DOI: 10.21917/ijct.2016.0200

ZONE BASED PATH ROUTING APPROACH FOR THE DETECTION AND PREVENTION OF MALICIOUS BEHAVIOUR OF THE NODE IN MANET

Akansha Shrivastava[1] and Ekta Chauhan[2]
[1]*Department of Computer Science and Engineering, Shri Ram College of Engineering and Management, India*
E-mail: [1]akanshasrivastav9oct@gmail.com
[2]*Department of Computer Science and Engineering, Maharana Pratap College of Technology, India*
E-mail: [2]ektachauhan81@gmail.com

Abstract

Mobile Ad-hoc Network (MANET) is one of the important research areas. MANET is a cluster of movable nodes that communicate without any wired connection. It refers to a network of moving nodes communicating with other mobile nodes in a multi-hop fashion. Mobile nodes provide flexibility to this network. Thus this flexible network is prone to a variety of attacks. Wormhole attack is a major threat to this network. In this attack, a tunnel is created between two nodes. These nodes transmit all communication through this tunnel. Detecting such attack is a major task. This paper presents a zone-based approach that detects and prevents such attack.

Keywords:

MANET, Wormhole Attack, Security, AODV

1. INTRODUCTION

The communication that takes place without the use of any predefined structure or access point, such communicating network is regarded as a wireless medium for communicating with other devices. The vital role played by the devices known as mobile nodes responsible for establishing such a familiar network the mobile ad-hoc network. These mobile device or nodes communicate with other devices or nodes for sharing as well as transferring data. The overall communication is completed with these devices. The transmission is carried node by node in other words multi-hop routing. Mobile nodes provides flexibility to this network in sense they are moveable; free from any boundations; independently moves across the network; joining or leaving the network on own wish. The flexibility and mobility makes MANET vulnerable to different types of attack. These attacks are on different layers of the network. The most susceptible attacks are on network routing protocols. These attack effect the forwarding and routing of the data during transmission, network performance is degraded, results in congestion, a collision of packets due to hidden terminals, loss of data packets, much more. Securing MANET against these attacks is a challenging task. The security goals are also affected by them [1].

1.1 THE SECURITY GOALS

The basic security goals are depicted as follows [1]:

1.1.1 Authentication:

The principle security goal ensures the authenticity of a node. The node taking part in transmission is a legitimate node or malicious. The identity of the node is verified.

1.1.2 Confidentiality:

This security goal ensures that the transmitted data send to receiver node is not read by any malicious node, only the intended recipient is able of accessing it.

1.1.3 Integrity:

By the term integrity, we mean that the transmitted data reached the intended recipient in the way forwarded by a source without any modification in the data packet.

1.1.4 Non-Repudiation:

It ensures, after sending as well as receiving of the data packet the source and receiver can't denying of sending or receiving the packet.

1.1.5 Availability:

The network resources are available whenever needed by a legitimate node.

1.2 SECURITY ATTACKS

Various security attacks are present which hinder the network operations and performances. The Network layer attacks are generally active attack. Some examples of network layer attack are black hole, wormhole, gray hole, and many more. These attacks have a great impact on the routing protocols that responsible for routing the data [1].

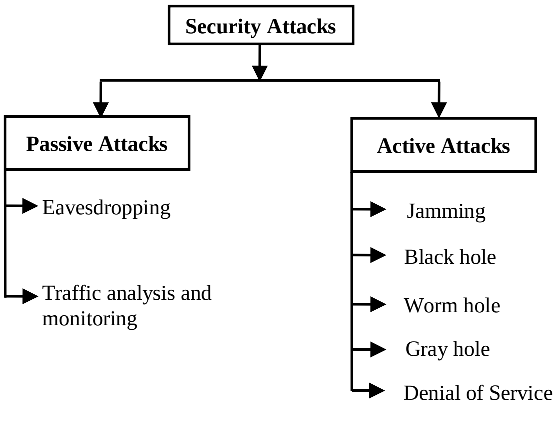

Fig.1. Types of Attacks

1.3 AODV WORKING

Ad-hoc On-demand Distance Vector Routing Protocol is a reactive protocol. Routes are established when needed. Whenever a source node has a packet for the destination, it checks for a valid path if available otherwise it begins a route discovery process. In this process, two phases are involved;

Route establishment phase and Route maintenance phase. In route establishment phase, the route is established on demand by sending route request packet (RREQ). This packet is broadcasted in the network. On receiving this packet if the node is destination node it replies with route reply packet (RREP) if the node is not destination node but has a valid route it replies the source with packet otherwise, it forwards the request packet to its neighbor node. With the aid of intermediate nodes, the request packet reaches the destination. On receiving the packet by destination node it floods the RREP packet in reverse route to a source. This packet is delivered to the source by the same process used for RREQ. Once the route is established the route is maintained till there is the requirement on the route. In the case of any failure takes place the source is acknowledged with route error packet (RERR). Hence three messages are used: RREQ, RREP and RERR [2].

1.4 WORMHOLE ATTACK

Wormhole attack is a network layer attack launched for disrupting the operation of the routing protocols. This attack is one of the most severe attacks as its detection and prevention is a major challenge as it is harder to identify it.

Such type of attack operates in collaboration with more than two malicious nodes. The node captures the packet from the source then transmits the captured packet to the other malicious node with the aid of wormhole tunnel. All the transmission is then carried out by this wormhole tunnel. Detection is difficult as the malicious node does not include their identities in the packet header during the process of route discovery.

The malicious nodes catch the attention of the source node, creating a delusion to source or other nodes of having optimal path to the destination. The attacker makes a tunnel record the ongoing transmission and traffic at one location and tunnel the packet to other location in the network. Hence creating a direct link among each other, receives a packet at one position and transmitting to other position. When two nodes are at this position the attack is known as out of the band. When attacker creates an overlay tunnel over existing medium then the attack is in-band [3], [4].

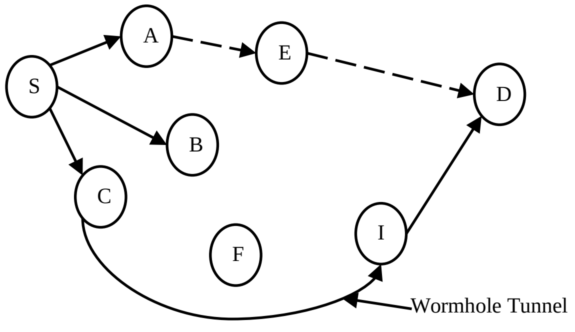

Fig.2. Example of Wormhole

In given Fig.2, an example of wormhole attack is depicted. Here node S and D are source and destination node respectively. A, B, E, F is good nodes, nodes C and I are malicious nodes connected with each other through a link' "wormhole tunnel".

1.4.1 *Types of Wormhole Attack:*

Different types of wormhole attack are described in different works of literatures [3] [4] [5].

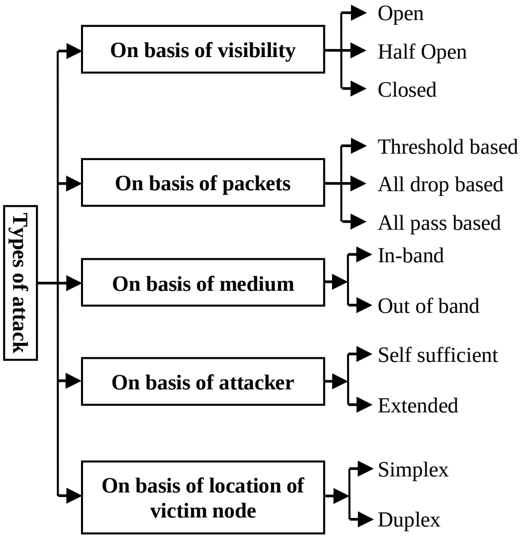

Fig.3. Types of wormhole

1.4.2 *Types of Wormhole Modes:*

The given Fig.4 depicts the various modes of operations of wormhole attack. With the aid of these modes wormhole attack is launched [6].

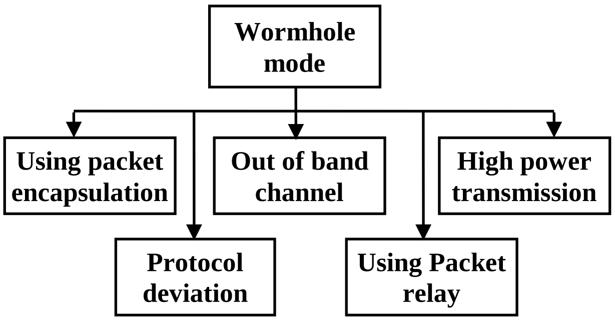

Fig.4. Modes of wormhole attack

2. RELATED WORK

Biswas et al. [7] devised an approach for detecting and removal of wormhole attack as well as removes false alarm. WADP detects both hidden and exposed wormhole attack. This approach WADP together with authentication works in order for removing the false positive alarm. Here the AODV is modified. In the route reply packet two new fields which is a combination of IP address of intermediate node and a unique number for verifying the authenticity of the node. The overhead is increased as node observes neighbor's behavior.

Sundararajan et al. [8] implemented a unique approach for detecting the misbehaviour of the nodes known as "Biological based artificial intrusion detection framework". BAID make use of an intrusion detector capable of detecting the misbehaving node obtaining the information relating to routing protocols. This approach is applied on the three routing protocols in there extended forms namely; AODV, DSR and DSDV.

P. Anitha et al. [9] a Path Tracing (PT) algorithm is devised to detect and prevent the wormhole attack. This PT algorithm works on each node in the path during the AODV procedure of route discovery. It is the responsibility of every node in the route to evaluate the per hop distance of its neighbor with the previous value of per hop distance so as to identify the wormhole attack. The relative node detects the existence of wormhole in the event when per hop distance crosses the highest threshold range. This approach is used for identifying the existence of wormhole link.

Alshamrani et al. [10] represented an algorithm to detect the wormhole attacks, both in hidden or exposed mode named Packet Travel Time. In this mechanism each and every node evaluates the neighbors and records the evaluation values in the neighbor node table. With the use of the threshold cryptography no malicious node can record any value in the neighbor node table. In this mechanism, whenever there is node that does not want to broadcast the monitoring table than there is no need to use threshold cryptography. The neighbor node table will be broadcasted whenever a negative value has been recorded.

Alam et al. [11] presented a unique method for detecting wormhole known as RTT-TC, depending on round trip time (RTT) measurements and topological comparisons (TC). Depend on the two observations of wormhole attacks: Two forge intermediate nodes with a wormhole tunnel contain longer RTT, in respect to the RTT that authentic neighbors have. Two authentic neighbors usually share other legitimate neighbors between them, and two fake neighbors do not share common legitimate neighbors. Author proposed to combine topological comparison and RTT measurements to detect wormhole attacks they first depend on RTT measurements to identify the suspected wormhole attacks and then use topological comparison to exclude authentic neighbors from the suspected list.

3. PROPOSED METHODOLOGY

The first problem encountered in the previous work is a node can be treated as a malicious node. When the radius of a node is small and node is mobile moves out of the transmission range of the other nodes for particular time duration and when it returns to the network that time the node can be treated as wormhole node. And second is Packet can be modified. As for node authentication in the RREP packet, two fields the IP address as well as a unique number are used. When a node forwards an RREP packet to its neighbor node it verifies the combination as the authentic node knows this information. When a passive attack is launched it cannot detect it as a result packet can be modified as the nodes are unable to collect the correct information.

So in proposed approach, the two things carried out are, first is to set a value. Because sometimes due to congestion in the network acknowledgment is not received by the nodes and it is assumed that there is the presence of malicious node. Hence by setting value nodes wait for acknowledgment which reduces the possibility of treating node as malicious. And second thing is that in route request packet (rreq), contains the previous route information and route reply packet (rrep) contains the node id's of its neighbor node thus possibility of modification of packet is solved.

In proposed approach, wormhole attack is detected and prevented by using zone-based approach. On the basis of zone information and previous route information detection and prevention is done. In this approach, zones are created on the basis of the transmission range of nodes this is done by calculating the number of hops counts. Once the zones are created the source node flood the rreq in the network. Since source node has the packet but the route is not known, for route establishment rreq packet is flooded, on receiving the rreq packet nodes unicast an rrep packet to source node now the route is established and optimal route is obtained communication begins. On not receiving an acknowledgment from the node the source node waits for the set_value i.e. 2, (waiting for acknowledgment 2 times.) when an acknowledgment is received before this set_value it is assumed that no congestion or no existence of malicious node is detected and this route is optimal and transmission begins on this route. But if an acknowledgement is not received within the set_value, the node generates new request packet that contains previous (prev) rreq and previous route information the node forward this packet to neighbor nodes. On receiving this new rreq send the neighboring nodes to reply with rrep, this rrep contains the node_id as well as the distances between nodes. On the basis of previous route information, route check as well as zone information the malicious nodes are detected and removed by blacklisting them. The zone in which the malicious node exists will not be considered for further communication.

3.1 PROPOSED ALGORITHM

1. Initializing the network.
2. Creating zones in the network on the basis of node's transmission range, this is done by calculating the number of hops, source hop its next hop and it's next to next hop.
3. Flooding the route_request packet (RREQ) in the network.
4. The route is obtained from step (3).
5. Obtained route is assumed as optimal route, follow this route.
6. On not receiving the acknowledgement on set_value

   set_value>2

   {Go to (7)}

   Else

   The optimal route is followed
7. For new route, generate new rreq_packet; containing prev_rreq+prev_route_info
8. New rreq_packet is send to neighbouring nodes.
9. On receiving new rreq_packet, nodes generate rrep_packet.
10. rrep_packet contain node_id's and distances of neighbouring nodes.
11. if (prev_route_info== new_route_info)

    Goto (12)

    Else

    Follow the route. Update info in routing_table.
12. Check distance among nodes.

```
13. If (Distance of nodes == stored nodes || next hop is same), checking the reception of acknowledgement of that node.
    Else
    Node is authentic and follows the route
14. Acknowledgement received the node is authentic, follow the route
    Else
    Nodes are malicious. Blacklist these nodes.
15. End
```

4. SIMULATION AND RESULTS

The simulation is carried over NS-2. The total number of nodes is 14.

Table.1 Simulation Parameters

Parameters	Value
Channel	Wireless
Propagation	Two Ray Ground
Network Interface Type	Wireless Physical
MAC type	Drop tail
Link Type	Logical Link
Queue length	50
Number of nodes	14
XY dimension	800X800
Routing Protocol	AODV
Simulation ends	100.0ms

4.1 PACKET DELIVERY RATIO

Packet delivery ratio means that, the total numbers of packets delivered per number packets send.

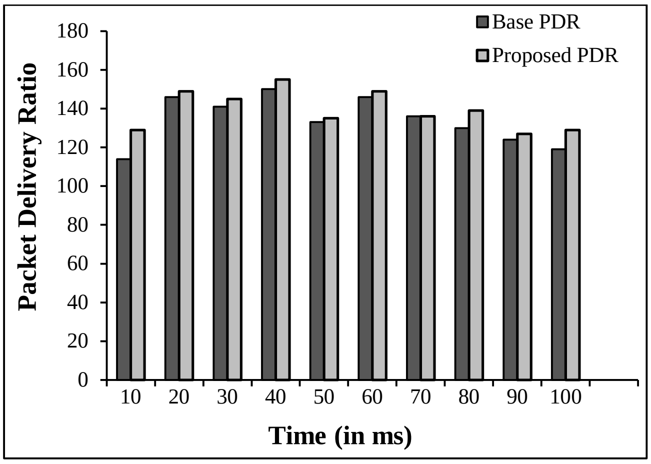

Fig.5. PDR graph between base and proposed approach

The graph depicts the maximum number of packets are delivered by proposed approach as compared with the base approach. The least value of existing approach is 114 in 10ms and maximum is 150 in 40ms, whereas of minimum and maximum value of proposed approach is 127 in 90ms and 155 in 40ms respectively.

4.2 SEND PACKETS

Send packet means that, the total number of packets sends from source to destination.

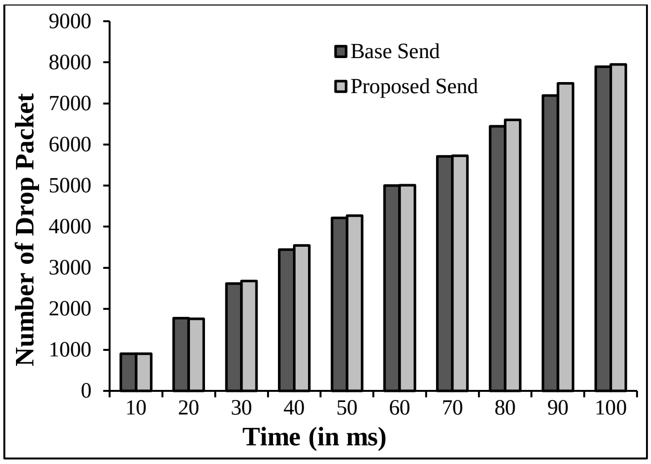

Fig.6. Send packet ratio graph between base and proposed approach

The graph depicts the maximum number of packets are send by proposed approach as compared with the base approach. The least value of base approach is 904 in 10ms and maximum is 7892 in 100ms, whereas of minimum and maximum value of proposed approach is 904 in 10ms and 7947 in 100ms respectively.

4.3 RECEIVE PACKET

Receive packet means that, the maximum number of packets received by destination node.

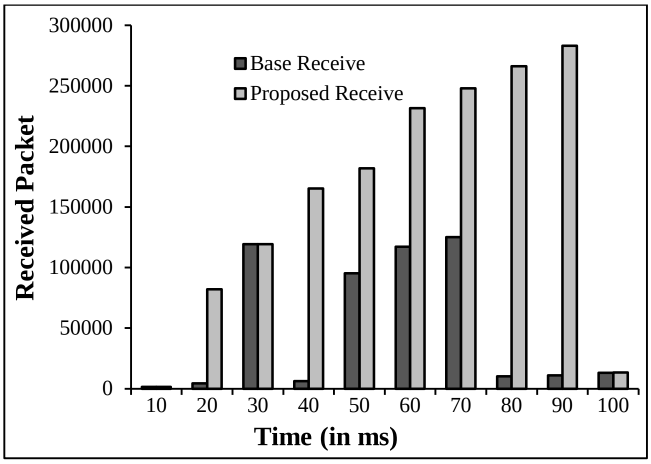

Fig.7. Received packet graph between base and proposed approach

The graph depicts the maximum number of packets are received by proposed approach as compared with the base approach. The least value of base approach is 1345 in 10ms and maximum is 125094 in 70ms, whereas of minimum and maximum value of proposed approach is 1355 in 10ms and 283080 in 90ms respectively.

4.4 DROP PACKET

Drop packet means that, the minimum number of packets dropped while reaching the destination node.

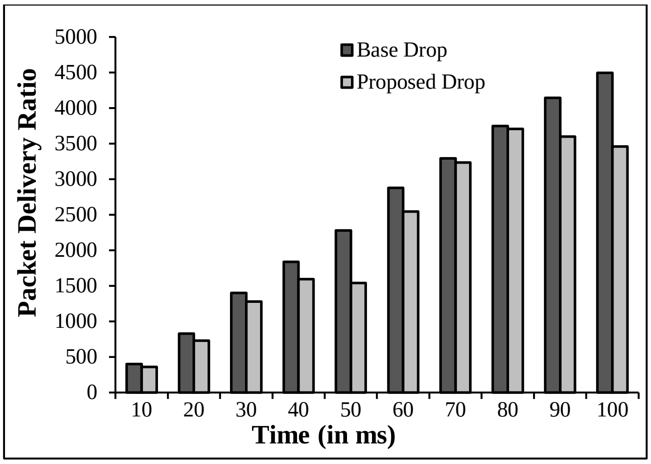

Fig.8. Drop packet ratio graph between base and proposed approach

The graph depicts the minimum number of packets are dropped by proposed approach as compared with the base approach. The least value of base approach is 402 in 10ms and maximum is 4497 in 100ms, whereas of minimum and maximum value of proposed approach is 360 in 10ms and 3708 in 80ms respectively.

5. CONCLUSION

Wormhole attack is a severe attack on MANET routing protocol. This attack works in collaboration of more than one node using a tunnel for communication. The malicious nodes attract the source node of having the optimal path to the destination, captures the packet; tunnels it to another malicious node. As a result, the network is disrupted and packets are dropped. The detection, as well as prevention of such attack, is a challenging task. The proposed approach is better than the base approach in terms of parameters like packet delivery ratio, a number of packets sent, received and a minimum number of packets dropped. The approach can be applied in various optimization techniques.

REFERENCES

[1] P. Sharma, H.P. Sinha and A. Bindal, "A Review on Prevention of Wormhole Attack in Mobile Ad-hoc Network", *International Journal of Research in Information Technology*, Vol. 2, No. 3, pp. 303-308, 2014.

[2] S. Goyal and H. Rohil, "Securing MANET against Wormhole Attack using Neighbour Node Analysis", *International Journal of Computer Applications*, Vol. 81, No. 18, pp. 44-48, 2013.

[3] R. Maulik and N. Chaki, "A Comprehensive Review on Wormhole Attacks in MANET", *Proceeding of 9th International Conference on Computer Information Systems and Industrial Management Applications*, pp. 233-238 2010.

[4] Reshmi Maulik and Nabendu Chaki, "A Study on Wormhole Attacks in MANET", *International Journal of Computer Information Systems and Industrial Management Application*, Vol. 3, pp. 271-279, 2011.

[5] Saurabh Upadhyay and Brijesh Kumar Chaurasia, "Impact of Wormhole Attacks on MANETs", *International Journal of Computer Science and Emerging Technologies*, Vol. 2, No. 1, pp. 72-82, 2011.

[6] M. Azer, S. El-Kassas and M. El-Soudani, "A Full Image of the Wormhole Attacks towards Introducing Complex Wormhole Attacks in Wireless Ad Hoc Networks", *International Journal of Computer Science and Information Security*, Vol. 1, No. 1, pp. 41-52, 2009.

[7] Juhi Biswas, Ajay Gupta and Dayashankar Singh, "WADP: A Wormhole Attack Detection and Prevention Technique in MANET using Modified AODV routing Protocol", *Proceeding of 9th International Conference on Industrial and Information Systems*, pp. 1-6, 2014.

[8] T.V.P. Sundararajan, S.M. Ramesh, R. Maheswar and K.R. Deepak, "Biologically inspired Artificial Intrusion Detection System for Detecting Wormhole Attack in MANET", *Wireless Networks*, Vol. 20, No. 4, pp. 563-578, 2013.

[9] P. Anitha and M. Sivaganesh, "Detection and Prevention of Wormhole Attacks In Manets Using Path Tracing", *International Journal of Communications Networking System*, Vol. 1, No. 2, pp. 106-111, 2012

[10] Adel Saeed Alshamrani, "PTT: Packet Travel Time Algorithm in Mobile Ad-Hoc Networks", *Proceedings of IEEE Workshops of International Conference on Advanced Information Networking and Applications,* pp. 561-568, 2011.

[11] Mohammad Rafiqul Alam and King Sun Chan, "RTT-TC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET", *Proceedings of 12th IEEE International Conference on Communication Technology*, pp. 991-994, 2010.