A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks

A.VANI

Assistant Professor, ECE Department, CBIT,
Hyderabad, Andhra Pradesh, INDIA
vanialamur@yahoo.in

D.Sreenivasa Rao

Professor, ECE Department, JNTUniversity,
Hyderabad,Andhrapradesh,INDIA
dsraoece@yahoo.co.uk

Abstract—The infrastructure of a Mobile Ad hoc Network (MANET) has no routers for routing, and all nodes must share the same routing protocol to assist each other when transmitting messages. However, almost all common routing protocols at present consider performance as first priority, and have little defense capability against the malicious nodes. Many researches have proposed various protocols of higher safety to defend against attacks; however, each has specific defense objects, and is unable to defend against particular attacks. Of all the types of attacks, the wormhole attack poses the greatest threat and is very difficult to prevent; therefore, this paper focuses on the wormhole attack, by combing three techniques. So that our proposed scheme has three techniques based on hop count, decision anomaly, neighbor list count methods are combined to detect and isolate wormhole attacks in ad hoc networks. That manages how the nodes are going to behave and which to route the packets in secured way.

Keywords: AODV, MANET, Secure routing, Wormhole attack.

I.INTRODUCTION

In all possible methods of attacks in Mobile Ad hoc Networks (MANETs), the wormhole attack is one of the most threatening and hazardous attacks. A wormhole attack is usually performed by two or more malicious nodes in conspiracy. Two malicious nodes at different locations send received routing messages to each other via a secrete channel. In this way, although the two malicious nodes are located far from each other, they appear to be within one-hop communication range. Therefore, the route passing through the malicious nodes is very likely to be shorter than any other regular one. Wormhole nodes can easily grab the route from the source node to the destination node, and then sniff, drop, or selective-drop data packets passed by. The wormhole attack can be launched regardless of the MAC, routing, or cryptographic protocols used in the network and is thus difficult to defend against. Defense mechanisms against this attack are either very complex or very expensive. Most of the wormhole defense mechanisms aim to detect wormholes successfully with minimal false positives. Unfortunately, the defense schemes ignore the removal of the links created by the wormhole. We note that a single two-end wormhole could be thought of logically as a single link. In reality, the wormhole creates a large number of links between many nodes in the network. The nodes will not be aware of this fact and will be using the wormhole links as legal links. Wormhole nodes can successfully execute such attacks without compromising any computer, and are unavoidable, even though some MANETs provide authenticity and confidentiality protection.

In a wormhole attack, malicious node m1 first captures routing message from a neighboring node, and then sends the message to another malicious node, m2, by means of a secret tunnel, m2 then broadcasts or propagates the message received. In this way, a tunnel-like channel is formed between the two malicious nodes. Even though the tunnel has a very long distance, other normal nodes may mistakenly think that there is only a distance of a one-hop count. The tunnel-like channel can be realized by two methods [8]: packets encapsulated channel and out-of-band channel, as shown in Fig.1 (a) and (b), respectively. Packets encapsulated channel is also called in-band channel, where a malicious node puts a captured routing message in a data packet payload, and uses normal nodes to transmit the data packet to another malicious node. The malicious node receiving the

data packet draws the routing message out of the packet payload and further broadcasts or propagates it. In this way, the hop count is reduced to increase the chance of grabbing a route, and as no field information is changed, neither Secure AODV (SAODV) [2], which can protect routing messages, nor Authenticated Routing for Ad hoc Networks (ARAN)[3], which can authenticate each neighbor, have any way of defending against attacks from a encapsulated channel. As shown in Fig.1 (a), a path is built in advance between the two malicious nodes, m1 and m2, and s is the source node and d is the destination node. When s broadcasts a Route Request (RREQ), it would be received by malicious node m1, and then m1 encapsulates the RREQ into the payload of a data packet, and transmits it using the pre-built path between m1 and m2. After receiving the data packet, m2 would extract the original RREQ and broadcast it till it reaches the destination node. As the path passing through the malicious nodes saves 4 hop counts on the surface and thus is shorter than the other two paths, node d would finally choose the path to respond a Route Reply (RREP). In this way, the malicious nodes would deprive the route of passing data packets. The method of an out-of- band channel differs from encapsulating packet mainly in the type of tunnel-like channel. A special channel may be a connection by a wired network between the two malicious nodes, or a private channel between the two ends using a high-powered transmission to send signals over a long distance, as shown in Fig. 1(b).

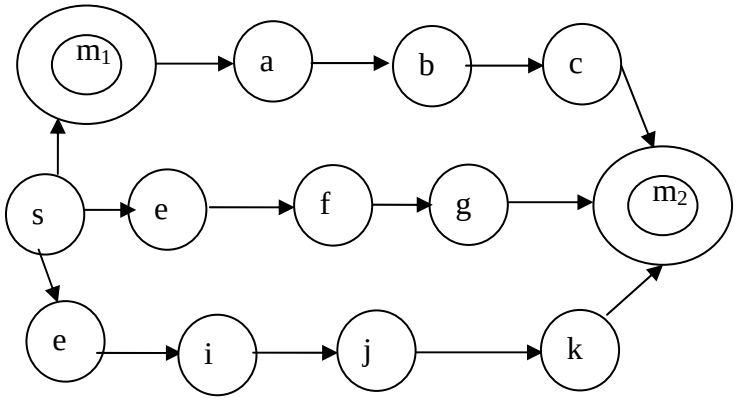


Fig: 1. (a) Packets encapsulated channel

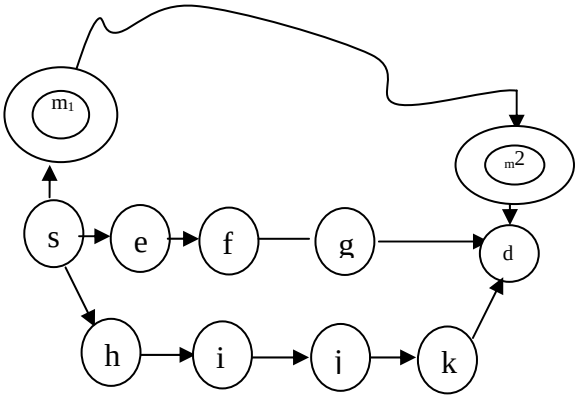


Fig: 1. (b) out-of-bandchannel

Impacts of wormhole attacks: If the wormhole will only peacefully transport all the traffic from one location in the network to another location that is far away, then it could be useful for the network operation as it will improve the network connectivity. Unfortunately, once the traffic is routed through the wormhole, the attacker will gain full control over the traffic. Then he can start his malicious actions by selectively dropping data packets which will lower the network throughput or store all the traffic and later perform cryptanalysis attacks. The attacker can decide when to drop data packets that pass through the wormhole at some critical situations. For example, if the network is used for some alarm or surveillance system, then the attacker can decide to time his packet dropping with a planned intrusion into the system. The wormhole attack was shown to have significant impact on both proactive and reactive ad hoc routing protocols.

Wormhole detection using hop count is based routing discrepancies between neighboring nodes along a path from a source to the destination to detect wormhole attacks. Worm hole diction and removal using route reply-decision-packet uses secure routing protocol to defend against wormhole attacks based on the Ad hoc On-demand Distance Vector (AODV) routing protocol [4],which is named WARDP (Wormhole-Avoidance Route reply decision packet)). WARDP considers link-disjoint multipaths during path discovery in order to choose a safer path to avoid wormhole nodes. And finally, neighbor list method is used for detection and removal of worm hole attack in this using the neighboring nodes exchange their neighbor lists. Each node will compare its neighbor list with its neighbors' neighbor list. If they are similar, either these nodes are close enough or are connected by a wormhole. Next, both of these nodes and their neighbors will reconstruct their neighbor lists which will remove these two nodes and their neighbors.

The remainder of this paper is organized as follows. Section 2 provides a brief review on previous work against wormhole attacks. Section 3 describes the details of the proposed hybrid routing algorithm for detection and removal of wormhole attacks. Section 4 is the outcomes and analysis of ns2 simulation. Section 5 offers conclusions.

II. RELATED WORK

Since proposed Hybrid routing is used to detect and remove wormhole attack at physical layer using hop count [alternate route] and modification of AODV protocol using route reply decision and finally we using secure

neighbor discovery using neighbor list method. These three methods are combined to obtain the command solution which is for better then individual methods. These hybrid routing is based on ON-Demand ad hoc routing protocol (AODV). Different methods used to detect and eliminate the wormhole attacks are briefly reviewed.

The methods proposed in literature to defend against wormhole attacks can be divided into three categories. The first is to modify a well-known routing protocol, such as Ad hoc On demand Distance Vector (AODV)[4] or Dynamic Source Routing (DSR) [5], to avoid wormhole nodes during path discovery, such as [3,4,5,6,7].The second is to adopt extra hardware, such as a positioning system, a time synchronization mechanism or a directed antenna, in addition to modifying the routing protocol. Some of which are [8, 9, 11, 12, 13]. Finally, the third is to deploy an intrusion detection system (IDS) with or without hardware support, such as [14, 15, 10, and 16]. Since the proposed approach in this paper is a secure routing protocol without hardware support, only those researches belonging to the first category are introduced as follows.

Wormhole attack detection in [3] proposed a modified DSR [2] protocol to defend against wormhole nodes by adopting a multi-path routing method. A source node initiates route discovery, and the destination node, after receiving multiple paths, begins to calculate the proportion of each link between two nodes in the total paths. Due to wormhole node's great ability to grab routing paths, if the occurrence of one link exceeds the threshold value, the two ends of this link may be wormhole nodes. The destination would first send a test data packet to verify if this link is abnormal, such as the packet being dropped. If it is confirmed that the two ends of this link are wormhole nodes, the destination would send a warning message to the neighbors of the malicious nodes, informing them not to process any messages from the malicious nodes. In this way, the malicious nodes would be isolated, and then Quarantine. An AODV-based routing protocol proposed [4], named DelPHI, to defend against wormhole attacks. DelPHI also applied a multi-path approach, and recorded the delay and hop counts in transmitting RREQ and RREP (actually named DREQ and DREP in Delphi) through the paths. In this way, the average time taken by each hop can be calculated. In the case of a path subjected to wormhole attacks, the delay would be obviously longer than a normal path with the same hop count (i.e., the wormhole nodes may have a heavy load, and therefore, packet processing is slow).Hence, the path with longer delays would not be selected to transmit data packet and wormhole nodes could be avoided.

A proposed scheme in which each node must broadcast messages that can be transmitted over 2 hops [5]. Each node records the neighboring list of 1 hop and 2 hops, as well as the corresponding session keys. When a node received a routing message without a valid Message Authentication Code (MAC), there may be wormhole attacks. The purpose of maintaining a 2 hops neighboring list by each node is to allow the node to recognize if a wormhole attack is a hidden wormhole attack or an exposed wormhole attack, as wormhole nodes may reveal themselves or hide themselves in a routing path. The former is an exposed wormhole attack, while the latter is hidden [5] A proposed a routing protocol to alleviate wormhole attacks [6]. This protocol is a modification of the Ariadne [17] routing protocol, and can only defend against in-band (or packets encapsulated) channels of wormhole attacks. Their method calculates the average time in transmitting RREQ through normal nodes, so that a normal node can distinguish a particularly long duration in transmitting an RREQ when malicious nodes executing in-band wormhole attacks. The protocol [7] used four message exchanges to defend against wormhole attacks in the Optimized Link State Protocol (OLSR) [18] based routing protocol, as wormhole nodes should process a large amount of packets, causing longer delays of packets than in normal nodes. The authors mainly used Hello and ACK messages as the messages to confirm the delay.

III. PROPSED ROUTING ALGORITHM

Hybrid routing algorithm is used to provide the common solution to three different techniques. This protocol is based on On-demand ad hoc routing protocol (AODV).Brief description of three different techniques.

A.Hop Count Based Detection (Alternate Route).

Wormhole attack generally affects the routing at network layer. It also degrades the security services at the physical layer. This technique is used to detect and isolate the wormhole attack at physical layer.

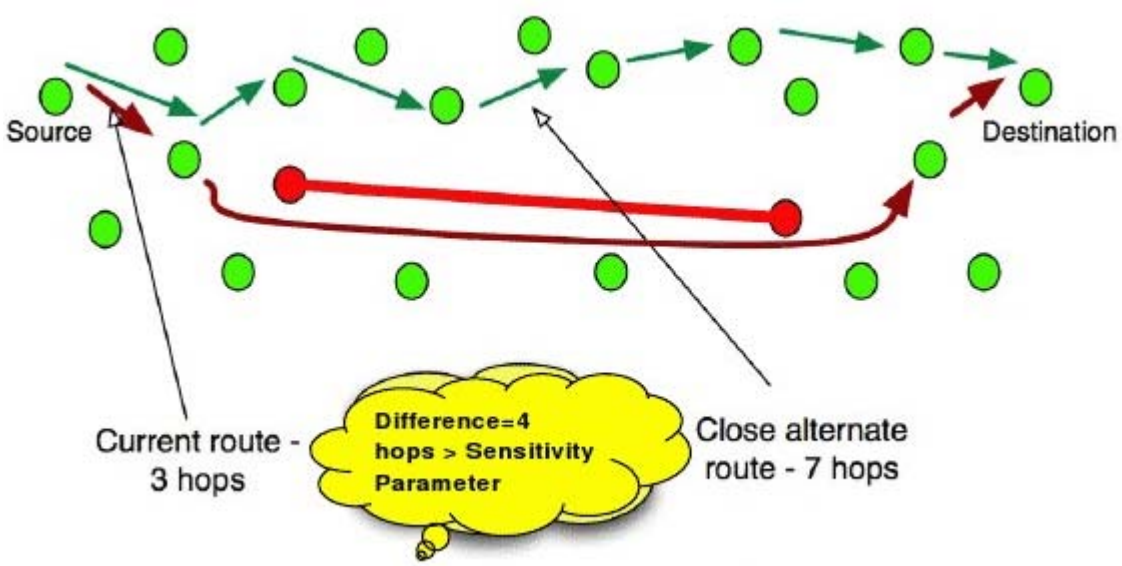


Fig: 2.Illustration of Detection of worm hole [example]

The sender node S in Figure 2 will initially have a route to the destination node D and wishes to test whether this route includes a wormhole or not. Detecting such wormholes is considered to be extremely difficult The sender S will start by discovering his one-hop neighbors. Based on the received replies, he will create a list of his one-hop neighbors that excludes the next hop along the route. The sender will check the routes (we call these the test routes) that are used by these one-hop neighbors to the second hop along the route to the destination (throughout this technique we will refer to this node as the target node). Node S compares the length of a selected route with the one he has to the target node. The selected route is chosen from the routes reported from the neighbors. If the difference between the numbers of hops of the two routes is greater than a certain value called the \Threshold value", the sender will assume that a wormhole exists. If not, this process is repeated by each node that lies on the route (such nodes also exclude the previous hop from the list). The idea is that when a node that is close to M1 is reached, its next hop neighbor along the route will be on the other side of the wormhole link (near M2)[the link in dark red color connected between two nodes called as M1 and M2]. If at least one of the \perceived" one-hop neighbors is located within the transmission range of the node, (i.e., it is not on the other side of the wormhole), the route from this neighbor to the target node can be rendered very different (typically long) and thus the wormhole will be detected.

B. Anomaly Based Detection (Route Reply Decision Packet)

The principle of WARRDP is to allow neighboring nodes of a wormhole node to notice that the wormhole node ha extreme capacity of competition in path discovery. In the path discovery of WARRDP, an intermediate node will attempt to create a route that does not go through a hot neighbor node, which has a route-building rate higher than the threshold. Thus, not only are wormhole nodes gradually identified and isolated by their normal neighboring nodes.

C. Neighbor List Based Detection

In this method secure neighbor discovery from source to destination obtained by neighbor list and detect the anomaly if attack is present. The steps are

- One-hop neighbor discovery;
- Initial route discovery
- Data dissemination and wormhole detection, and
- Secure route discovery against a wormhole attack.

Each node sends a hello message for the neighbor discovery immediately after the deployment of the mobile nodes. Each node that receives a hello message sends a reply. Each node builds its neighbor list which could include remote neighbors connected by a wormhole. The neighboring nodes exchange their neighbor lists. Each node will compare its neighbor list with its neighbors' neighbor list. If they are similar, either these nodes are close enough or are connected by a wormhole. Next, both of these nodes and their neighbors will reconstruct their neighbor lists which will remove these two nodes and their neighbors. Finally, to secure the data

dissemination between neighbors, we build a pair-wise shared key using the initial key KI and random function f.

Algorithm Steps

1. Whenever a source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcast RREQ packets through neighboring nodes. RREQ packet contains destination address and sequence number along with source address. Sequence number provides the freshness of route.
2. Once an RREQ packet is received by an intermediate node and verifies destination address. If the destination address not matches with the RREQ packet then forwards it to its next hop. This process is repeated until it reaches the final destination.
3. While receiving the RREQ packet each node update their routing table
4. Once the destination node receives RREQ message from neighboring nodes, it then unicasts the RREP (route_reply) back to the source node.
5. RREP contains route reply count (rrep_count) and neighbor lists NL_d
6. As the RREP propagates, each intermediate node creates a route to the destination
7. Each forwarding intermediate nodes increment rrep_count.
8. When the source receives the RREP, it records the route to the destination.
9. It records the destination neighbor list (NL_d) and hop count between source and destination (hop_count)
10. Each node in the path first selects the second hop node as target node.
11. To check the Neighbor list verification go **to step 19**
12. Once source receives RREP message it will send additional message of route reply decision packet (RREP_DEC) to destination. Route Decision packet confirm the particular node that it is participating in the route from source to destination.
13. It contains source neighbor list NL_s and rrep_dec_count.
14. Each forwarding node along the route between source and destination forwards RREP_DEC message and increment rrep_dec_count by 1
15. Each node in the path selects the second hop node as target node
16. To check the hop_count verification go to step 26
17. Destination stores neighbor list NL_s entry sent by source
18. To check the Neighbor list verification go to step 19

//neighbor list detection method

19. Source node neighbor list stored in NL_S
20. Source node neighbor list stored in NL_d
21. Compare both neighbor list and calculate the number of common neighbor nodes (common_node) present between sources to destination.

```
For i=0;i<number_of_source_neighbors;i++
For j=0;j< number_of_destination_neighbors;j++
        If (NLS(i) =NLD(J))
                Common _node++;
```

22. While receiving the RREP from destination it stores the hop count (hop_count) between source and destination. The number of hops from the sender IP Address to the node handling the request
23. The hop count between two nodes means the minimum number of hop-by-hop transmissions to reach one node to another.
24. Depends on the hop_count value fix threshold value for nbr_thresh
25. Number of common neighbors between source and destination exceeds the nbr_thresh (Common _node > nbr_thresh) wormhole may present among the path.
26. Go to step 46

//hop_count detection method

27. Each node sends hop detect message to all of its neighbors. It contains the target node id.
28. Hop count between the selected node in the path and the target node (target_hop_count) is 2. Selected node justifies the target_hop_count between their neighbor node to the target node.
29. One hop neighbor finds the target_hop_count by checking target node entry in the routing table.
30. If target node id is not present in the routing table it will send the RREQ message to neighbors and find the target_hop_count between the target node.

31. In normal scenario one hop neighbors can reach target node with maximum of 3hop and minimum of 1 hop. If maximum target_hop_count exceeds 3 then target node and their previous hop may be the worm hole node. So we fix the threshold for the target_hop_count as hop_count_thresh. This threshold value range from 3 to 6. By applying Minimum threshold value, all the wormhole nodes are detected but in some cases false positives may occur. For maximum Threshold false positive may reduced some of the wormhole node may not be identified. So we have to choose the proper hop_count_thresh depends on the environment.
32. If **target_hop_count > hop_count_thresh** we declare the target node and their previous hop nodes are wormhole nodes.
33. Go to step 46
//**Anomaly Detection Method**

34. Each Node sends Hello message to its entire neighbor periodically to ensure the neighbors presence. We create an additional field Anomaly_value which holds the node anomaly value.
35. Anomaly value of a node is defined as its presence in different route from source to destination
36. Anomaly value depends on the no of source and destination pairs present in the network.
37. Each node calculate their anomaly value by using the formula
Anomaly_ value = rrep_dec_count/(rrep_count+1).
38. Each Node receives Hello message it checks the anomaly values of the neighbor.
39. Initially anomaly value is zero at each node. It needs some time gap to update their anomaly values.
40. Anomaly values varies from ½,2/3,3/4,… depends on the number of sending RREP_DEC messages and number of RREP messages.
41. The anomaly threshold value should be less than 1 always.
42. So we fixed threshold for Anomaly_value as anomaly_thresh=1
43.If any wormhole node presents it grab messages on route and accumulate the anomaly values. For the wormhole node anomaly value is high.
44.If any neighbor node has high anomaly value (**Anomaly_value > anomaly_thresh**), that would be a wormhole node.
45. Go to step 46
//Wormhole Isolation
46. Send worm_annoucement message to all nodes
47. Any node receives worm_annoucement message it removes wormhole node id from its neighbor table and Routing Table.
48. If any forwarding node receives worm_announcement message it will send RERR message to source. It will reinitiate route discovery process, and find the new path to the destination without worm hole node.

IV.SIMULATION RESULTS

Simulation can be performed in terms of Avg End-to-End delay, routing over head, Packet delivery ratio

A. Simulation Parameters

Table1: Simulation parameters

parameter	value
Simulator	NS-2[ver 2.32]
Simulation time	300s
No. of nodes	150
Routing protocol	AODV
Traffic model	CBR
Pause time	2(s)
Terrain area	600m x 600m
Transmission range	250m

B. Simulation Performance Metrics

The simulation was done to analyze the performance of the networks for various parameters. Different metrics are used to evaluate the performance of the network under black hole attack.

1).
a) Packet Delivery Ratio: The ratio of the data packet sent from source to destination.

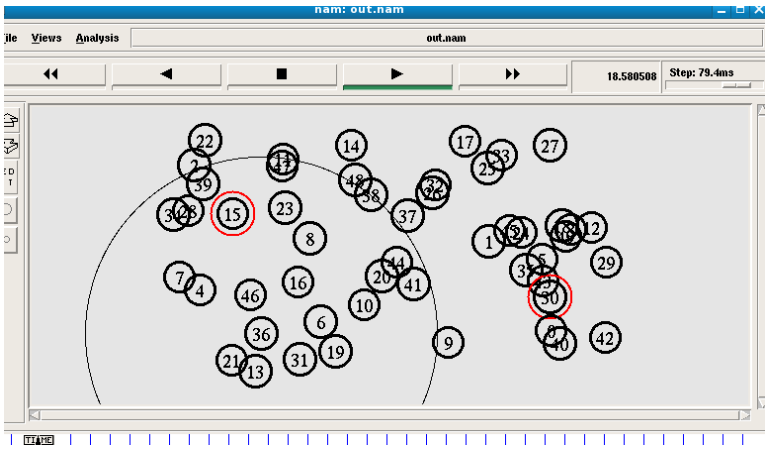
b). Average End-to End Delay: It is the time taken for the packet to reach from source to destination.

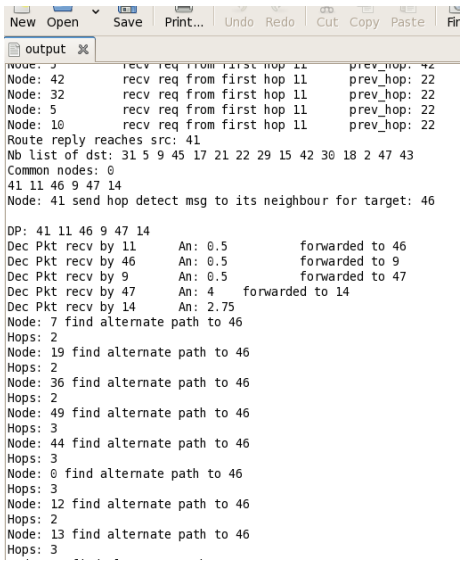
c). Normalized Routing Overhead: This gives the ratio of routing related transmissions. (RREQ, RREP, RERR) to data transmission in a simulation.

*C. **Simulation Results:***

SNo:	NO. of Nodes	PDR	Throughput	Routing Overhead	Avg End-to-End delay
1	20	99.24454	0.151210	55	0.155677
2	40	99.45669	0.163654	56	0.167654
3	60	99.46890	0.178987	57	0.170231
4	80	99.58356	0.189655	58	0.169968
5	100	99.86567	0.197821	58	0.16747

*D4**. Simulation Screenshots***





V.CONCLUSION

In this study we analyzed the effects of wormhole attack in ad hoc wireless networks. We implemented an AODV protocol that simulates the behavior of wormhole attack in NS-2.In this method we have used very simple and effective way of providing security in AODV routing protocol against wormhole attack that causes the interception and confidentiality of the ad hoc wireless networks. Security against wormhole attack is provided by using a simple wormhole algorithm. This algorithm has better performance comparing to three

individual methods [Hop count, Anomaly based, Neighbor list methods].The solution detects the malicious nodes and isolates it from the active data forwarding. As from the results we can easily infer that the performance of the normal AODV drops under the presence of worm hole attack.

References

[1] Perkins CE, Royer EM, Das SR. Ad hoc on-demand distance vector (AODV) routing, IETF internet draft. MANET Working Group;

[2] Johnson DB, Maltz DA, Hu YC. The dynamic source routing protocol for mobile ad-hoc network (DSR), IETF internet draft (work in progress); July 2004.

[3] Ning Song, Lijun Qian, and Xiangfang Li. Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach. In the proceedings of the 19th IEEE international parallel and distributed processing symposium (IPDPS'05); 2005.

[4] Hon Sun Chiu, King-Shan Lui. DelPHI: wormhole detection mechanism for ad hoc wireless networks. In the proceedings of the 1st international symposium on wireless pervasive computing; 2006.

[5] Gunhee Lee, Dong-kyoo Kim, Jungtaek Seo, An approach to mitigate wormhole attack in wireless ad hoc networks. In the proceedings of the international conference on information security and assurance; 2008 pp. 220-5.

[6] Xu Su and Rajendra V. Boppana. On mitigating in-band wormhole attacks in mobile ad hoc networks. In the proceedings of the IEEE international conference on communications; 2007. pp. 1136–41.

[7] Farid Naıt-Abdesselam, Brahim Bensaou, Jinkyu Yoo. Detecting and avoiding wormhole attacks in optimized link state routing protocol. In the proceedings of the IEEE conference on wireless communications and networking; 2007. pp. 3117–22.

[8] Issa Khalil, Saurabh Bagchi, Ness B. Shroff. LITEWORP: a Lightweight countermeasure for the wormhole attack in multihop wireless networks. In the proceedings of the international conference on dependable systems and networks (DSN'05); 2005.

[9] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff. MOBIWORP: mitigation of the wormhole attack in mobile multihop wireless networks. In the IEEE securecomm and workshops; 2006. pp. 1–12

[10] Xia Wang, Intrusion detection techniques in wireless ad hoc networks. In the proceedings of the IEEE international computer software and applications conference; 2006

[11] Xia Wang and Johnny Wong, An end-to-end detection of wormhole attack in wireless ad-hoc networks. In the proceedings of the 31st annual international computer software and applications conference (COMPSAC); 2007.

[12] Hu Yih-Chnu, Perrig Adrian, Jonhson David B. Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communication 2006; 24(2):370–80.

[13] Lazos L, Poovendran R, Meadows C, Syverson P, Chang LW. Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach. In the proceedings of the IEEE conference on wireless communications and networking; 2005, vol. 2. pp. 1193–9.

[14] Gorlatova MA, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano. Detecting wormhole attacks in mobile ad hoc networks through protocol breaking and packet timing analysis. In the proceedings of the IEEE conference on military communications; 2006.

[15] Marianne A. Azer, Sherif M. El-Kassas, Abdel Wahab F, Magdy S. El-Soundani. Intrusion detection for wormhole attacks in ad hoc networks a survey and a proposed decentralized scheme. In the proceedings of the IEEE international conference on availability, reliability and security; 2008. pp. 636–41.

[16] Tran Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee. Transmission time-based mechanism to detect wormhole attacks. In the proceedings of the IEEE Asia-Pacific service computing conference; 2007. pp. 172–8

[17] Hu YC, Perrig A, Davic B. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. In the proceedings of the ACM conference on mobile computing and networking (Mobicom); 2002. pp. 12–23

[18] Clausen T, Jacquet P. Optimized link state routing protocol (OLSR). 3626. IETF RFC; October 2003.