If it can transmit a packet then they accept as true with price is maximized otherwise its miles minimized. This trust cost is stored in the routing desk of that node and within the direction discovery step of DSR routing protocol the direction is set up in keeping with that agree with fee in preference to the shortest course hence the less depended on node can be averted all through the route establishment in DSR routing protocol.

Step 1

I. Count the number of packet collected at each active node.

II. Count the number of packet transmits by each active node.

III. Count the number of RREQ collected at each active node.

IV. Count the number of RREP transmits by each active node.

Step 2

Parameter	values
Routing protocol	T-DSR
Application traffic	CBR
Transmission range	500m
Packet size	512 bytes
Transmission rate	4 packets/sec
Number of nodes	100
Area	650*650m
Propagation model	Free space
Attack types	Block hole
Movement model	Random waypoint

$$\text{Calculate the threshold value (W1)} = \frac{\text{Number of packet collected}}{\text{Number of packet transmit}}$$

$$\text{Calculate the weight factor (W2)} = \frac{\text{Number of RREP transmit}}{\text{Number of RREQ collected}}$$

Step 3

Increase the packet trust value when threshold value is greater than the threshold value. Otherwise decrease the packet trust value.

Step 4

Calculate Trust Value = W1 * W2 * packet trust

Step 5

Insert Trust value into routing table.

Step 6

Route in establishment according to routing table. Rest of the part is similar to the traditional DSR routing Protocol.

3.1. SIMULATION ENVIRONMENT

The community Simulator (NS2) software program is used to test the advanced approach. NS2 is an extensible, modular, aspect primarily based C++ simulation library and situation, basically for constructing community simulators. Our simulation results with different research works, we adopted the default state of affairs settings in NS 2.34. The most hops allowed in this configuration putting are four. The bodily and MAC layer are each protected in the air medium extension of NS2. The shifting pace of mobile node is limited to 20 m/s and a pause time of 1000 s.

In NS 2.34, the default configuration specifies 50 nodes in a flat area with a length of 650× 650m consumer Datagram Protocol site visitors with steady bit charge is applied with a packet size of 512 B. For every model, we ran each active network framework three moments and analysis the average overall performance to be able to evaluation and examine the results of our evolved scheme, we keep to adopt the following overall performance metrics.

Table 1 Simulation Parameters:

IV. RESULTS AND DISCUSSION

In this implemented work, the minimum forward capacity nodes are provided the ability to loss packets. This way, weakest nodes simply loss message and acknowledgement the packets that they receive and send back to secondary forward capacity node to reduce loss packets to their previous nodes whenever necessary. This is a common method for degrade network performance while still maintaining their reputation. The developed approach T-DSR is designed to tackle weaknesses oldest DSR trust based scheme. To evaluate the performance we apply the above scheme / design at various threshold values. The threshold value indicates the ability to forward packets. An absolute value 0.9 means that the node is thinker as trusted when it can forward communication at least 80 % of the received packet. The performance of the proposed technique is amazing. The trust value randomly varies from various active nodes to active node depending upon the all other different network parameters. The interesting observation is that the rate of packet loss changes significantly with the change of the trust value. Our technical research simulated following parameters namely PDR, RO, and Throughput.

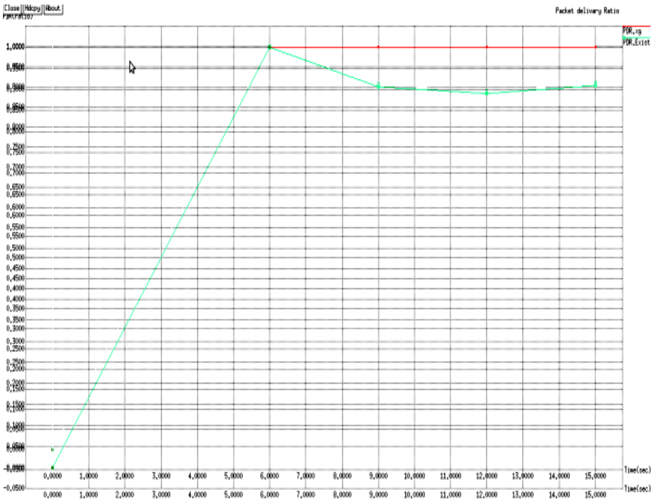

Fig 2 Packet delivery ratio Vs. Malicious node.

In Fig 2 we observe that our developed method T-DSR surpassed DSR performance by above 95% when there are 10 to 100 of nodes in the network.

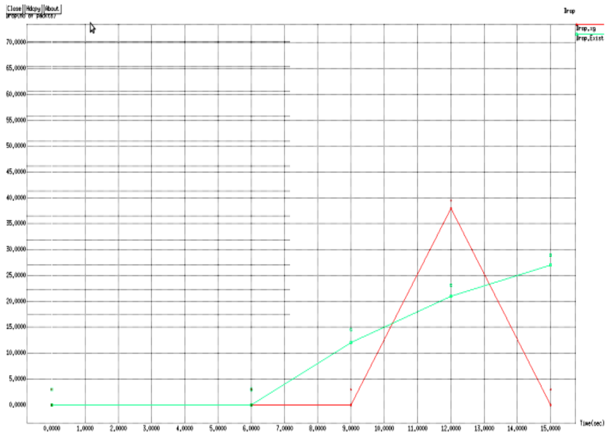

Fig 3 Packet loss Vs. Malicious node

From the fig 3 shows that comparison of the DSR with corresponding dynamic routing algorithm since on along with T-DSR where it shows the packet loss is decrease with increase in the number of malicious nodes.

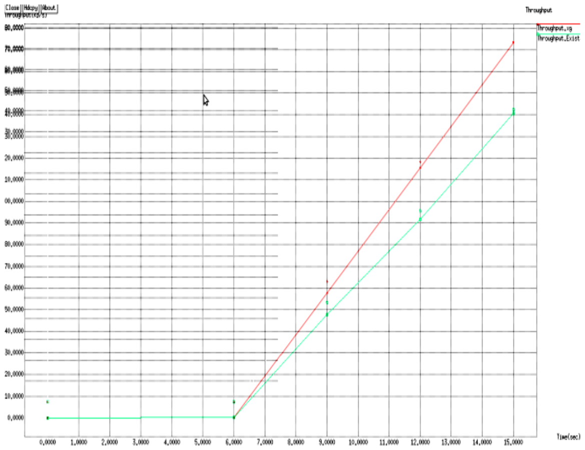

Fig 4 Throughput Vs. Malicious node

In Fig 4 shows that our proposed T-DSR decease the throughput with increasing malicious nodes compare to the existing algorithm.

V. CONCLUSION

Consider management is crucial in infrastructure less network due to the fact here any node can be a part of and any node exits away at any time that is why the ad-hoc community is most sensitive in the direction of specific techniques of attack. Black hollow assault is one in every of them, wherein sure node permits all the facts packets in the same network 0 packets is forwarded closer to its real goal therefore the pleasant of provider of the community turns into an vital difficulty with respect to packet losing here a believe fee is evaluation to every node and this fee may be expanded relying upon the ability to ahead packet and capability to ahead RRRQ. Then this analysis accept as true with value is inserted into the routing table it's far applied on DSR routing protocol. The agree with price is evaluation at each 0.10 2d of c language and the new trust cost is updated. In this situation, the set of trusted nodes is maintained that is dynamic in nature depending upon the believe fee and the edge price the black hole node is diagnosed and it's miles excluded from the route established order operations on the time of course discovery if alternative trusted nodes are to be had it's going to always attempt to establish a path in which greater trusted nodes are concerned right here the path established order is carried out in line with the evaluation consider fee stored within the routing table in preference to the conventional minimum shortest path for that reason as it avoid the low level nodes relied on, the common packet drops of the community is also reduced significantly thus the quality of service of the network is stronger in phrases of packet loss.

REFERENCES

[1] Johnson and Maltz *"Dynamic source routing in ad-hoc wireless networks"*, Springer, pp 153–181, 1996.

[2] Jacquet, et al *"Optimized link state routing protocol for ad-hoc networks"*, IEEE INMIC Pakistan, 2001.

[3] Chlamtac, et al *"Mobile ad-hoc networking: imperatives and challenges, Ad-hoc networks"*, ICSE Vol. 1, No. 1, pp. 13 – 6, 2003.

[4] Pham and Perreau *"Performance analysis of reactive shortest path and multipath routing mechanism with load balance"*, IEEE Societies, Vol. 1, pp. 251–259, 2003.

[5] Srinivas and Modiano *"Minimum energy disjoint path routing in wireless ad-hoc networks"*, ACM, New York, pp. 122–133, 2003.

[6] Mueller, et al *"Multipath routing in mobile ad-hoc networks: issues and challenges"*, Springer, Vol. 29, No. 65, pp. 209–234, 2004.

[7] Badis, et al *"Q-OLSR multi-path routing for mobile ad-hoc networks based on multiple metrics: bandwidth and delay"*, IEEE Conference, Vol. 4, pp. 2181–2184, 2004.

[8] Alzoubi and Frieder *"Distributed construction of connected dominating set in wireless ad-hoc networks"*, Mobile Networks and Applications, Vol. 9, pp. 141–149, 2004.

[9] Kun, et al *"The research and simulation of multipath-OLSR for mobile ad-hoc network"*, IEEE, Vol. 1, pp. 540–543, 2005.

[10] Gregori and Maselli *"Improving the performability of data transfer in mobile ad-hoc networks"*, IEEE, pp. 153–163, 2005.

[11] Zhou, et al *"A novel routing protocol for ad-hoc sensor networks uses multiple disjoint paths"*,

International Conference on Broadband Networks, Boston, Vol. 2, pp. 944–948, 2005.

[12] Aiache, et al *"Tavernier. Improving security and performance of an ad-hoc network through a multipath routing strategy",* JCV, Vol. 4, pp.267–278, 2008.

[13] Tarique, et al *"Survey of multipath routing protocols for mobile ad-hoc networks",* JNCA, Vol.32, No. 6, pp. 1125–1143, 2009.

[14] Mangrulkar, et al *"Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MANET",* IJCA, Vol. 7, No.10, 2010.

[15] Cervera, et al *"Mitigation of topology control attacks in OLSR networks",* CRISIS, Canada, pp. 81–88, 2010.

[16] Clausen and *"Herberg. Security Issues in the Optimized Link State Routing Protocol version 2 (OLSRv2)",* INRIA, 2010.

[17] Yi, et al *"Multipath optimized link state routing for mobile ad-hoc networks",* Ad-Hoc Networks, Vol. 9, No. 1, pp. 28–47, 2011.

[18] Cervera, et al *"Mitigation of flooding disruption attacks in HOLSR networks",* CNSR, Canada, 2011.

[19] Biradar and Neighbor *"supported reliable multipath multicast routing in MANETs",* JNCA, Vol. 35, No. 3, pp. 1074–1085, 2012.

[20] Guo, et al *"Multipath routing in spatial wireless ad-hoc networks",* Computers and Electrical Engineering, Vol. 38, No. 3, pp.473–491, 2012.

[21] Chen and Ku *"A novel acknowledgment-based approach against collude attacks in MANET",* Expert Systems with Applications, Vol. 39, No. 9, pp. 7968–7975, 2012.

[22] Karuturi Satish, K. Ramesh et al., "Intrusion Determent using Dempster-Shafer Theory in MANET Routing", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, no. 1, pp. 37-41, 2015.