A trust based approach for AODV protocol to mitigate black hole attack in MANET

Fidel Thachil[#], K C Shet[#]

[#]*Department of Computer Science and Engineering, National Institute of Technology, Karnataka*

[1]fidelthachil@gmail.com, [2]kcshet@nik.ac.in

***Abstract*— This paper presents a trust based collaborative approach to mitigate black hole nodes in AODV protocol for MANET. In this approach every node monitors neighbouring nodes and calculates trust value on its neighbouring nodes dynamically. If the trust value of a monitored node goes below a predefined threshold, then the monitoring node assume it as malicious and avoids that node from the route path. The experiments reveal that the proposed scheme secures the AODV routing protocol for MANET by mitigating and avoiding black hole nodes.**

***Keywords*-Blackhole; MANET; AODV; Trust**

I. INTRODUCTION

Black hole attack can easily disrupt communication among mobile nodes in Ad-hoc On demand Vector Protocol (AODV) for Mobile Ad-hoc Network (MANET). A black hole node attracts all packets towards it and then drops like a black hole acts in the universe. Such malicious activities are not monitored or mitigated in AODV protocol.

MANET is a collection of independent wireless mobile nodes. MANET doesn't need any predefined infrastructure or a centralised management and so it is very much vulnerable to attacks. Each node is responsible for delivering packets to its neighbour thus the packets are delivered from source to destination through intermediate nodes. Since mobile nodes can move around and join and leave the network at any time, MANET is more vulnerable to attacks. Current solutions which are based on PKI(Public Key Infrastructure), highly depends on a central third party which is responsible for key distribution and applying cryptographic mechanism in the network. PKI is costlier for mobile nodes in terms of computations needed for cryptographic arithmetic. More over the central system itself can act as a malicious node and can remain undetected.

AODV protocol is the most widely used protocol for MANET. All mobile nodes work in cooperation to find a route path from source to destination. Actual data transmission takes place only after the route is established. There are three control messages being used in AODV protocol that are RREP (Route Reply), RREQ (Route Request), and RERR (Route Error). To find a path the source broad cast RREQ packet to the network and all nodes which receives RREQ transmits the same to its neighbours unless it has a fresh enough route to the destination. On receipt of RREQ, a node sends a RREP packet, if it is the destination or if it has a fresh enough route to the destination. On receipt of RREQ message, every node increases hop count by one and on receipt of RREP, intermediate nodes update their route entry with the new data. Whenever a new RREQ, RREP or RERR messages are sent, nodes increase their own sequence number. Higher the sequence number more considered that information.

A. AODV Route Discovery

Fig. 1 shows the illustration of AODV route discovery. Source node S broadcast RREQ packet to establish a route to the destination D. When RREQ packet is received, node A, B and C do one of the following

1) Send a RREP packet back if the node is the destination node or if it has a fresh enough route to the destination.
2) Update the routing table and broadcast the RREQ again.

When the destination receives RREQ, It send back RREP to the source. The RREP message reached at source node through intermediate nodes and these intermediate nodes will update their routing table. The source node accept this RREP if

1) destination sequence number is higher than the one in routing table
2) destination sequence number are equal with the one in routing table, source will check the whether the hop count is lesser with the one in routing table.

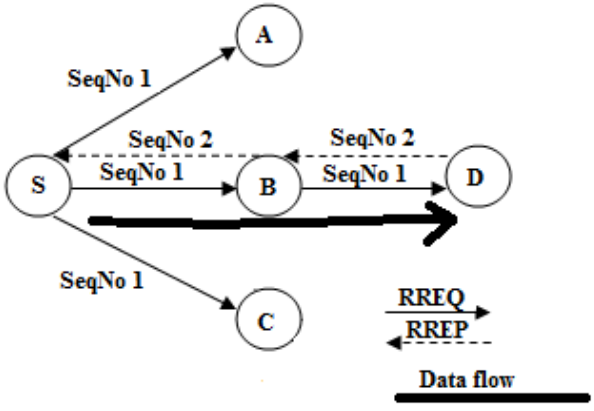

Fig. 1 AODV route discovery

978-0-7695-4817-3/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCS.2012.7

B. *Black hole Attack*

One of the very common attacks in MANET is black hole attack. On receiving a RREQ message, a black hole node immediately send a RREP with highest sequence number without checking for fresh enough route. On receipt of this RREP, route will be established and the source will send all data packets towards the black hole thinking it has fresh enough route to the destination. Black hole will drop all the packets it receives and thus the attack taken place. In case of TCP packets, after a while source will come to know about the malicious node as it will not receive ACK and source will choose a different route. Still that route can also be taken to the same black hole. In case of UDP, the black hole node will never be detected as UDP do not send acknowledgements. The black hole attack is a kind of denial of service attack.

Fig. 2 illustrates black hole attack in AODV protocol. Being malicious, node M pretends, it has a fresh enough route to the destination and will send RREP with highest sequence number with hop count as 1. Upon receiving RREP from node M, source will update its routing table with this RREP as it has the highest sequence number. Thus the route is getting established and data packets will be sent to node M> Being malicious M will drop all the data packets.

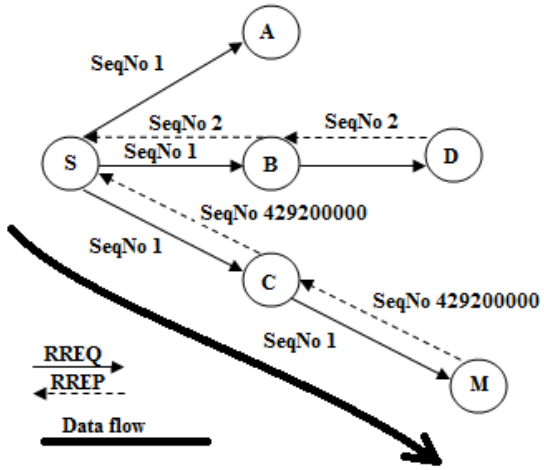

Fig. 2 Illustration of Black hole attack

II. RELATED WORKS

Most of the routing protocols [3-8] proposed for mobile adhoc network for secure route discovery in recent years are based on PKI (Public Key Infrastructure). Here a major concern is to establish a trusted third party. And PKI add up additional processing cost of key distribution, maintenance, encryption and decryption at source and destination etc. Here we propose a trust based approach in AODV protocol to mitigate black hole attack in MANET.

A. Pirzada and C. McDonald [10] proposed a protocol based on network and link layer acknowledgement but can be failed in heavy traffic as the acknowledgement packet may not reach in time and packets like UDP do not provide any acknowledgement at all. They have implemented the solution using DSR protocol.

TAODV [11] is another protocol based on trust which calculates it on the basis of others opinion. This method uses two additional special messages: Trust Request (TREQ) and Trust Reply (TREP) and adds addition 3 new fields to the routing table for calculating the trustworthiness of nodes. TAODV use digital signature which is an additional overhead. Opinion of other nodes cannot be trusted as it can also be from malicious nodes itself. This is an extension of basic AODV protocol.

S. Marti, et al in [12] proposed a method in which they introduced the concept of watchdog [9]. Watch dog listens to neighbouring nodes transmission and based on the information, it calculates a trust value. Based on the values from this watchdog, trust value on the neighbour is being increased or decreased dynamically. The method is implemented only on DSR protocol.

S. Park, et al proposed a solution [8] in which it requires more than one path to destination. Source node waits for RREP packet to arrive from two or more different nodes. This solution fails, if more than one path is not available. And the solution may bring unwanted delays to the network by waiting for multiple RREP packets.

S. Sarafijanovic et al. in [13] proposed an Artificial Immune System (AIS) to detect a misbehaving node in mobile adhoc network. This system requires a protected environment at beginning for learning and then only it can be adapted to the real time environment. The system itself needs another protection at the time of initial stage that is to learn the behaviour of the network.

A Balaji Proposes a trust based approach [1] using AODV protocol. But they do not consider the data packets. Instead they consider only control packets like RREQ, RRER and RREP and network layer acknowledgement. A black hole can even drop data packets by perfectly transmitting control packets. There the system fails by thinking there is no black hole as the control packets are transmitted without any delay or drop.

Satoshi has proposed a method [2] based on the number of RREQ messages sent and RREP messages received. It calculated the average sequence number and try to find out the malicious node, as the malicious node will send RREP messages with extremely higher sequence number. There are chances of getting RREP packet with highest sequence number from a genuine node too.

III. TRUST BASED APPROACH TO MITIGATE BLACK HOLE

Every node keeps a trust value on its neighbours and the trust value is calculated as a ratio of number of packets dropped to the number of packets forwarded. In this method every node listen its neighbours promiscuously. Each node confirms, packets sent to neighbouring nodes are further being forwarded, provided the packet is not destined to that node. Each node monitors the transmission of data packets, not the control packets, so that it can prevent even selective dropping where black hole drops not all packets but only a few selected packets. In order to verify that packets are forwarded by a neighbouring node, a caching mechanism is implemented at every node to collect the packets being forwarded to a neighbour but not destined. If the node cannot tap the same packet from neighbour, when neighbour further forwards the packet, node will assume the neighbour as malicious. To determine if it is the same packet, node verifies the tapped packet with the cached packets. If cached packets are not able to be tapped from its neighbour, then those packets are considered to be dropped. When the trust value of a neighbour goes below a threshold value, then the node will be considered as malicious and will be removed from route and further route selection. Thus avoids the black hole.

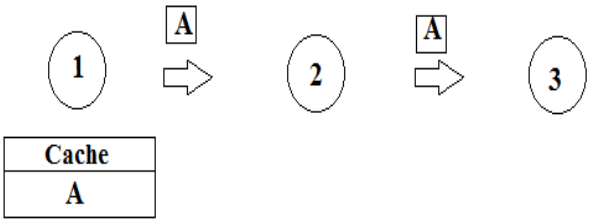

Fig. 3 Tapping of packets in promiscuous mode

A. *Promiscuous mode*

in promiscuous mode, every node taps the packets being forwarded by its neighbouring node so that a node can determine whether a neighbouring node forwards a packet or drops. Each node cache the packets being forwarded and then after taping the neighbouring node, it check for a match in the cache. If it finds a match, then node can assume the packet has been further forwarded by its neighbour, else after a particular amount of time, node will assume that the packet has been dropped by its neighbour and it is suspicious. As shown in Fig.3 node 1 caches the packet A before it send it to node 2. Once node 2 forward the packet A to node 3, node 1 captures the packet in promiscuous mode and verify it with the one in cache and if it matches, node 1 comes to know, the packet A has been forwarded. Thus in a course of time, every node will come to know the behaviour of its neighbouring nodes.

B. *Trust value calculation*

Every node in a network keeps a trust value that represents the trustiness of each of its neighbouring nodes. This trust value gets updated based on the ongoing data transmission with its neighbouring nodes.

Trust value: Trust value of a neighbour is calculated as a ratio of number of packets dropped to the number of packets to be forwarded by that neighbouring node. Trust value is calculated using a simple formula

T = 1-D/F

Where

T = Trust value

D = Number of packets dropped by a node, which are actually to be forwarded.

F = Number of Packets forwarded to that node, which are actually to be further forwarded.

Trust value will be on a range of 0 to 1.

At the beginning all neighbouring nodes are given a range value of 0.5 by each node. The trust value is calculated based on most recent set of packets transmitted to neighbouring nodes. A node keeps a range value on all of its neighbouring nodes. If the trust value is less than threshold, the range value is decremented according to the trust value until it reaches 0.0. If trust value is above the threshold, the range value is incremented until it reaches 1.0. When the range value of a node goes below threshold, it is considered to be malicious. Once a node identified its neighbour as malicious, it broadcast a message to the network with the node id of the malicious one. So that other nodes can exclude the malicious node from their routing table and from establishing route in future.

Every node caches those packets being forwarded to its neighbouring nodes which are not destined to it but to be further forwarded. Then nodes listen to its neighbouring node in promiscuous mode. Whenever the neighbouring node, forwards the packet further, then the listening node captures it and confirm that the cached packet has been forwarded. If the neighbouring nodes are not forwarding packets, then it is considered to be dropped and will be counted to the number of dropped packets. Even though, a node is not malicious, it may drop packets due to broken link. In that case the node will send an error message i.e. RERR packet to its previous node and precursors. That RERR packet has been modified to include unique identifier of the dropped packet so that on reception of RERR packet, a node can delete the packet from its cache and will not be counted as dropped packet. Thus avoids the false positives.

C. *Distinguishing nodes based on trust value*

Higher the range value, more trust worthy the node is. Based on this, all nodes which are below the range value of 0.3 are considered to be malicious.

Association between the nodes is asymmetric. Node x may not have trust value on node y in the same way that node y has trust on node x. Though node x trusts node y, it doesn't mean that node y trusts node x. The trust is being gained based on

the experience a node having with the other one.

D. Routing Mechanism

When any node wishes to send messages to a distant node, it sends the ROUTE REQUEST to all the neighbouring nodes. The ROUTE REPLY obtained from its neighbour is sorted by trust ratings. RREP messages from non-trusted nodes are omitted and thus the routing path avoids the malicious nodes and establishes a secure channel of trustworthy nodes.

E. Blackhole avoidance

Once a node has been identified as malicious, all RREP packets from non trusted nodes are omitted and thus route will be selected only through trusted nodes and data packets will be transmitted only to these nodes. At the same time, it removes all the routing paths containing the malicious nodes from the route table of that particular node and its precursors. Thus black hole nodes are completely removed from existing routes and prevented from establishing route in future

F. Reception of confirmation packet

On reception of confirmation packet i.e.: the packet contains malicious node id, a node checks whether the packet is from a trusted source. If the packet is from a trusted source, then the node updates the range value of node id mentioned in that packet to 0.0 so that it will not establish route through that malicious node in future by dropping the RREP packets from the malicious node. And it also removes all the routing paths that contain the malicious node from the route table.

IV. Simulation Scenario

Blackhole nodes have been created and analysed the result of simulation with the above specified scenario for 500 seconds and 1000 seconds in NS2. Performance matrix we used to evaluate the performance of both the system is Packet Delivery Ratio (PDR).

TABLE 1

Parameter	Value
Examined Protocol	AODV
Application traffic	CBR
Transmission range	250 m
Packet size	512 bytes
Transmission rate	10 Kbps
Pause time	10 s
Maximum speed	20 m/s
Simulation time	500 s / 1000s
Number of nodes	50
Area	750 m * 750 m
Movement Model	Random waypoint
Types of attack	Blackhole attack

V. Analysis and Result

The packet delivery ratio is higher in the proposed method than pure AODV in the presence of malicious nodes. And the ratio increases as the time passes since once the malicious nodes are detected, they are prevented from further establishing a route. The graphs in the Fig.4 and Fig.5 show the comparison of packet delivery ratio in the presence of black hole attack in the proposed AODV and pure AODV in mobile ad hoc network for 500 ms and 1000 ms accordingly. In pure AODV, packet delivery ratio reaches even to 0 i.e. none of the packets are getting delivered in the presence of multiple black hole nodes in the network. From the Fig. 3 and Fig. 4, it is clear that, packets dropping are significantly reduced and the packet delivery ratio got increased in the proposed AODV, as the time passes since the black hole nodes are detected at the earliest. There is no significant change in packet delivery ratio in both AODV and proposed AODV during the absence of black hole nodes.

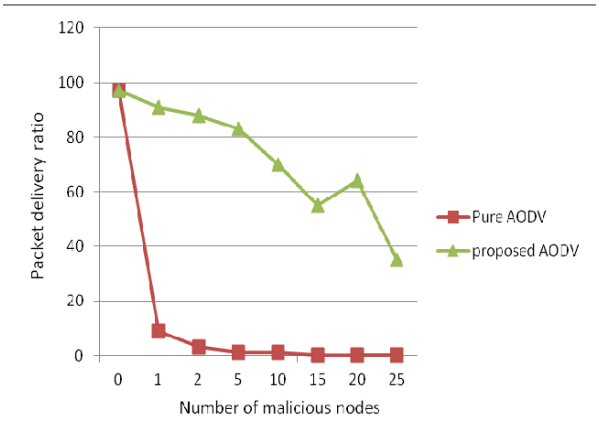

Fig.4 Packet delivery Ratio Vs Number of malicious nodes for 500 ms

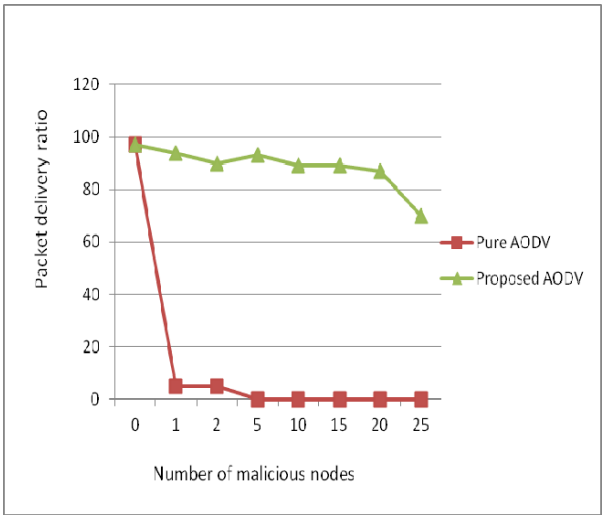

Fig.5 Packet delivery Ratio Vs Number of malicious nodes for 1000 ms

VI. Conclusion

A trust based approach for mitigating black hole attack in AODV protocol has been proposed. The method monitors the data packets being transmitted to neighbouring node in promiscuous mode and assigns a trust value to its neighbour dynamically and periodically. Future communications with neighbouring nodes are based on this trust value. The result shows, an efficient packet delivery ratio at the presence of malicious nodes. And the packet delivery ratio increases as the time passes as once the malicious node is detected, the network avoids that node from establishing routes to destination. As the method dynamically calculates trust level based on recent set of packets, even a node starts an attack after a long time; it detects the malicious activity in the network.

References

[1] N. Bhalaji, A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet", European Journal of Scientific Research, ISSN 1450-216X Vol.50 No.1,2011

[2] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[3] A.Rajaram, Dr. S. Palaniswami,"Malicious Node Detection System for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010.

[4] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks," The 4th IEEE Wksp. Mobile Computing Systems and Applications (WMCSA'02), June 2002.

[5] Y.-C. Hu, D. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks, Elsvier, vol. 1, no. 1, 2003.

[6] C. Castelluccia and G. Montenegro, "Protecting AODV Against Impersonation Attacks," ACM SIGMOBILE Mobile Comp. and Commun. Rev. Archive, vol. 6, no. 3, July 2002.

[7] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. (CNDS'02), Jan. 2002.

[8] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. 8th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom'02), ACM Press, 2002.

[9] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehaviour in mobile ad hoc networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, MOBICOM, Boston, Massachusetts, August 2000.

[10] Asad Amir Pirzada and Chris McDonald. Establishing Trust In Pure Ad-hoc Networks. In Proceddings 27th Australasian Computer Science Conference (ACSC'04), Dunedin, New Zealand, 26(1), pages 47-54, January 2004.

[11] A Trusted AODV Routing Protocol for Mobile Ad Hoc Networks. PhD thesis, Department of Computer Science and Engineering, The Chinese University of Hong Kong, 2003

[12] Seungjin Park, M. Al-Shurman and Seong-Moo Yoo. Black Hole Attack in Mobile Ad hoc Network, ACMSE'04, Huntsville, AL, U.S.A., April, 2004.

[13] Slavisa Sarafijanovic and Jean-Yvess Le Boudec. An Artificial Immune System Approach With Secondary Response for Misbehaving Detection in Mobile Ad hoc Networks,16, IEEE September 2005.