WAD-HLA: Wormhole Attack Detection Using Hop Latency And Adjoining Node Analysis In MANET

Vandana C. P
Scholar, Department of Information Science & Engineering, Oxford College of Engineering, Bangalore, India

Dr. A. Francis Saviour Devaraj
Professor, Department of Information Science & Engineering, Oxford College of Engineering, Bangalore, India

Abstract

Mobile Adhoc Networks (MANET) are vulnerable to both active and passive attacks at all the layers of network reference model. Wormhole attack is a routing attack, targeting the network layer resulting in complete disruption of the communication path in MANET. In this paper, a novel approach WAD-HLA:Wormhole Attack Detection using Hop latency and Adjoining node analysis in MANET, is proposed to detect wormhole attack launched in Adhoc On Demand Distance Vector (AODV) routing protocol based MANET. The proposed approach is based on per hop latency determination and adjoining node (intermediate node) detection techniques. The effectiveness of the proposed mechanism is evaluated using ns2 network simulator.

***Index Terms*— MANET, AODV, Tunnel, Round Trip Time, detection rate, adjoining node.**

1. Introduction

A Mobile adhoc network (MANET) [1] is a dynamic collection of mobile hosts with a decentralized, ad-hoc topology without any fixed infrastructure. Due to the open nature of the wireless medium, MANET is subjected to both active and passive attacks [2]. Among the security attacks in MANET, routing attacks launched at network layer is critical. Wormhole attack [3] is one such routing attack where the replay attack is launched at network layer.

In wormhole attack the malicious nodes or wormhole peers establish a wormhole link or tunnel through which the packets are replayed to another region in the network disrupting the communication channel, corrupting the routing protocol and adversely affecting the localization based systems. These wormhole tunnels cause the routing protocols to include them in the discovered route. After successful establishment of wormhole tunnel, wormhole peers can sniff, modify, drop or selective-forward/drop the data packets passing through them.

A wormhole tunnel is normally established by any two malicious nodes (generally at distant location) which collude together to create an illusion of one hop neighbors (adjoining nodes), causing the routing of packets to happen through them. Wormhole tunnels are established using several mechanisms like packet encapsulation, high quality/out-of-band communication channel, and high power transmission capability. Since the malicious nodes are replaying the packets, it is not a trivial job to detect the wormhole attack in routing protocols in MANET.

Adhoc On Demand Distance Vector [4] (AODV), an on demand routing protocol used in MANET is subjected to wormhole attack during the route discovery phase. Wormhole attack is launched by the colluding nodes by creating a tunnel, emulating as one hop neighbor, hence causing the Route Request (RREQ) during route discovery phase to reach the destination at a faster rate(or low hop count) compared to normal path. Destination node discards all the later RREQ packets received, even though they are from authenticated node. Destination node chooses the wormhole tunnel infected path to send the Route Reply (RREP) leading to the inclusion of wormhole tunnel in the data route. Once the data route is established through the wormhole tunnel, wormhole peers can drop, modify or selectively forward the data packets.

Evaluation of impact of wormhole attack on AODV [5] depicts that the various network parameters like network throughput, average end to end delay, packet drop ratio and drop rate are adversely affected by the presence of wormhole tunnels in the network. Hence it is particularly important to detect wormhole attack in MANET.

This paper aims at proposing an efficient approach to detect wormhole attack launched in AODV based MANET. Rest of the paper is organized as follows: Section 2 reviews the related work done; Section 3 explains the proposed approach, WAD-HLA to detect the wormhole attack in AODV, Section 4 describes the implementation details, followed by result analysis and Section 5 is conclusion and future work.

2. Related Work

Various wormhole attack detection mechanisms have been proposed. In wormhole attack detection mechanism [6], the fact that the transmission time between two wormhole nodes is much longer than that between two legitimate neighbours which are close together is considered. Round trip time (RTT) is used as a metric to compute transmission time. But detection based solely on transmission time, can lead to high false positive rate since the link latency may go exceptionally high due to congestion in certain cases.

In Delphi (Delay Per Hop Indicator) [7] every possible disjoint path between sender and receiver is computed. Delay per Hop value is used to detect wormhole attack. WORMEROS [8] technique considers round trip time between source node and destination node for detecting wormhole link based on high latency.

In MOBIWORP [9] neighbour discovery process confirms the presence of wormhole attack. In statistical approach SAM [10] (Statistical Analysis of Multi-path) relative frequency of each link appearance in a set in multi-path routing is considered for detection of wormhole attack.

3. Proposed Wormhole Attack Detection Scheme: WAD-HLA

3.1 Threat Model

This section describes the system model, scope of threat, and the assumptions considered in WAD-HLA. In our simulation model, wormhole attack is launched or simulated by using the approach of encapsulating the packets in AODV routing protocol. All the packets are encapsulated/decapsulated by the wormhole peers W1 and W2 respectively as shown in Figure.1 creating a wormhole tunnel or link. Through this approach, the wormhole peers create an illusion of low hop count route, however the latency of the wormhole link would be higher than the link latency between any two legitimate nodes in the network. Wormhole peers exhibit the behavior of tunneling the packets which is studied in WAD-HLA. Once wormhole tunnel is created, wormhole peer nodes drop the data packets.

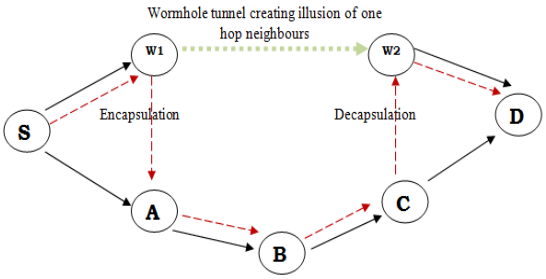

Figure1. Wormhole tunnel creation through encapsulation

3.2 WAD-HLA

Wormhole detection in WAD-HLA is two step based: Observation phase and followed by Confirmation phase.

1. **Observation phase** - The main luring characteristic of wormhole attack is that the wormhole peers create the impression of one hop neighbors but in reality they are distant apart. Hence the transmission time taken (per hop latency) for a wormhole link is much higher than between any two legitimate neighbor nodes. Per Hop latency computation based on round trip time (RTT) is carried out for all the links between source and destination nodes during the AODV route discovery phase. The link with maximum RTT (per hop latency) (exceeding threshold value) would be marked as candidate wormhole link and the corresponding nodes as suspicious wormhole peers. RTT is defined as the time difference between AODV RREQ and AODV RREP packet propagation at a node.

Notations used in per hop latency estimator:

RREQTS X: Timestamp when the RREQ packet is broadcasted by the current node X.
RREPTS X: Timestamp when the RREP packet is received by the current node X.
RTTprevious: RTT value of the previous hop.
RREQ{RREQTSX}: Modified RREQ request including RREQTSX.
RREP{RREQTSX, RTTBD}: Modified RREP packet including RREQTSX , RTTBD previous hop RTT

AODV RREQ packet format as per the RFC3561 is modified to include a RREQTS as shown in Figure 2. AODV RREP packet format as per RFC3561 is modified to include two new fields: RREQTS, RTT previous (previous hop RTT value) as shown in Figure 3. Each node stores two

values: RREQTS of its route request sending neighbour nodes, RTT value calculated in its routing table. Destination or intermediate nodes (storing route to destination) create the RREP packet, appending stored RREQTS and RTT value computed.

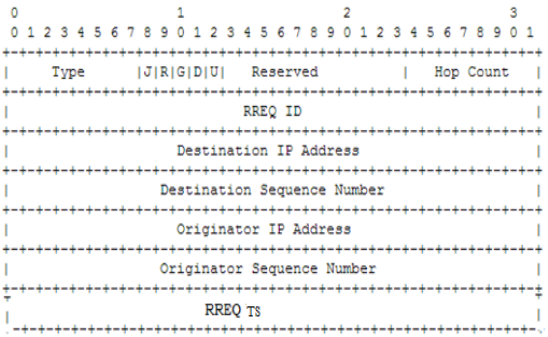

Figure2. Modified AODV RREQ packet format

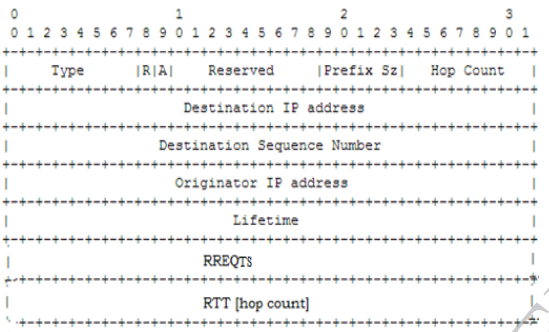

Figure3. Modified AODV RREP packet format

Each node receiving the RREP, computes the per hop link latency (RTT) as the difference between the RREPTS, RREPTS (stored in RREP packet), RTT previous (for all intermediate and source nodes) as shown in Figure 4.

RTT = RREPTS – RREQTS– RTT previous

Source node will receive the round trip time (RTT) values of all the per hop links on the path from source to destination, in the AODV RREP packet. It is the responsibility of the source node to find the suspicious wormhole links out of all the network links. Source node would compute the $RTT_{threshold}$ based on the previous simulation runs. $RTT_{threshold}$ value for WAD-HLA is computed which is furnished in result analysis section.

Link latency greater than $RTT_{threshold}$ value is marked as suspicious link by the source node and the corresponding peer nodes are marked as suspicious wormhole peers.

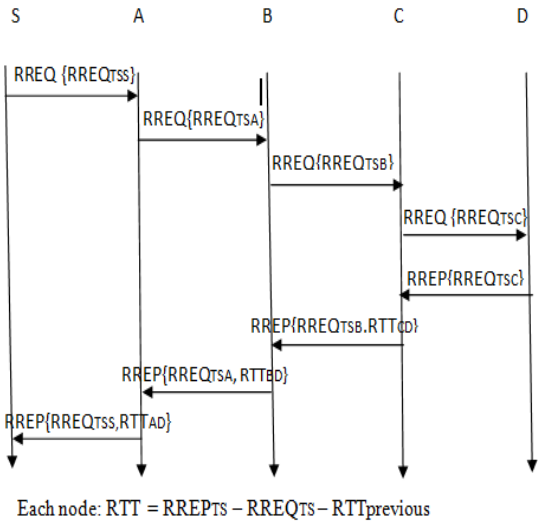

Figure 4. Per hop latency calculation

Efficiency of per hop latency calculator is discussed below:

1. **RTT calculation during node mobility**: The RTT calculation performed in the related work [6], [8] suggests the storing of RREQTS and RREPTS values in the current node itself. But during node mobility, when the node finds a better route to source as against during previous route request path, this approach becomes inadequate as the node stores the RREQTS and the new node in the path will not have the RREQTS. However, in case of WAD-HLA, the AODV RREQ contains the time stamp which would be available for any discovered path.
2. **Adequate RTT calculation for intermediate nodes:** In AODV routing, if an intermediate node has a route to the destination, then it creates a RREP packet and sends it back. So, if the node is storing the RREQTS as suggested in [6], [8] then RTT can't be calculated for the link to destination. Again WAD-HLA is efficient in this scenario as the RREQ packet carries the RREQTS.
3. **Per hop link latency calculation is time optimized:** For multiple routes using the same link, RTT value need not be computed every time by the node. RTT value for links can be reused as the nodes store the RTT value in routing table which gets refreshed every 10sec according to AODV route update.
4. **Strict clock synchronization not required:** Each node is using its own local clock to capture the values of RREQTS and RREPTS. Hence strict clock synchronization is not required in WAD-HLA.

2. **Confirmation Phase** – In this phase of WAD-HLA, the suspicious wormhole peers identified in the previous stage of WAD-HLA are confirmed by verifying if any adjoining node (intermediate node) exists between the candidate wormhole peers. In the related work [8], the wormhole link is confirmed using frequency hopping challenge which is different from WAD-HLA confirmation phase. The source node which has the information about the suspicious wormhole peers transmits a new AODV control packet namely; 'wormhole_dt_pkt' destined to one of the wormhole peers.

   'wormhole_dt_pkt' packet contains the following five fields: packet type, wormhole peer id, next-hop id, Source IP address, Destination IP address.

   Figure 5 depicts the flowchart for the confirmation phase of WAD-HLA. As shown in Fig 5, reception of 'wormhole_dt_pkt' triggers the wormhole peer to reply back with the next-hop node id of the other wormhole peer from its routing table. If the node id returned matches the node id of other wormhole peer node, then it means they are one hop neighbors and are not wormhole links. If the node id match fails, then the presence of wormhole link is confirmed resulting in successful detection of wormhole attack in AODV based MANET.

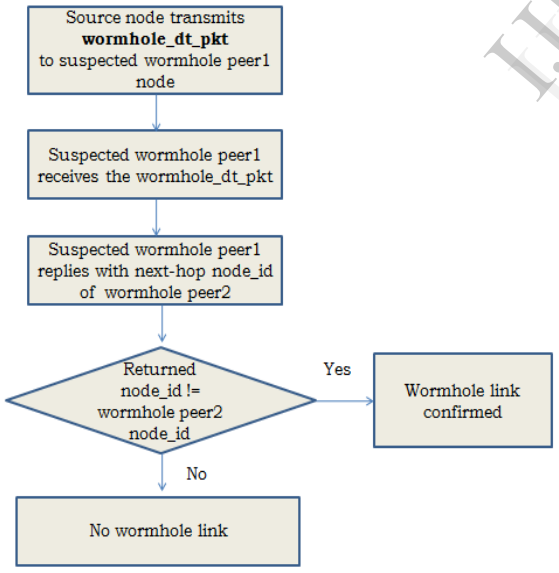

Figure5. Flowchart of intermediate node detection

4. Implementation

4.1 Simulation Model

The proposed wormhole detection approach is simulated using network simulator ns2 [11].A network topology of 50 nodes with CBR traffic pattern is adopted, with random way point mobility model [12] [13]. Five wormhole tunnels (10 wormhole peers) are considered. Simulation parameters are shown in Table1.

Table 1 Simulation Parameters

PARAMETER	VALUE
Area	1000 m * 1000m
Simulation Time	200 seconds
Number of nodes	50
Traffic Model	CBR
Mobility model	Random Way Point
Number of wormhole tunnels	1/2/3/4/5 (upto 10 wormhole peers maximum)
Number of network connections	1/2/3/4/5
Mac protocol	802.11
Data rate	2 Mbps
Data Packets	512 bytes/packet

4.2 Result Analysis

$RTT_{threshold}$ value is decided by running the simulation several times (50) times and is chosen as 1 sec.

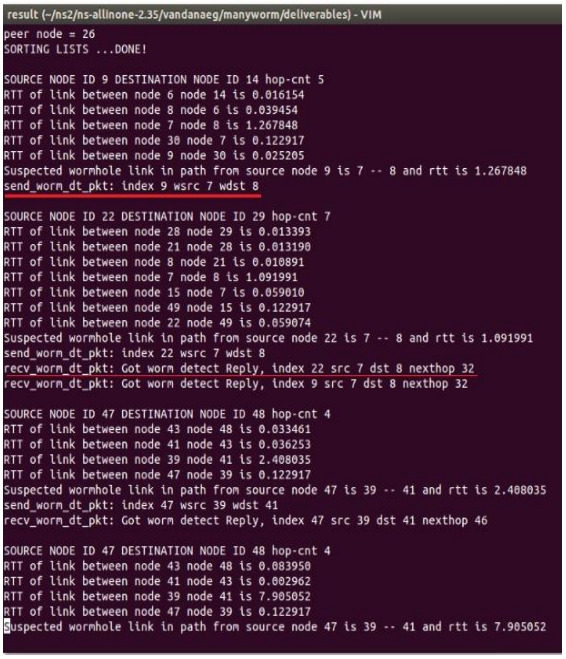

Figure6. WAD-HLA traces.

Figure 6 shows the traces for observation and confirmation phases of WAD-HLA. It depicts the RTT values for various per hops between source and destination. Also the routing of 'wormhole_dt_pkt' is depicted in Figure 6. The AODV trace file for WAD-HLA shows the packet type for 'wormhole_dt_pkt' as WDT.

Control Packet Overhead: It is evaluated by comparing the number of bytes transmitted in the network in each route request during the normal AODV routing (no wormhole detection mechanism) and after WAD-HLA deployment. The size of AODV RREQ is 32 byte and AODV RREP size is 20 bytes. The size of modified RREQ size is 36bytes and RREP size 28 bytes. Also each 'wormhole_dt_pkt' packet size is 20 bytes. Figure 7, shows the control packet overhead comparison with normal AODV depicting a bandwidth overhead of 40%.However, this overhead is observed only when a new route request is initiated. This overhead is acceptable in exchange for an efficient mechanism computing the per hop latency even during high mobility scenario, 100% detection rate and a minimum false positive rate.

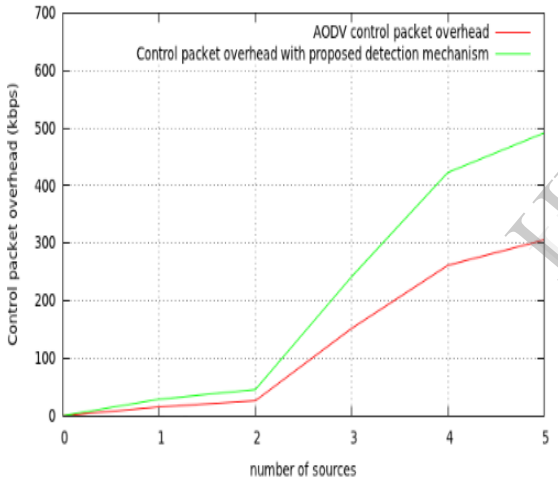

Figure7. Control packet overhead

Detection rate: A network may have many wormholes, but not all may be active (traffic flow) during the simulation period. In [6], the detection rate is discussed as proportional to the wormhole length and is solely based on RTT calculation. As observed in Figure 8, when total 8 wormhole nodes are present, during that time period the traffic is not flowing through one of the wormhole tunnels, hence detection rate reduced by 20% for the two undetected wormhole nodes. However, when all the five wormhole links (ten wormhole nodes) are active, WAD-HLA is successful in detecting all the ten wormhole nodes leading to 100% detection rate.

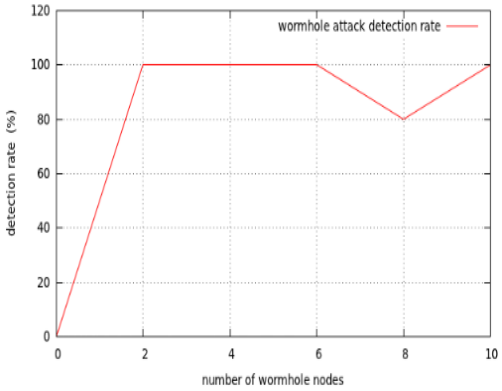

Figure8. Detection rate of WAD-HLA

False positive rate: It is calculated as the ratio of number of non-wormhole peers detected as wormholes to that of the total number of participating nodes in the network connection. As shown in Figure 9, when the number of connections is increased to 4, traffic is flowing through more links and some links are identified as candidate suspicious wormhole link due to RTT value greater than threshold value. During the confirmation phase, due to mobility, such candidate suspicious nodes may no longer be one hop neighbours and are confirmed as wormhole nodes. So, it is observed that when 4 connections are present; false positive rate is 0.034, since one of the links is falsely detected as wormhole peers. Due to the 2 step detection mechanism in WAD-HLA, false detection rate is better compared to [6].

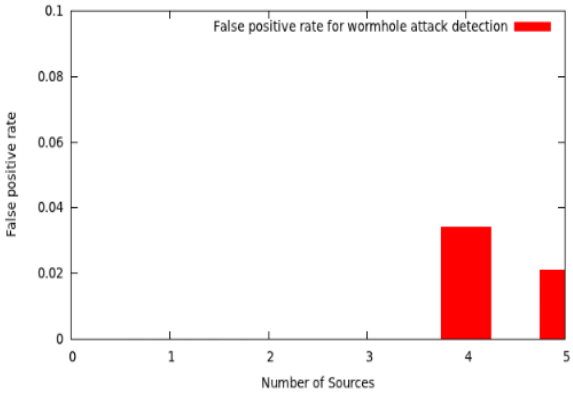

Figure 9. False positive rate of WAD-HLA

Memory Overhead: Each node stores the RREQTS from its immediate forwarding node. Value of RREQTS is 4bytes.Size of RTT value is 4 bytes. If there are N neighbourhood nodes to a node, so a maximum of N*8bytes is required to store the values. In our simulation of 50 nodes, in worst case a node is surrounded by all 49 neighbours, so maximum the memory occupied in each node is 49*8 = 392bytes.

5. Conclusion and Future Work

In this paper, a novel approach, WAD-HLA to detect wormhole attack in MANET is proposed. The main advantage of WAD-HLA includes the early detection of wormhole attack during AODV route discovery phase, no requirement of specialized hardware or strict clock synchronization, effective mechanism with good performance is achieved. As a part of the future work, we would propose prevention mechanisms for wormhole attack in MANET.

References

[1] C.Sivaram Murthy and B.S Manoj, "Ad Hoc wireless Networks", Pearson Education, Second Edition India, 2001.

[2] R.H. Khokhar, Md. A.Ngadi, S. Manda,"A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, 2 (3), pp. 18-29, 2008.

[3] Reshmi Maulik and Nabendu Chaki,"A Study on Wormhole Attacks in MANET",International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279

[4] C. E. Perkins and E. M. Royer, "The ad hoc on-demand distance vector protocol," in Ad hoc Networking, Addison-Wesley, pp. 173–219, 2000.

[5] Vandana C.P, A. Francis Saviour Devaraj, "Evaluataion of impact of wormhole attack on AODV", International Journal of Advanced Networking and Applications, ISSN 0975-0290 Volume: 04 Issue: 04 pp. 1652-1656, 2013

[6] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Heejo Lee,Sungyoung Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", Wireless Sensor Network Track at IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA, Jan 11-13, 2007.

[7] Hon Sun Chiu King-Shan Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", International Symposium on Wireless Pervasive Computing ISWPC 2006.

[8] H. Vu, A. Kulkarni, K. Sarac, N. Mittal, "WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks". In Proceedings of International Confernce on Wireless Algorithms Systems and Applications, LNCS 5258, pp. 491-502, 2008.

[9] Lijun Qian, Ning Song, and Xiangfang Li,"MOBIWORP Detecting and locating wormhole attacks in Wireless Ad Hoc Networks through statistical analysis of multi-path", IEEE Wireless Communications and Networking Conference - WCNC 2005.

[10] S. Choi, D. Kim, D. Lee, J. Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks". In International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 343-348, 2008.

[11] The Network Simulator ns-2, http://www.isi.edu/nsnam/ns/

[12] Geetha Jayakumar, Gopinath Ganapathi, "Reference Point Group Mobility and Random Waypoint Models in Performance Evaluation of MANET Routing Protocols", Journal of Computer Systems, Networks, and Communications, 2008

[13] C. Bettstetter and C. Wagner, "The spatial node distribution of the random waypoint mobility model," in Proc. of the 1st German Workshop on Mobile Ad Hoc Networks (WMAN), (Ulm,Germany), Mar. 2002

Authors Biography

Vandana C.P is currently perusing her M.Tech in computer networks under VTU University. She has 6 years of software industry experience in telecom domain mainly on network management systems (NMS) and storage area research interest includes security issues in MANET, network management systems and

Dr A Francis Saviour Devaraj has done his B.Sc and M.Sc in Computer Science from St.Xavier's College, M.E (Computer Science & Engineering) from Anna Universitv.He obtained his PhD in computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has also obtained certification in CCNA. He is a life member in technical societies like CSI, ISTE, CRSI, and ISOC. He has around eleven years of teaching experience in leading educational institutions in India and abroad. He has authored/co-authored research papers at the national and international levels. He has attended/conducted various national and international level workshops/ seminars/conferences.