MLDW- A MultiLayered Detection mechanism for Wormhole attack in AODV based MANET

Vandana C.P[1], Dr. A. Francis Saviour Devaraj [2]

[1]Scholar, Department of Information Science Engineering
Oxford College of Engineering, Bangalore, India
vandana.hareesh@gmail.com
[2]Professor, Department of Information Science Engineering
Oxford College of Engineering, Bangalore, India
saviodev@gmail.com

ABSTRACT

Wormhole attack is one of the serious routing attacks amongst all the network layer attacks launched on MANET. Wormhole attack is launched by creation of tunnels and it leads to total disruption of the routing paths on MANET. In this paper, MLDW- a multilayered Intrusion Detection Prevention System approach is proposed to detect and isolate wormhole attack on MANET. The routing protocol used is Adhoc On Demand Distance Vector (AODV). MLDW has a layered framework consisting of link latency estimator, intermediate neighbor node discovery mechanism, packet drop calculator, node energy degrade estimator followed by isolation technique. MLDW effectiveness is evaluated using ns2 network simulator.

KEYWORDS

MANET, AODV, Routing Attack, wormhole link, Tunnel

1.INTRODUCTION

The dynamic, decentralized, infrastructure less nature, ad-hoc topology of Mobile adhoc network (MANET)[1] make them most vulnerable to security threats [2].Various MANET routing protocols[3] like table-driven/proactive, demand-driven/reactive or hybrid variants are subjected to routing attacks resulting in compromised confidentiality, integrity and message authentication.

1.1 Wormhole Attack

Wormhole attack [4] is a routing attack, where the replay attack is launched at the network layer. Wormhole peers which are normally distinct apart on the network collectively launch the wormhole attack by pretending to be one hop neighbors. A wormhole link or tunnel is established by these wormhole peers and it is used to replay the packets to another region on the network leading to corruption of routing protocol. Wormhole attack when successfully launched in localization based systems like environment monitoring systems, disaster alert systems etc. may cause complete disruption.

Wormhole tunnels [5] are created by employing several techniques like out-of-band/ high quality communication link, packet encapsulation, high power transmission capability (antenna), packet relay, protocol distortion etc. After establishing the wormhole tunnel and its successful inclusion in the routing path wormhole peers can perform packet relay, selective-forwarding, false-routing,

DOI : 10.5121/ijsptm.2013.2303

spoofing, packet drop/neglect or packet modification, hereby making the detection of wormhole attack in routing protocols a non-trivial job.

1.2 Wormhole attack on AODV based MANET

Adhoc On Demand Distance Vector [6] (AODV), is an on demand routing protocol in MANET. Wormhole attack is normally launched in AODV during the route discovery phase by creating the illusion of one hop neighbors by wormhole peers. Wormhole tunnel is established by using one of the mentioned techniques in [5]. Route Request (RREQ) packets are routed through these wormhole tunnels to reach the destination at a faster rate (low hop count) compared to usual normal path. As per AODV protocol, the destination node discards all the later RREQ packets received and selects the false wormhole tunnel infected route to send the Route Reply (RREP). This results in inclusion of wormhole tunnel in the data flow route leading to a successful launch of wormhole attack in AODV data transfer phase.

Network parameters [7] like throughput, packet delivery ratio (PDR), average end to end delay and drop rate are adversely affected by wormhole attack launched in AODV based MANET. The same is studied through simulation results in Evaluation of impact of wormhole attack on AODV [7] depicting the importance of detection of wormhole attack in MANET.

The remaining paper is arranged in the following ways: Section 2 briefs about the related work done in this field, Section 3 explains the proposed approach MLDW to detect the wormhole attack in AODV based MANET, Section 4 talks about the result analysis and finally the Section 5 concentrates on conclusion and the future work.

2. RELATED WORK

Detection of wormhole attack has been an active area of research and many mechanisms have been proposed so far luring the various behaviours of wormhole attack.

2.1 Distance-bound based approach

In packet leaches [8], based on the geographic location, distance between nodes is calculated and is used for detecting wormhole attack. Temporal and geographic leashes are proposed where strict clock synchronization and Global Positioning system (GPS) coordinates of all nodes are required. This requirement may not be supported by all mobile devices in the network and hence may not be a practical solution.

2.2 Special Hardware-based approach

SECTOR [9] The Secure Tracking of Node Encounters in Multi-Hop Wireless Networks uses Mutual Authentication with Distance-bounding (MAD) protocol with specialized hardware and directional antenna that enables fast sending of one-bit challenge messages without CPU involvement is used. Usage of specialized hardware like directional antenna may be too complex to be implemented for hand held devices in the network.

2.3 Time of flight based approach

In wormhole attack detection mechanism TTM[10], WORMEROS [11], 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. But, detection based solely on transmission time, can lead to high false positive rate. The link latency may go exceptionally high due to link congestion observed during heavy network traffic. In WAD-HLA [12], hybrid approach of RTT approach along with adjoining node detection is proposed providing low false positive rate. In this approach, the RTT computation is efficient; time optimized and supports node mobility, intermediate link breakage.

2.4 Hop Count / delay per hop based approach

In Delphi (Delay Per Hop Indicator) [13] every possible disjoint path between sender and receiver is computed. Hop count and Delay per Hop value is used to detect wormhole. Delphi detects exposed wormhole attacks but does not consider mobility. In statistical approach SAM [14] (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.SAM works well for stationary topology.

2.5 Secure Neighbour Discovery and watch-dog based approach

In MOBIWORP [15] neighbour discovery process confirms the presence of wormhole attack. Position of each node is traced by a central authority, which isolates the malicious nodes. But mobility is a limiting factor. LITEWORP [16] is wormhole countermeasure based on monitoring local traffic monitoring systems but is applicable to only stationary networks.

2.6 Trust and Reputation based approach

TARF[17] A trust aware routing framework computes the trust level of each neighbour nodes and the lowest trust levels are considered to be wormhole nodes. Packet drop behaviour of the malicious nodes along with the remaining energy of the nodes is considered to detect the wormhole nodes. Packet tunnelling or replaying behaviour of the wormhole peers is not captured here.

3. MLDW DETECTION SCHEME

3.1 System Model and Assumptions

A homogeneous network consisting of 50 nodes with same transmission capabilities, energy (battery) resources is considered. 10 wormhole peers are present in the network.

3.2 Threat Model

In MLDW, the wormhole tunnel is launched by using packet encapsulation technique. As shown in Figure.1, all the packets are encapsulated in AODV routing protocol at one of the wormhole peers and are sent across to another wormhole peer, where it is de-capsulated. Through this packet

encapsulation technique, an illusion of low hop count is created. Link latency of the wormhole tunnel is relatively high compared to other normal network links. MLDW addresses the tunneling and packet drop behavior of wormhole peers. Selective dropping of packets is simulated at wormhole peers.

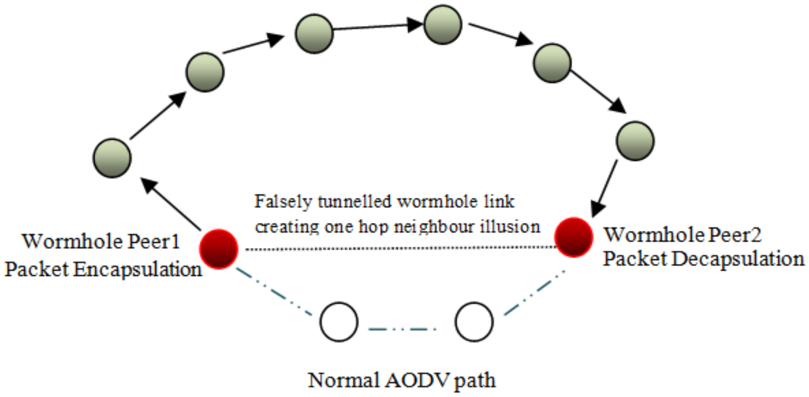


Figure1. Wormhole tunnel creation through encapsulation

3.3 MLDW Design

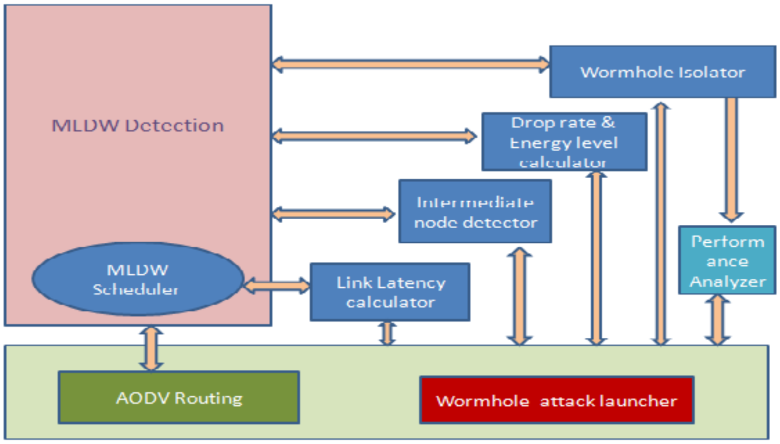


Figure2. MLDW Architecture Diagram

As shown in Figure.2, wormhole attack launcher module establishes the wormhole tunnel and selective packet dropping behavior in AODV routing. MLDW scheduler module invokes the MLDW layered framework starting with link latency calculator, intermediate node detector, drop rate and energy level calculator and followed by isolation of wormhole nodes. Performance analyzer module computes the various network parameters to prove the effectiveness of MLDW approach in detecting the wormhole attack launched in AODV based MANET.

3.4 MLDW layered Approach

MLDW follows a layered structure as shown in Figure. 3. It consists of 4 main layers namely: Observation layer, Detection layer, Confirmation layer and Isolation layer. The first 3 layers

detects the wormhole attack and the 4th layer prevents further wormhole attack by isolating the detected wormhole nodes in the AODV based MANET.
Various phases of MLDW are discussed below

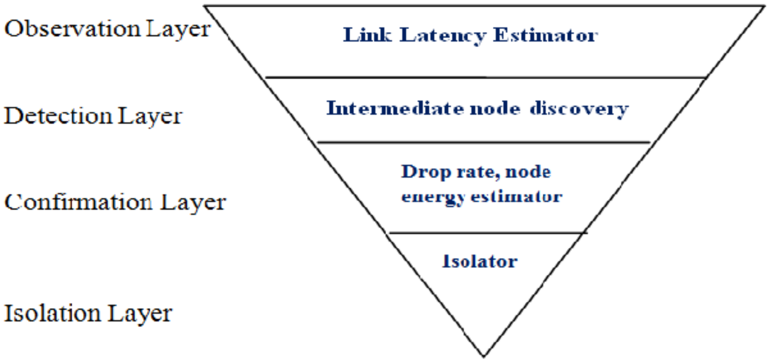


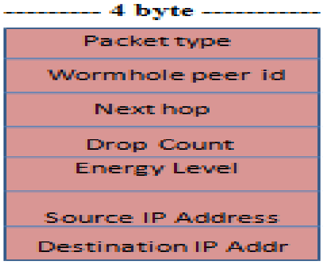
Figure3. MLDW Layered structure

MLDW Layer1: Link Latency Estimator – Link latency for all the links between source and destination nodes is computed during the AODV route discovery phase. Link Latency for a particular link is computed as RTT (Round Trip Time). It is the time difference between AODV RREQ and AODV RREP packet propagation at a node. As shown in equation 1, each node receiving the RREP, computes the per hop link latency as the difference between the TS_{RREP} (time stamp when RREP packet reaches the node), TS_{RREQ} (stored in RREP packet), RTT pre_link(for all intermediate and source nodes).

$$\text{Link Latency} = TS_{RREP} - TS_{RREQ} - RTT_{pre\_link} \qquad \text{----------------------} \ (1)$$

Source node collects the link latency value (AODV RREP) for all links between itself and destination node. Based on the previous simulation done (50 times), threshold value $TH_{latency}$ is computed as 1second. Link latency greater than $TH_{latency}$ value is marked as suspicious link and the corresponding peer nodes as suspicious wormhole peers. This link latency calculator works [12] even with node mobility, and does not require any strict clock synchronization.

MLDW Layer2: Intermediate neighbor node discovery Suspected wormhole peers identified during MLDW layer1 are confirmed to be wormholes by verifying if there are any


---------- 4 byte -----------

Packet type
Wormhole peer id
Next hop
Drop Count
Energy Level
Source IP Address
Destination IP Addr

Figure4. MLDW_finder packet format

intermediate nodes [12] existing between the candidate wormhole peers. The source node unicast new AODV packet ‘MLDW_finder’ to one of the wormhole peers. ‘MLDW_finder’ packet format is shown in Figure.4.Suspected wormhole peer upon receiving the ‘MLDW_finder’, replies back with its next-hop node id of its corresponding suspected wormhole peer from its routing table. Presence of wormhole is confirmed based on returned nodeid match. Confirmed wormhole peers are marked for isolation.

MLDW Layer3: packet drop calculator, node energy degrade estimator- Suspected wormhole peers which didn’t confirm as wormholes during MLDW level2 are subjected to

MLDW Layer3 and the source node transmits the 'MLDW_finder' packets to such suspected wormhole peers. This Layer3 is included in MLDW to reduce the false positive rate. Reception of 'MLDW_finder' starts the wormhole_drop event timer and energy degrade estimator.

Drop rate is computed as shown in equation 2.

$$\text{Drop rate (\%)} = \frac{\text{Number of packets dropped}}{\text{Total number of packets received}} \times 100 \quad \text{--------------------------------(2)}$$

The following Energy Model [18], [19] is used in MLDW

Transmission mode: **Consumed energy = Pt * T** ------------------------------- (3)

Pt is the transmitting power and T is transmission time.
Reception mode: **Consumed energy = Pr * T** ------------------------------- (4)

Pr is the reception power and T is the reception time.

T= Data size / Data rate ------------------------------- (5)

Remaining energy = Current energy – Consumed energy ------------------------------- (6)

From the previous simulation run, Dropthreshold is estimated as 2%. Remaining energy for suspected nodes is computer as per equations 3,4,5,6.Also, it is observed from simulation runs, that the remaining energy of the suspected wormhole peers which have high drop rate (greater than Dropthreshold) degrades to 50% of the initial node energy level.Whenever the packet drop rate for any of these suspected wormhole peers exceeds the DropThreshold, wormhole_drop event timer is stopped, 'MLDW_finder' is populated with packet drop rate, remaining node energy level and are transmitted back to the source node. Source nodes confirm such suspected nodes as wormhole peers and marks them for isolation.

MLDW Layer4: Node Isolation

The suspected wormhole peers confirmed in Layer2 and Layer3 of MLDW are isolated. The transmitting and the reception radio interfaces of the nodes are made down, so that they don't participate in any further routing operations.

4. Implementation And Results

4.1 Simulation Set-Up

MLDW is simulated using network simulator ns2 [20].A network topology of 50 nodes with CBR traffic pattern is adopted, with random way point mobility model [21]. Simulation parameters are shown in Table1.

Table 1 Simulation Parameters

PARAMETER	VALUE
Area	1000 m * 1000m
Simulation Time	100 seconds
Number of nodes	50
Traffic Model	CBR (UDP)
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
Transmission Range	250m
Data rate	2 Mbps
Data Packets	512 bytes/packet
Initial Node Energy	1000J
Transmission Power (mW)	1
Reception Power (mW)	1

4.2 Simulation Result Analysis

Network Throughput [7]: MLDW performance is measured in terms of throughput as the number of packets received at the destination over a period of time and is measured in kbps. Figure.5 depicts that the network throughput decreases drastically when the number of wormhole peers are increased from 0 to 10 (wormhole links increased from 0 to 5).With MLDW launched, it is observed from table 2 that the throughput improves by 49.4% compared to wormhole attacked AODV.

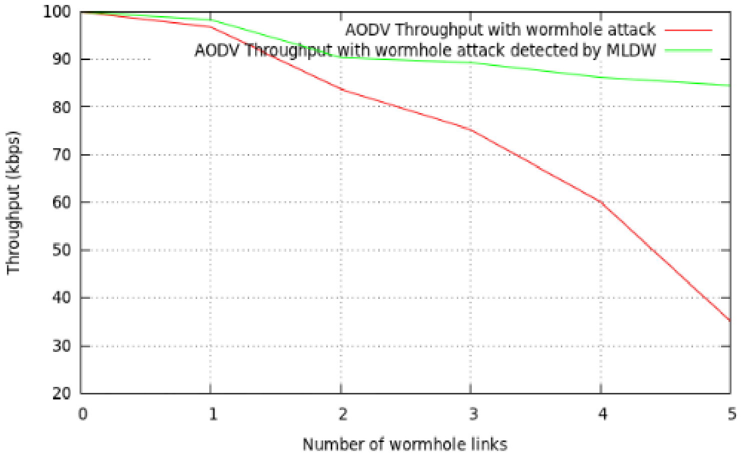


Figure5. Network Throughput comparisons

Table2. Throughput in kbps

Number of connections	**Throughput in wormhole infected AODV**	**Throughput with MLDW in AODV**	**Percentage increase in Throughput**
1	96.809349	98.344525	2.5%
2	83.778225	90.420781	7%
3	75.292582	89.344525	14%
4	60.131866	86.220781	26%
5	35.139876	84.528980	49.4%

Average end to end delay [7]: It is the total time taken for a packet to reach from source to destination and it is measured in seconds. As shown in Figure. 6, average end to end delay increases drastically when number of wormhole links are increased as the link latency is high for wormhole tunnels leading to more time consumption. With all 5 wormhole links activated, delay is 4.6723 sec in AODV, however with MLDW in launch, it is reduced to 0.989sec as depicted in Table3.

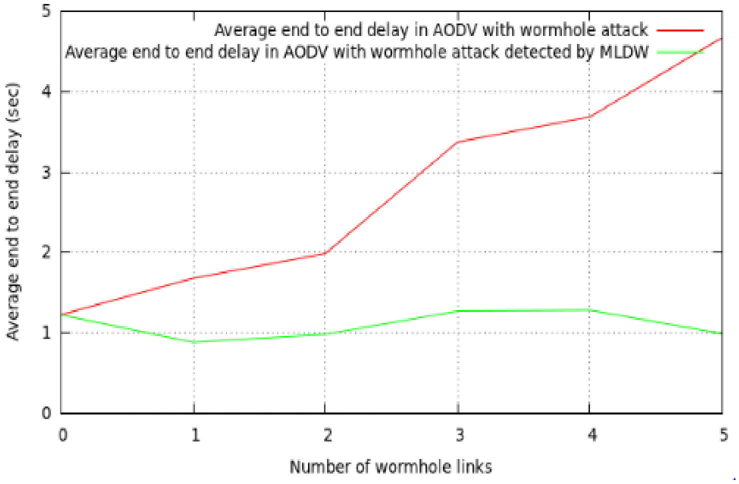


Figure6. Average end to end delay comparison

Table3. Average End to end delay in sec

Number of connections	**End to end delay in wormhole infected AODV**	**End to end delay with MLDW in AODV**	**Percentage decrease in end to end delay**
1	1.678211	0.881254	0.8%
2	1.986114	0.981655	1%
3	3.373981	1.270899	2.1%
4	3.685773	1.283235	2.4%
5	4.672311	0.989856	3.7%

Packet delivery ratio [7]: PDR is the ratio of number of packets received at destination node to that of number of packets sent by source node.Again PDR decreases drastically with increase in wormhole links as more wormhole peers perfomr slective packet dropping.As shown in Figure. 7, PDR improves by 24% with MLDW in place compared to wormhole infected AODV.Table 4 shows the improvement made in PDR with MLDW in action in network.

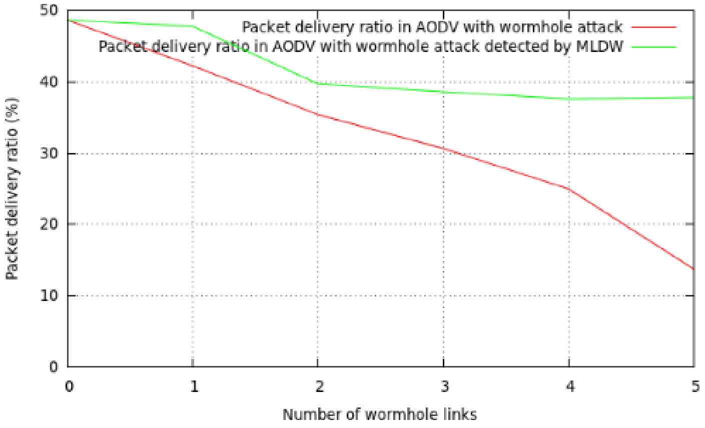


Figure7. Packet Delivery Ratio comparison

Table 4. Packet delivery ratio (PDR) in (%)

Number of connection	PDR in wormhole infected AODV	PDR with MLDW in AODV	Percentage increase in PDR
1	42.229232	47.781283	5.5%
2	35.394322	39.705573	4.4%
3	30.641430	38.590957	8%
4	24.963197	37.590957	13.4%
5	13.711882	37.791798	24%

Drop rate [7]: Drop rate is the ratio of number of packets dropped during transmission to that of number of packets sent by the source node.Drop rate increases steadily with increase in womehole links in AODV. As observed in Figure. 8 and Table 5, packet drop rate reduces by 24% in the presence of MLDW compared to wormhole infected AODV.

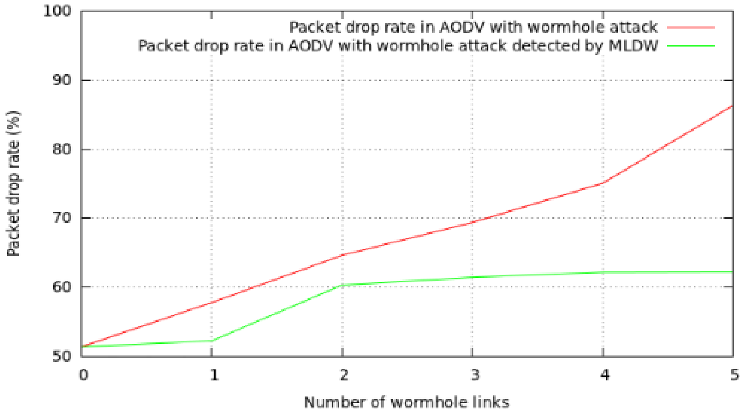


Figure8. Packet drop rate comparison

Table 5. Packet drop rate in (%)

Number of connections	**Packet Drop rate in wormhole infected AODV**	**Packet drop rate with MLDW in AODV**	**Percentage decrease in packet drop rate**
1	57.770768	52.218717	5.5%
2	64.605678	60.294427	4.4%
3	69.358570	61.409043	8%
4	75.036803	62.166141	13%
5	86.288118	62.208202	24%

Control Packet Overhead: The number of bytes transmitted in the network in each route request during the normal AODV routing is compared with number of bytes transmitted after MLDW is deployed. The size of AODV RREQ is 32 bytes [22] and AODV RREP size is 20 bytes [22]. In MLDW, the size of modified RREQ size is 40bytes and RREP size 36 bytes. Also each "MLDW_finder" is 20 bytes. From Figure.9, an overhead of 16% is observed which is acceptable for the better MLDW performance and response time provided, which is discussed in the later sections of the paper.

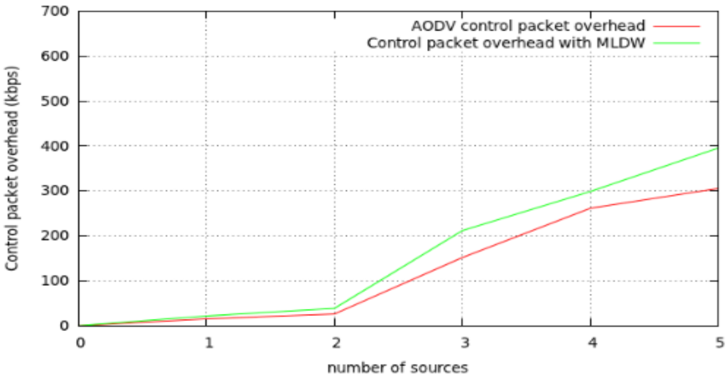


Figure9. MLDW control packet overhead

Response Time: MLDW response time is defined as the time when all the 10 wormhole nodes are detected and isolated from the network. In Figure.10, it is observed that the last wormhole link is isolated at the end of 23.8 seconds. And the system is brought back to stable condition.

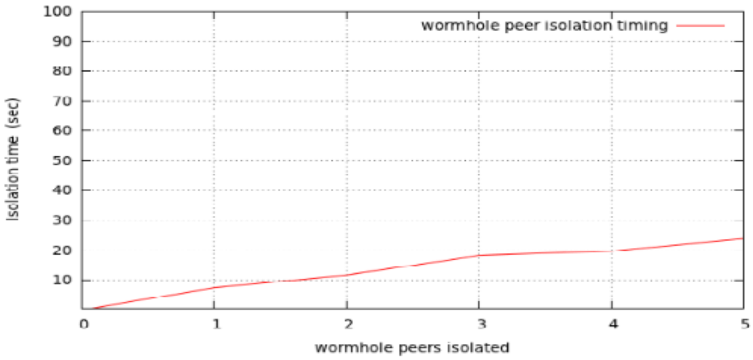


Figure10. MLDW response time

MLDW Performance Level – Figure. 11 depicts how MLDW reacts to wormhole attack with respect to time and the throughput improvement after all wormhole peers are isolated. It is observed that the throughput is maintained at a constant level after all wormholes are isolated after 23.8 seconds.

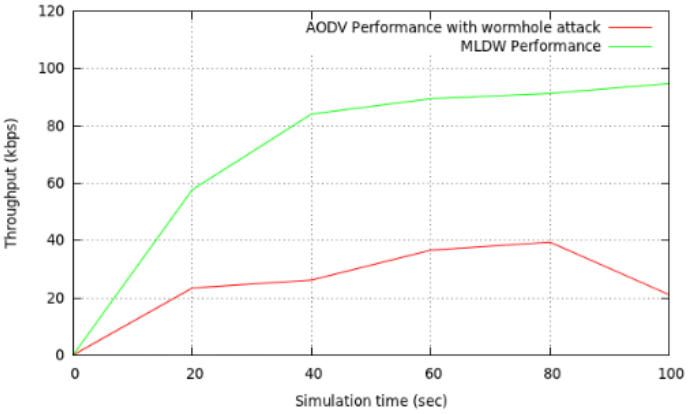


Figure11. MLDW Performance level

Table 6 MLDW Performance Inference Table

Worm hole Link	MLDW Response Time	MLDW Layer Detected	Throughput Degrade %	PDR difference %	Drop rate difference%	Av. end to end delay sec
1	7.4	Layer 2	52%	54.2%	44.3%	1.73
2	11.7	Layer 2	47%	44.7%	38.21%	1.51
3	18.2	Layer 2	41%	38.4%	30.11%	1.39
4	19.7	Layer 2	33%	36.3%	27.8%	0.9
5	23.8	Layer 3	20%	24.1%	21.9%	0.84

It is observed from Table 6, that MLDW isolates the 1st wormhole link at 7.4 seconds and completes isolating all the 5 wormhole links by end of 23.8 seconds. During this MLDW response time, there is an improvement of 32% in network throughput degrades. PDR improves by 30% till all wormhole links are isolated by MLDW during its response time. Packet drop rate improves by 24% from the initial isolation time till the final response time. Average end to end delay has reduced to 0.89 seconds at the end of MLDW response time. Thus it justifies the control packet overhead of 16% as shown in Figure. 9 against the better response time which leads to system stability attainment at a faster rate.

5. CONCLUSION AND FUTURE WORK

MLDW allows the early detection of wormhole attack during AODV route discovery phase with efficient response time. MLDW doesn’t require any specialized hardware or strict clock synchronization and achieves higher performance. As a part of future work, reduction in MLDW control packet overhead would be achieved. A novel approach would be proposed to address the packet modification behavior of the wormhole attack by employing encryption mechanisms. MLDW application would be implemented in intelligent Transportation System (ITS) using mobireal simulator.

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] Jhaveri, R.H., Parmar, J.D., Patel, A.D., and Shah, B.I, “MANET Routing Protocols and Wormhole Attack against AODV”, International Journal of Computer Science and Network Security, 10 (4).

[4] 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

[5] Meghdadi M, Suat Ozdemir and Inan Guler ,” A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks”, Volume 28 (2012) pp 89-102

[6] 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.

[7] 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

[8] Y. Hu, A. Perrig, and D. Johnson, “Packet leashes: a defense against wormhole attacks in Wireless Ad Hoc Networks”, In Proceedings of theIEEE Conference on Computer Communications (Infocom), 2003.

[9] L. Hu and D. Evans, “SECTOR Using directional antennas to prevent wormhole attacks”, In proceedings of the IEEE Symposium on Network and Distributed System Security (NDSS), 2004.

[10] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, 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.

[11] 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.

[12] Vandana C.P, A. Francis Saviour Devaraj, “WAD-HLA: Wormhole Attack Detection using Hop Latency and Adjoining node analysis in MANET”, International Journal of Advanced Networking and Applications, ISSN 0975-0290 Volume: 04 Issue: 04, 2013

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

[14] 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.

[15] 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.

[16] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, “LITEWORP: A Lightweight countermeasure for the Wormhole Attack in Multihop Wireless Networks”, International Conference on Dependable Systems and Networks (DSN 2005): 612-621

[17] Guoxing Zhan, Weisong Shi, Julia Deng,"Design and Implementation of TARF:A Trust-Aware Routing Framework for WSNs", IEEE Transactions on dependable and secure computing pp 1545-5971(2012)

[18] Laura, Energy Consumption Model for performance analysis of routing protocols in MANET ,Journal of mobile networks and application 2000.

[19] LIXin MIAO Jian –song, “A new traffic allocation algorithm in AdHoc networks”, “The Journal of China University of Post and Telecommunication”, Volume 13, Issue 3, September 2006

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

[21] 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

[22] AODV, http://www.ietf.org/rfc/rfc3561.txt

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 networks (SAN) domain. Her research interest includes security issues in MANET, network management systems and functionalities.

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 University.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.