International Journal For Technological Research In Engineering
Volume 4, Issue 8, April-2017 *ISSN (Online): 2347 - 4718*

MISBEHAVIOR NODE DETECTION AND ELIMINATION IN MANET ROUTING

Ch. Chaithanya Deepthi[1], J. Mounika[2], B. Sri Harsha[3]
[1,2,3]B.Tech Students CSE Department, Lendi Institute of Engineering and Technology, Andhra Pradesh, India.

ABSTRACT: A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or indirectly depending on nodes in the network. As the nodes in the MANETs having mobility the position of nodes can changeas per the movements of the nodes, hence the network topology of a MANETs may change dynamically. Due to the dynamic change in topology, computing the route is a challenging task. During the network process the nodes consumes energy and utilizes the other resources of the network, but in the process of networking some nodes may misbehave. Because of this, unnecessary wastage of energy and resources may result and also security and performance of the network can be affected. Here in this work, we proposed an algorithm to establish route in such a way to detect and avoid misbehavior nodes. This reduces unnecessary wastage of energy and resources also provide security and improve the performance of the network. This algorithm is H-ALARM (Heterogeneous Anonymous Location Aided Routing in Suspicious MANET),this can Withstand DoS-Attacks based on AODV as an extension of PRISM,ALARM, we used watchdog and pathrater concepts for the detection of the misbehavior nodes. AODV protocol is designed to protect the network from malicious and selfish nodes.

I. INTRODUCTION

In the past few years, we have seen a rapid expansion in the field of mobile computing due to the proliferation of inexpensive, widely available wireless devices. However, current devices, applications and protocols are solely focused on cellular or wireless local area networks (WLANs), not taking into account the great potential offered by mobile ad hoc networking. A mobile ad hoc network (MANETS) is an autonomous collection of mobile devices (laptops, smart phones, sensors, Bluetooth, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for numerous new and exciting applications. In this project we are going to detect the misbehaving nodes in the network.

II. LITERATURE REVIEW

A Mobile ad hoc network (MANET) is a group of wireless mobile computers (or nodes); in which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. These systems work with the support of a centralized supporting structure such as an access point. The wireless users can be connected with the wireless system by the help of these access points, when they roam from one place to the other. The adaptability of wireless systems is limited by the presence of a fixed supporting coordinate. It means that the technology cannot work efficiently in that places where there is no permanent infrastructure.

Easy and fast deployment of wireless networks will be expected by the future generation wireless systems. This fast network deployment is not possible with the existing structure of present wireless systems. Recent advancements such as Bluetooth introduced a fresh type of wireless systems which is frequently known as mobile ad-hoc networks. Mobile ad-hoc networks or "short live" networks control in the nonexistence of permanent infrastructure.

MANET is a kind of wireless ad-hoc network and it is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which forms an arbitrary topology. The routers, the participating nodes act as router, are free to move randomly and manage themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

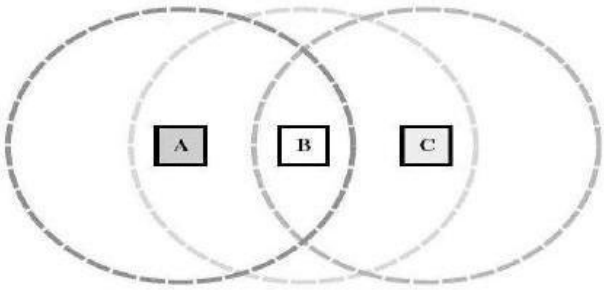

Fig 1: Example of a simple ad-hoc network with three participating nodes

Mobile ad hoc network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes can directly communicate to those nodes that are in radio range of each other, whereas others nodes need the help of intermediate nodes to route their packets. These networks are fully distributed, and can work at any 3 place without the aid of any infrastructure. This property

makes these networks highly robust. In (Figure 1.2) nodes A and C must discover the route through B in order to communicate. The circles indicate the nominal range of each node‘s radio transceiver. Nodes A and C are not in direct transmission range of each other, since A‘s circle does not cover C.

III. EXISTING SYSTEM

In the Existed System is ALARM (Anonymous Location Aided Routing in suspicious MANET) , in this they used DSR algorithm for the route establishment.
The ALARM can work as follows:

- Here, the group manager (GM) initializes the group signature scheme and enrolls all legitimate MANET nodes as group members. During this phase, each member (node) creates a unique private key, that is not revealed to anyone. This key is needed to produce valid group signatures. It also creates a corresponding public key, that is revealed only to the GM.
- Each node broadcasts a Location Announcement Message (LAM), containing its location, time-stamp, temporary public key, and a group signature. Each LAM is flooded throughout the MANET.
- It uses nodes current locations to construct a secure MANET map. Based on the current map, each node can decide which other nodes it wants to communicate with.

LIMITATIONS OF ALARM:
ALARM has an disadvantages like:

- Flooding is used to disseminate LAMs, scalability becomes problematic for large MANETS .
- Any node can lie about its location or generate multiple LAMs(Location Announcement Message) .

IV. PROPOSED SYSTEM

The Proposed System is H-ALARM, this uses AODV algorithm for the route establishment. This also uses the concept of Watchdog and Pathrater along with the group signature policy of existed system both to detect and avoid misbehavior node in the route establishment.
AODV (Ad Hoc On- Demand Vector) Routing Protocol:
This routing protocol is an on demand protocol. In order to identify the most recent routes it employs the destination sequence numbers. The main difference between the Dynamic Source Routing (DSR) and AODV is that DSR uses source routing in which a data packet carries the complete path to be traversed and in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission.

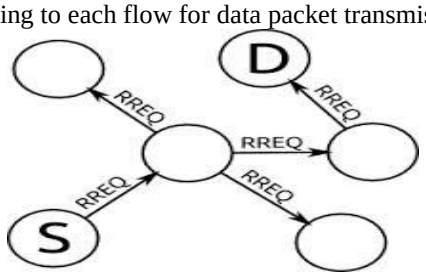

Fig 2:Generating the route request packet

In the above figure 3.1 sources generates the route request packet and is sent to all the nearby nodes until it reaches to its destination and find outs the route .It uses the destination sequence number to determine the up-to-date path to the destination.

AODV is an on demand routing protocol. AODV supports both unicast and multicast communication between nodes. AODV uses hop by hop routing which means routing not only involve source node but also intermediate node takes part in it. AODV is most used protocol in ad hoc networks. AODV uses symmetric links between neighboring nodes. AODV combines the features of DSR and DSDV.AODV uses a broadcast route discovery mechanism as is also used in the DSR. To maintain the most recent routing information between nodes it borrows the concept of destination sequence numbers from DSDV. AODV involves separate process for route discovery and for rout maintenance AODV also uses routing table for maintain routing information. This is called route table management.

Route discovery
First source node initiates the route discovery process when it needs to communicate with another node to discover a new path, source node broadcast a route request (RREQ) packet to or its neighbor. When the RREQ packet goes to intermediate nodes that node first check its routing table. If a valid route is present and the node reply with a RREP packet and if not when the node rebroadcast the RREQ packets to its own neighbor. If a node gets more than one copy of a RREQ packet for the same broadcast id when the node broadcast then the node drop the packet and does not forward duplicate copy. Route discovery set a path in two phases on is reverse path set-up and other is forward path set-up.

Routing Table:
AODV has separate routing table for both unicast and multicast routing. The routing table has all the useful information for a node like sequence number, lifetime of a route, hop count etc. besides these values it also has an entry for a timer all route request expiration time and route cache time out after which the route is considered as invalid. Like DSDV, its routing table also has sequence number of all routes. The sequence number ensures loop free path. This information helps when any link between the path break. When a new route is discover then the node first checks the destination sequence number present in it table. Destination sequence number gives information about the freshness of route.

Route maintenance:
During data delivery the source node moves away the path is lost than it can reinitiate the route discovery process. When a intermediate node on the route moves away from the path then a route error message sent a source. To detect link failure hello messages and link layer acknowledgement is used. When a link break is noticed on source node then the source node can reinitiate route discovery if the route still needed by the source. AODV used so much because it can

handled different types of mobility rate with different types data traffic. AODV also reduces routing overhead of control packets and modifications are further applied to improve scalability of the protocol. AODV applies local repair when the upstream node is closer to destination. There are many ways to improve the local route repair in AODV.

Two components are used to identify the misbehaving nodes:

- Watchdog: Runs on every node to keep track of the behavior of the other nodes.
- Pathrater: Uses the Watchdog information to find out the reliable routes.

Watchdog

Detects misbehaving nodes by overhearing transmission

- Maintain a buffer of recently sent packets
- Compare each overheard packet with the packet in the buffer to see if there is a match
- If a packet remained for longer than timeout, increments a failure tally for the node responsible
- If the tally exceeds a threshold, the node is determined to be misbehaving and the source will be notified

Watchdog Advantages

- Can detect misbehavior at the forwarding level

Pathrater

- Each node maintains a rating for every other node it knows about in the network
- It calculates a path metric by averaging the node ratings in the path
- The metric gives a comparison of the overall reliability of different paths
- If there are multiple paths to the same destination, it choose the path with the highest metric

RESULTS

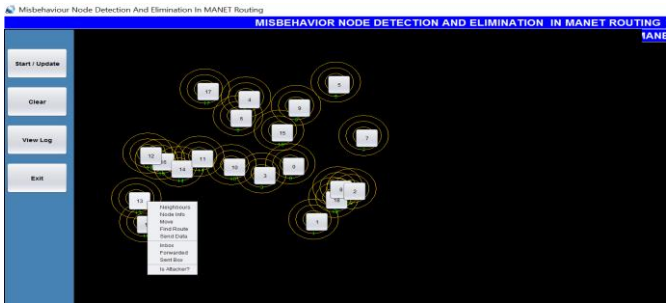

Fig 3:Network establishment

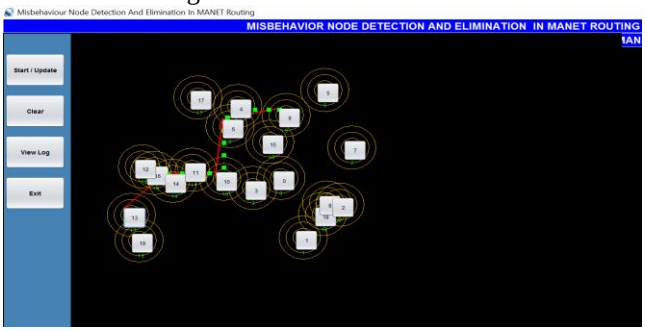

Fig 4:Path establishment between source an destination

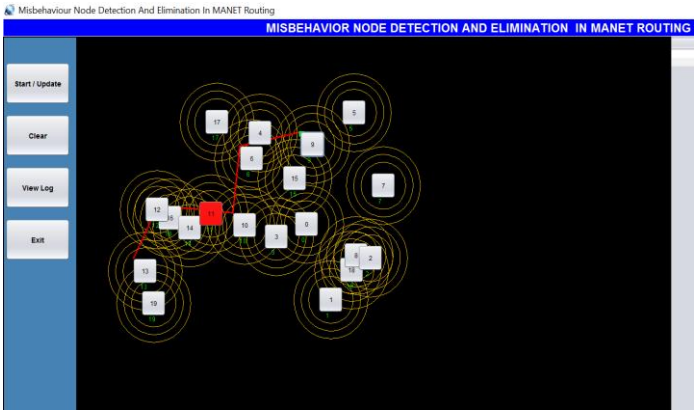

Fig 5:Detection of misbehavior node and showing alternative path

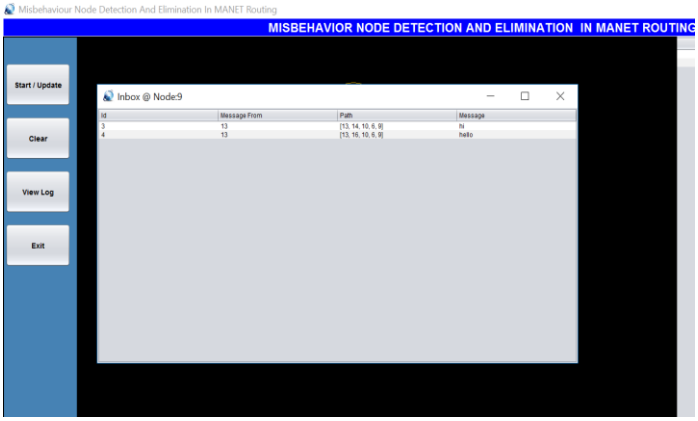

Fig 6:Path with misbehavior node and alternative path on the detection of misbehavior node

V. CONCLUSION

This paper presents the H-ALARM protocol which supports anonymous reactive routing in suspicious location-based MANETs. This, algorithm is to establish route in such a way to detect and avoid misbehavior nodes, using Watchdog and Pathrater. This reduces unnecessary wastage of energy and resources also provide security and improve the performance of the network. Thus, H-ALARM reveals less of the topology and is more privacy friendly and ensures security. Hence, it results in a good performance of the network and increases efficiency, it also obeys the Scalability of the network

REFERENCES

[1] S.N.Chobe, Deepali Gothawal, "An Acknowledgement Based Approach For Routing Misbehavior Detection In Manet With Aomdv", International Journal of Advanced Computational Engineering and Networking, Volume- 1, Issue- 5, July-2013.

[2] H.D.Trung, W. Benjapolakul, P. M. Duc, Performance evaluation and comparison of different ad hoc routing protocols‖, Department of Electrical Engineering, Chulalongkorn University, Bangkok, Thailand, May 2007

[3] Jakobsson, M. and Hubaux, J.P. and Butty, ―A

micro-payment scheme encouraging collaboration in multi-hop cellular networks‖, Computer Aided Verification, pages=15–33, year=2003, organization= Springer

[4] Liu, K. and Deng, J. and Varshney, P.K. and Balakrishnan, K.,―An acknowledgment-based approach for the detection of routing misbehavior in MANETs‖, Mobile Computing, IEEE Transactions volume=6, number=5, pages=536–550, year=2007, publisher=IEEE.

[5] H.D.Trung, W.Benjapolakul, P.M.Duc, ―Performance evaluation and comparison of different ad hoc routing protocols‖, Department of Electrical Engineering, Chulalongkorn University, Bangkok, Thailand, May 2007

[6] L.B.Oliveira, I.G.Siqueira, A.A.F.Loureuro,‖On the performance of ad hoc routing protocols under a peer-to-peer application‖, Computer Science Department, Federal University of Minas Gerais, Brazil, July 2005

[7] T.Fujiwara, T.Watanbe, ―An ad hoc networking scheme in hybrid networks for emergency communication‖, Information Technology Lab, Eugene Co. Ltd, Hamamatsu, Shizuoka, Japan

[8] P.P.Pham, S.Perreau, ―Increasing the network performance using multi-path routing mechanism with load balance‖, Institute of Telecommunications Research, University of South Australia, Australia, September 2003

[9] M.K.Marina and S.R.Das, ―On-Demand multipath distance vector routing in ad hoc networks‖ in: Proceedings of the 9th IEEE

[10] C.S.R.Murthy, B.S.Manoj, Ad hoc Wireless Networks, Architecture and Protocols, 6th Edition.

[11] R.Balakrishna, M.Murali Mohan Reddy Dr.U. Rajeswar Rao, Dr. G. A. Ramachandra, ―Routing Misbehavior Detection in MANET Using 2ACK‖, in IEEE Advanced Computing Conference, Thapur University, Patala,2008.

[12] R.Balakrishna, M.Murali Mohan Reddy, Dr.U.Rajeswar Rao, Dr.G.A.Ramachandra,‖ detection of routing misbehavior in mobile ad hoc networks using enhanced 2ack (e-2ack)‖,in IEEE Advanced Computing Conference in at , Thapur University, Patal,2008.

[13] R. Balakrishna, Dr. U. Rajeswara Rao, Dr. N. Geethanjali, ―Secure Key Exchage protocol for Credential Services‖, Published in Defence science Jounal in May 2009.

[14] R. Balakrishna, Dr. U. Rajeswara Rao, Dr. N. Geethanjali, A secured authenticated key exchange protocol for credential services‖, in 3rd International conference ICACCT-2008, Page 120-129,www.apiitindia.org/icacct2008.

[15] R. Balakrishna, Dr. U. Rajeswara Rao, Dr. N. Geethanjali,‖Video Conferencing on Mobile Adhoc Network‖, in 2nd International Conference CCR2008,Page298-305.

