ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Secure Routing and Detection of Hybrid Attacks in MANET

Dr.B.Rosiline Jeetha, K.Sivakamipriya

HOD, PG & Research Department of Computer Science, Dr.N.G.P. Arts & Science College, Coimbatore, India.

Research Scholar, PG & Research Department of Computer Science, Dr.N.G.P.Arts & Science College,

India.

Coimbatore, India.

ABSTRACT: Mobile Ad-Hoc network (MANET) is a type of communication network which is used for data communication between mobile nodes using wireless channels. Clustering has evolved as an important research topic in MANETs as it improves the system performance of MANETs. A novel routing protocol based on A* path finding algorithm and hybrid BAT algorithm is proposed to solve the cluster issues There are five phases namely discovery, cluster formation, cluster head selection, path selection and route maintenance. In path discovery, the shortest path between the gateway and other nodes is found using A* path finding algorithm based on AOMDV where more than five routes have been discovered. in NS2 and compare with existing protocols. The proposed method is zone based routing protocol for supporting power heterogeneous MANETs. In the previous method, number of protocol is provided for communication. The base station gathers data from sources and then delivers the collected data to other nodes. It provides hotspot problem, high congestion, and large amount of energy consumption. It increases the network life time and delay. Proposed method reduces hot spot problem and gives more efficiency in terms of data delivery ratio.

KEYWORDS: Routing; Route discovery; Link availability; Ad hoc on-demand multipath distance vector (AOMDV)

I. INTRODUCTION

With emerging mobile applications [1–3], mobile ad hoc networks (MANETs) have attracted research from vari- ous groups due to its flexibility and usability in diverse applications. A MANET is a self-configuring temporary network of mobile nodes which are independent with each other and do not have any fixed infrastructure. MANETs do not control or regulate traffic [4] within the network but utilize the intermediate node's routing capability. Since source and destination nodes use inter- mediate nodes as routers, a routing path must be estab- lished for actual communication. Routing protocols are the key to MANET success and are an active area for MANET research [5–9].

Many routing protocols have been proposed for ad hoc networks in literature which find a route based on given criteria for packet delivery from source to destin- ation. In literature, routing protocols are broadly classified as table-driven protocols and on-demand protocols. In the former, also called proactive routing protocols, every node maintains a table of data containing routing information such that source can reach any node in the destination if a route exists. Popular table-driven proto- cols include optimized link state routing (OLSR) and destination sequenced distance vector (DSDV). In on- demand routing protocols, routes are created as and when needed. They are also called as reactive protocols, and the source invokes route discovery process when data has to be transmitted. A route is valid till destin- ation is reached or until route is not required. Popular existing on-demand routing protocols include dynamic source routing (DSR) and ad hoc on-demand distance vector AODV [10, 11] protocol.

In AODV, [12, 13] a source node broadcasts route request (RREQ) to its neighbors. When adjacent nodes received RREQ with source node and target node ad- dresses, it judges if it is the target. If yes, it sends a route reply (RREP); otherwise, it checks if it has active route to the destination in its table. If it has a fresh route, then it sends

DOI: 10.15680/IJIRCCE.2017. 0502046

RREP to the source or it continues flooding by sending RREQ. AODV protocol discovers neighborhood nodes through regular broadcast of hello messages. When a link breaks, it sends route error message while deleted/broken records are repaired.

Ad hoc on-demand multipath distance vector (AOMDV) [14] is an AODV extension for computing multiple loop-free and link-disjoint paths. The routing table for destination includes a list of next hops and the number of hops to reach the destination. In AOMDV, all the available next- hop neighbors are assigned the same sequence numbers. A node maintains advertised hop count for every destination, and this hop count sends destination route advertisements. Every duplicate route advertisement that has been broad- casted and received by a node defines an alternative destination path.

II. RELATED WORK

A multipath routing protocol proposed by Obaidat et al. [16] is a variant of single-path AODV routing protocol. The proposed method established node-disjoint paths with lowest delays based on interaction of factors from various layers. The proposed protocol's performance was investigated and compared to single-path AODV and multipath AOMDV protocols using Operations Network (OPNET). Results show improved performance of the proposed method in terms of throughput and end-to- end delay.

Garcia-Luna-Aceves [2008] approach is Multicast packets for a group is forwarded along with shortest paths from sources to receivers defined within the group's mesh. Camp uses cores only to limit the traffic needed for a router to join a multicast group. Failure of cores does not stop packet forwarding and the process of maintaining the multicast meshes.

Young-BaeKo [2008] approach is geocasting. In this method, group consists of set of all nodes within a specified geographical region. Hosts within a specified region at a given time forms the geocast group at that time. One drawback of this approach is to present two different algorithms for delivering packets to such a group and present simulation results.

Brad Karp [2009] recognized to compare the performance of Greedy Perimeter Stateless Routing for Wireless Network with Dynamic Source Routing. Simulation result demonstrate GPSR's scalability on densely deployed wireless networks. By keeping state only about the local topology, GPSR scales better in per-router state than shortest-path and ad-hoc routing protocols as the number of network destinations increases. Under mobility's frequent topology changes, GPSR can use local topology information to find correct new routes quickly.

III. METHODOLOGIES

A. POSITION BASED MULTICAST ROUTING

The forwarding decisions in position-based routing are usually based on the node's own position, the position of the destination, and the position of the node's direct radio neighbors. Since no global distribution structure as a route is required, position-based routing is considered to be very robust to mobility [15]. It typically performs best if the next-hop node can be found in a greedy manner by simply minimizing the remaining distance to the destination. There are situations where this strategy leads to a local optimum, and no neighbor can be found greedily to forward the packet further, although a route exists. This paper deals with the "Location-Guided Tree Construction Algorithms", the sender includes the addresses of all destinations in the header of a multicast packet. It remains open how the sender is able to obtain the position information, and the scaling limitations.

B. LOCATION-BASED MULTICAST PROTOCOLS

Two approaches may be used to implement location based Multicast: First, maintain a multicast tree, all nodes within multicast region at any time belong to the multicast tree. The tree would need to be updated whenever nodes enter or leave the multicast region [8]. Second, do not maintain a multicast tree. In this case, the multicast may be performed using some sort of "flooding" scheme. This paper considers multicast group members send a packet to specific multicast region.

C. EXISTING SCHEME

Reactive protocols, such as DSR and AODV, find a route only on demand fictitious nodes create fake MPR node send to neighbors nodes covered by networks. We propose a solution using trust analysis to verify whether corresponding node is malicious or not.Our method uses HOP_INFORMATION table store in OLSR table. In this paper we review a specific DOS attack called node isolation attack and propose a new mitigation method. Our solution called Denial contradictions with Fictitious Node (DCFN) relies on the internal knowledge acquired by each node during routine routing, and augmentation of virtual (fictitious) nodes. DCFM utilizes the same techniques used by the attack in order to prevent it. OLSR proposed by with detection attack node automatically intimate to all node board cast to topology control message.

D. NETWORK FORMATION:

In this module, multiple nodes will created by giving distance and range. Based on coverage the neighbor node will be detected. Each node finds all available paths (how long it can be travel) . This path finding mechanism is done by random linear walk algorithm and all the available paths to reach most possible destinations by every node.

E. FINDING MULTIPOINT RELAYING (MPR):

Each node finds Multipoint Relaying through OLSR technique. In this technique MPRs are selected by a node as a subset of its 1-hop neighbors, such that the MPR set allows coverage of all of its 2-hop neighbors. By minimal MPR selection, a node is able to communicate to all 2-hop neighbors with minimal duplication. Thus, both topology control messages and data packets are only forwarded by this minimal MPR set, allowing for fewer duplicate messages while maintaining network-wide coverage. 1 Hop neighbors' and 2 Hop neighbors are calculated based on the all available paths previously calculated. The number of destination a particular node can reach is identified and paths to reach every destination by 2 Hops are calculated. Minimal MPR set is found out by identifying the one hop nodes which is able to reach all of its two hop nodes effectively. From the minimal set a MPR is chosen by voting mechanism and which MPR got more support will be elected as the sole MPR for the particular node.MPR is chosen for each and every node and the 2 HOP paths to reach every location is found out and the tables are updated.

Note: MPR reduce the number of duplicate retransmission messages while forwarding a broadcast packet.Isolation attack by DDos In the voting mechanism one of the MPR which is going to do the Node isolation attack claims himself as the best MPR by having support from the fictitious node. Only the Single hop neighbors can be elected as the MPR. (The attacker can learn its 2-hop neighbors by analyzing the TC message of its 1-hop neighbors.) Now the target node believes attacker to be its only MPR. The only node that must be used to forward and receive the TC packets as well as data packets. By drooping TC message received from the target node and not generating the TC message for the target node, the attacker can prevent the link information of the target node for being disseminated to the whole network. Like this the target node will be gradually eliminated by DDOS Attack from the network. DDOS here refers to the message packets delivered and sent to the target node by attacker node.

F. DETECTING ISOLATION ATTACK AND SYSTEM RECOVERY:

In this module,the detection of Isolation attack by an acknowledgement scheme. The target node can keep track of the data packets and listens for acknowledgement from the communicating nodes. If the data is dropped or not forwarded to the other nodes the acknowledgement is other nodes about the Fake MPR. Now the MPR is valuated for the attacking process and if found lost and the target node will wait for some ttl time. After that the target node will intimate guilty the MPR node is dropped from network and another MPR from minimal MPR set is employed for data forwarding. Now the Network recovery will be done and all the nodes will update their records by removing the attacker node. All the OLSR paths will also be updated leaving the Attacking MPR.

Denial Contradiction with Fictitious node Mechanism The first requirement of the proposed method is that each node will only use information available to it, without relying on any centralized or local trusted authority. Our technique does not actively verify the HELLO message, rather it checks its integrity bysearching for contradictions between the HELLO message and the known topology. We allow for lone MPR nominations, provided that no contradictions are found. Even in the face of contradictions, an MPR can be nominated for all 2-hop neighbors for which it is the sole access point. It cannot, however, be nominated as sole MPR for 2-hop neighbors that can be reached through other paths. We assume that TC messages cannot be spoofed. We justify this assumption due to the fact that bogus TC messages do not preclude a legitimate (attacked) victim from transmitting a valid TC that contradicts the bogus one. In essence, by publishing a fraudulent TC, the attacker discloses that he is attacking; allowing others to take preventive measures. A fake HELLO message is a much more crippling attack, because it removes a victim from the network without its knowledge.

IV. RESULTS AND DISCUSSIONS

SIMULATION SCENARIOS

Packet Size	:	1000 bytes
No. of Nodes	:	30
Protocol Used	:	OLSR
Dimension	:	1000*1000
Channel Type	:	Wireless channel IEEE 802.11
CMUPriQueue	:	Omni Antenna
Protocol	:	TCP
Mobility	:	10 m/s
Traffic Type	:	CBR
Traffic interval	:	0.05

Performance Evaluation

Performance Metrics

Delay

It is defined as the average time taken by the packet to reach the server node from the client node.

Delay = (Inter arrival of 1st pkt time and 2nd packe time) / (simulation_time)

Delivery Ratio

Packet Delivery Ratio is defined as the average of the ratio of the number of packets received by the receiver over the number of packets sent by the source.
Delivery Ratio = (total_packets_received) / (total_packets_sent) *100

Energy Consumptions

Average Energy consumed on idle, sleep, transmit, and receive with respect to total energy consumed

Throughput

Throughput is the number of useful bits per unit of time forwarded by the network from a certain source address to a certain destination.

Delivery Ratio = (Number of Packets Received) / (Number of packets Sent)

Packet Drop:

Drop = (Number of Packets Received) - (Number of packets Sent)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

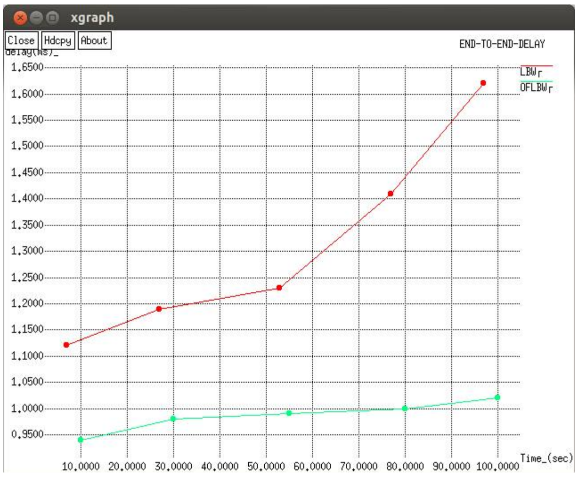

Figure 6.2 Time VS End-to-end delay

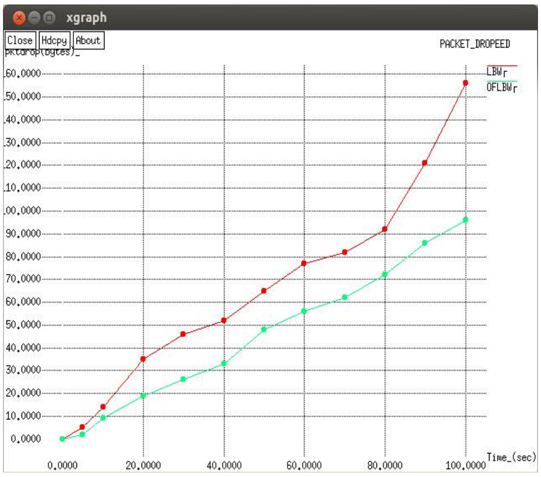

Figure 6.4 Time Vs Energy (joules)

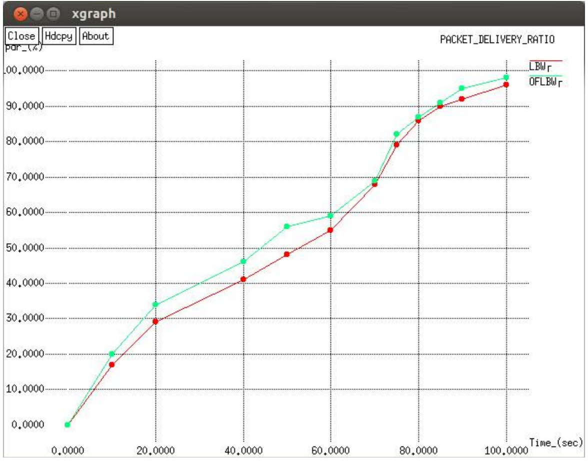

Figure 6.3 Time Vs PDR (%)

V. CONCLUSION

An efficient and novel strategy that protects critical nodes from DDoS attacks in MANETs. Considering the different roles that certain nodes play in a MANETs, it is assumed that there are some important nodes that should be protected with higher priority. Lower level nodes would be allocated as protection nodes to handle the incoming traffic to the higher level node is able to reduce suspect nodes and from nominating them as a sole MPR, thus, side stepping the essential element of the attack. Experiment done Through intensive simulation experiments using NS-2 and proved that every functionality works well as expected, there is raise in routing overheads about 5-10% for node velocities up to 30 m/s congestion of the network disappears and load is transmitted uniformly throughout the network. The modified OLSR also gives the reduction in average end to end delay.

REFERENCES

1. KS Chung, JE Lee, Design and Development of m-Learning Service Based on 3G Cellular Phones. JIPS 8(3), 521 (2012)
2. H Luo, ML Shyu, Quality of service provision in mobile multimedia-a survey.
Human-centric Computing and Information Sciences 1(1), 1–15 (2011)
3. JKY Ng, Ubiquitous healthcare: healthcare systems and applications enabled by mobile and wireless technologies. Journal of Convergence 3(2), 31–36 (2012)
4. Gawande, A. (2013). Performance analysis of DSR protocol under sinkhole attack in MANETs. International Journal, 1(4).
5. R Sumathi, MG Srinivas, A survey of QoS based routing protocols for wireless sensor networks. J Inf Process Syst 8(4), 589–602 (2012)

6. AU Bandaranayake, V Pandit, DP Agrawal, Indoor link quality comparison of IEEE 802.11 a channels in a multi-radio mesh network testbed. J Inf Process Syst 8(1), 1–20 (2012)
7. Li, X., Mitton, N., Nayak, A., & Stojmenovic, I. (2012). Achieving load awareness in position-based wireless ad hoc routing. Journal of Convergence, 3(3).
8. Chien, F. T., Wu, K. G., Chan, Y. W., Chang, M. K., & Su, Y. S. (2014). An Effective Routing Protocol with Guaranteed Route Preference for Mobile Ad Hoc Networks. International Journal of Distributed Sensor Networks, 2014. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 532049, 18 pages http://dx.doi.org/10.1155/2014/532049