ijecs open access www.ijecs.in

*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 3 Issue 10, October 2014 Page No. 8498-8501*

# Modified AODV for Detection and Recovery of Worm Hole Attack

**Aarushi, Mr. Harish Bedi**

Department of computer science and engineering, BRCM, Bahal, Bhiwani
Email:-aarushisharma19@gmail.com

Department of computer science and engineering, BRCM, Bahal, Bhiwani
Email:-hbedi@brcm.edu.in

## ABSTRACT

This paper studies the wormhole attack in the mobile adhoc network. This paper modifies the AODV routing protocol to detect and recover from the wormhole routing attack. The result analysis of modified AODV is done by varying the number of wormhole nodes. The result analysis is done by using the PDR and the end 2 end delay. The simulation results confirm the better performance of the modified AODV.

**Keywords:** MANET, Routing

## I. INTRODUCTION

MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an ―infrastructure less network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. [1].

Routing is one of the most vital mechanisms in the ad hoc networks. Improper and insecure routing mechanisms will not only degrade the performance of the ad hoc networks, but will also render such networks vulnerable to many security attacks. Most of the attacks is on the message, which is used to establish and maintain relationships between nodes in the networks. Attacks against the routing messages could be launched in many forms and may include all the characteristics described earlier. Information or messages could be deviated from the normal operation flow using modification, interception, interruption or fabrication attacks [2].

## II. WORMHOLE ATTACKS

In the wormhole attacks, a compromised node in the ad hoc networks colludes with external attacker to create a shortcut in the networks. By creating this shortcut, they could trick the source node to win in the route discovery process and later launch the interception attacks. Packets from these two connections to create the fastest route from source to the destination node. In addition, if the wormhole nodes consistently maintain the bogus routes, they could permanently deny other routes from being established. As a result, the intermediate nodes reside along that denied routes are unable to participate in the network operations.

### a. Wormholes And Its Variants

In wormhole attack, where two colluding nodes that are far apart are connected by a tunnel giving an illusion that they are neighbors. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there. By using this additional tunnel, these nodes are able to advertise that they have the shortest path through them. Once this link is established, the attackers may choose each other as multipoint relays (MPRs), which then lead to an exchange of some topology control (TC) messages and data packets through the wormhole tunnel. Since these MPRs forward flawed topology information, it results in spreading of incorrect topology information throughout the network . On receiving this false information, other nodes may send their messages through them for fast delivery. Thus, it prevents honest intermediate nodes from

establishing links between the source and the destination. Sometimes, due to this, even a wormhole attacker may fall victim to its own success. In , a particular type of wormhole attack known as "in-band wormhole attack" is identified. A game theoretic approach has been followed to detect intrusion in the network. Presence of a central authority is assumed for monitoring the network. This is a limitation in wireless scenario such as military or emergency rescue. In the wormhole attacks are classified as 1) In-band wormhole attack, which require a covert overlay over the existing wireless medium and 2) Out-of-band wormhole attack, which require a hardware channel to connect two colluding nodes. The in-band wormhole attacks are further divided in as 1.1) Self-sufficient wormhole attack, where the attack is limited to the colluding nodes and 1.2) Extended wormhole attack, where the attack is extended beyond the colluding nodes. The colluding nodes attack some of its neighboring nodes and attract all the traffic received by its neighbor to pass through them. In the second type of wormhole attacks , the intrusions are distinguished between a) hidden attack, where the network is unaware of the presence of malicious nodes and b) exposed attack, where the network is aware of the presence of nodes but cannot identify malicious nodes among them [2]

## III. ROUTING APPROACHES IN MOBILE AD HOC NETWORK

- In ad hoc mobile networks, routes are mainly multi hop because of the limited radio propagation range and topology changes frequently and unpredictably since each network host moves randomly. Therefore, routing is an integral part of ad hoc communications.
- Routing is to find and maintain routes between nodes in a dynamic topology with possibly uni-directional links, using minimum resources.

### i. Table-driven or Proactive Protocols

Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals. Representative proactive protocols include: Destination-Sequenced Distance- Vector (DSDV) routing, Clustered Gateway Switch Routing (CGSR), Wireless Routing Protocol (WRP), Optimized Link State Routing (OLSR)and*The Fisheye State Routing (FSR)*.

### ii. On-demand or Reactive Protocols

A different approach from table-driven routing is reactive or on- demand routing. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Representative reactive routing protocols include: Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) routing, Temporally Ordered Routing Algorithm (TORA) and Associativity Based Routing (ABR).

### iii. Hybrid Routing Protocols

Purely proactive or purely reactive protocols perform well in a limited region of network setting. However, the diverse applications of ad hoc networks across a wide range of operational conditions and network configuration pose a challenge for a single protocol to operate efficiently. Researcher's advocate that the issue of efficient operation over a wide range of conditions can be addressed best match these operational conditions [4]. Representative hybrid routing protocols include: Zone Routing Protocol (ZRP) and Zone-based Hierarchal Link state routing protocol (ZHLS) [3]**.**

## IV. AD-HOC ON DEMAND DISTANCE VECTOR PROTOCOL

Ad-hoc On Demand Distance Vector (AODV) is a reactive protocol that reacts on demand. It is probably the most well-known protocol in MANET. It is a modification of DSDV. The demand on available bandwidth is significantly less than other proactive protocols as AODV does not require global periodic advertisements. It enables multi-hop, self-starting and dynamic routing in MANETs. In networks with large number of mobile nodes AODV is very efficient as it relies on dynamically establishing route table entries at intermediate nodes. AODV never produces loops as there cannot be any loop in the routing table of any node because of the concept of sequence number counter borrowed from DSDV. Sequence numbers serve as time stamps and allow nodes to compare how fresh information they have for other nodes in the network. The main advantage of AODV is its least congested route instead of the shortest path[5].

Routing information is stored in source node and destination node, intermediate nodes dealing with data transmission. This Approach reduces the memory overhead, minimize of the network resources, and runs well in high mobility scenario. The communication between nodes involves main three procedures known as path discovery, Path establishment and path maintenance. Three types of control messages are used to run the algorithm, i.e. Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). The format of RREQ and RREP packet are shown in Table 1 and Table 2.

**Table 1: RREQ Field**

| Source Address | Source Sequence | Broadcast Id | Destination Address | Destination sequence | Hop Count |
|---|---|---|---|---|---|
| | | | | | |

**Table 2: RREQ Field**

| Source Address | Destination Address | Destination sequence | Hop Count | Lifetime |
|---|---|---|---|---|
| | | | | |

When the source node wants to send some data to the destination node, Source will issue the route discovery procedure. The source node will broadcast route request packets to all its accessible neighbors'. The intermediate

node receiving request (RREQ) will check the request whether he is destination or not. If the intermediate node is the destination node, will reply with a route reply message (RREP). If not the destination node, the request will be forwarded to other neighbor nodes. Before forwarding the packet, each node stores the broadcast identifier and the node number from which the request came. Timer is used by the intermediate nodes to delete any entry when no reply is received for the request. The broadcast identifier, source ID are used to detect whether the node has received the route request message previously or not. It prevent from the redundant request receiving in same nodes. The source node may receive more than one reply, in that case it will determine later which message will be selected on the basis of hop counts. When any link breaks down due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable because of loss of the link. Then it will create a route error (RERR) message. The node sends the RERR upstream to the source node. When the source receives the Route reply message, it may reinitiate route discovery if it still requires the route [6].

## V. Operation of Wormhole Attack in AODV

Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. Even if, the routing information is confidential, encrypted or authenticated, it can be very effective and damaging. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It may badly disrupt communication as AODV would be unable to find routes longer than one or two hops. It is easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route for tunneled distances longer than the typical transmission range of a single hop. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets.

Wormhole attack commonly involves two remote malicious nodes shown as X and Y in Figure 1. X and Y both are connected via a wormhole link and they target to attack the source node S. During path discovery process, S broadcasts RREQ to a destination node D. Thus, A and C, neighbors of S, receive RREQ and forward RREQ to their neighbors. Now the malicious node X that receives RREQ forwarded by A. It records and tunnels the RREQ via the high-speed wormhole link to its partner Y. Malicious node Y forwards RREQ to its neighbor B. Finally, B forwards it to destination D. Thus, RREQ is forwarded via S -A-X-YB-D. On the other hand, other RREQ packet is also forwarded through the path S-C-D-E-F-G-D. However, as X and Y are connected via a high speed bus, RREQ from S-A-X-Y-B-D reaches fist to D. Therefore, destination D ignores the RREQ that reaches later and chooses D-B-A-S to unicast an RREP packet to the source node S. As a result, S chooses S-A-B-D route to send data that indeed passes through X and Y malicious nodes that are very well placed compared to other nodes in the network. Thus, a wormhole attack is not that difficult to set up, but still can be immensely harmful for a MANET. Moreover, finding better techniques for detection of wormhole attacks and securing AODV against them still remains a big challenge in Mobile Ad-hoc Networks [5].

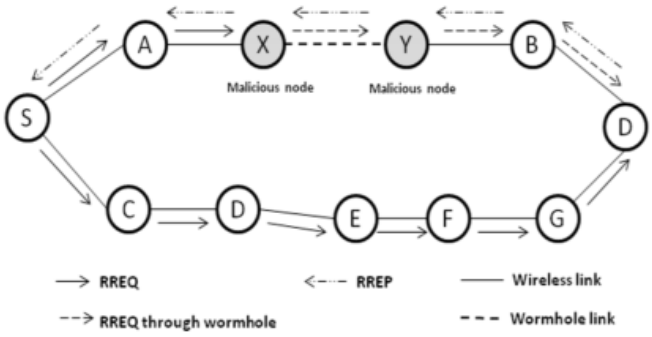


**Figure 1: Wormhole attack on AODV in MANET**

## VI. PROPOSED WORK

Here, a network with n nodes is given. Route[] is an array contains the nodes in the path from source node to destination node. Therec[] is the array denotes number of packets received at particular node in the network and similarly send[] represents number of packets forwarded to the other nodes. h is the number of hops in the route from the source to destination. source is the source and destination is the destination.

```
i.    For I =1 to h
ii.    If route[i]==source || route[i]==destination
iii.  Forwardingratio[i]=0
iv.    else
v.    Forwardingratio[i]= send[route[i]/ recv[route[i]
vi.    End if
vii.  end
viii.       Max=forwarding ratio[1]
ix.   Nodepostion=1
x.    For i=2:h
xi.          If forwardingratio[i]>Max
xii.  NodePosition=i
xiii.   End if
xiv.  End
xv.   Wormhole_node=max[Nodeposition]
```

## VII. RESULTS

**Parameter Analysis**

- **Packet Delivery Ratio (PDR)**

The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

∑ Number of packet receive / ∑ Number of packet send

- **End-to-end Delay**

The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections

**Table1 : Analysis Parameters Of Existing Algorithm**

| Nodes | PDR | E2E Delay |
|---|---|---|
| Pr1 | 18.8492 | 19.2535 |
| Pr2 | 18.8492 | 19.2535 |
| Pr3 | 18.8492 | 19.2535 |

**Table 2: Analysis Parameters OfProposed Algorithm**

| Nodes | PDR | E2E Delay |
|---|---|---|
| Pr1 | 29.9413 | 15.6795 |
| Pr2 | 31.1396 | 14.6528 |
| Pr3 | 28.9116 | 14.1250 |

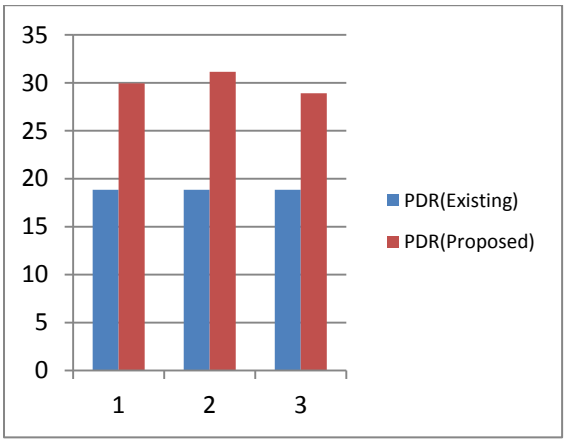


**Figure 2: Comparison of PDR between Existing And Proposed**

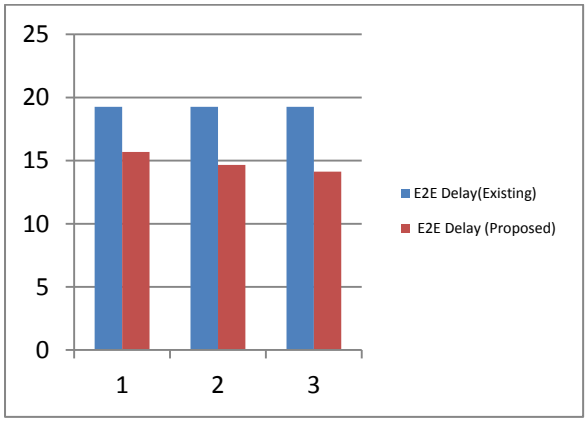


**Figure 2: Comparison of E2E Delay between Existing And Proposed**

## Conclusion

The paper shows that the modified AODV is better as compared to the existing AODV. The performance is better due to the detection and recovery of the wormhole attack. The existing AODV shows the same performance by varying the number of wormhole nodes. While the performance of proposed AODV is better than the existing in terms of the PDR. In future it can be extended to other types of attack detection and recovery.

## REFERENCES


[1] Goyal, Priyanka, VintiParmar, and Rahul Rishi. "Manet: vulnerabilities, challenges, attacks, application." *IJCEM International Journal of Computational Engineering & Management* 11 (2011): 32-37.

[2] Faisal, Mohd, M. Kumar, and Ahsan Ahmed. "ATTACKS IN MANET." IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[3] PandaIpsita*" A Survey on Routing Protocols of MANETs by Using QoS Metrics"*International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[4] M.S. Corson, J.P. Maker, J.H. Cernicione, Internet-based mobile ad hoc networking, IEEE Internet Computing 3 (4) (1999) 63–70.

[5] Jhaveri, Rutvij H., Ashish D. Patel, Jatin D. Parmar, and Bhavin I. Shah. "MANET routing protocols and wormhole attack against AODV." International Journal of Computer Science and Network Security 10, no. 4 (2010): 12-18.

[6] Achint Gupta, Dr, PriyankaVj, And SaurabhUpadhyay. "Analysis of Wormhole Attack in AODV based MANET Using OPNET Simulator." International Journal 1, no. 2 (2012).