International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183841

Performance Analysis of Prevention of AODV-based Mobile AdHoc Networks under Cooperative Wormhole Attacks

[1]A. S. Bhandare, [2]Prof. B. S. Patil, [3]M. A. Khade, [4]S. D. Patil

[1, 3,4]Assistant Professor Department of Information Technology, Padmabhooshan Vasantraodada Patil Institute of Technology, Budhgaon, Maharashtra, India

[2]Associate Professor Department of Information Technology, Padmabhooshan Vasantraodada Patil Institute of Technology, Budhgaon, Maharashtra, India

ABSTRACT

A Wireless ad-hoc network is a temporary network set up by wireless mobile computers (or nodes) moving arbitrary in the places that have no network infrastructure called as Mobile Ad-hoc Network (MANET). As MANET does not have fixed infrastructure and central administration, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of nodes. Wormhole attack is one of the severe attacks which absorb all data packet instead of sending it to destination. An Enhanced HSAM technique is used in order to compare the different performance parameters with HSAM and the results are monitored with the use of network simulator.

Keywords : MANET, AODV, HSAM, E-HSAM

I. INTRODUCTION

Mobile devices such as laptops and cellular phones are capable of sending data to each other on demand. This type of data transfer creates a temporary mobile ad hoc network (MANET) [1]. Unfortunately, MANETs do not have a centralized infrastructure providing security and are highly subjected to malicious attacks [2]. One example of an attack on MANETs is a wormhole attack. The consensus among the research community involved is that wormhole attacks aim to attack a fragile MANET by using two or more malicious nodes to fool a source node which is trying to send data. This is done by using a route which presents itself as the shortest route to the destination node [3]. A common wormhole attack involves a node which is used to record data and another node which is used to forward data back into the network [4]. In turn, there are other attacks which include the modification of data packets and thus the disruption of the integrity of the data as it travels in the network. Additionally, the dropping of data packets is also a possibility. Thus, the types of attacks are limitless. A MANET is a network structure without a centralized infrastructure, making it vulnerable to several types of attacks such as wormhole attacks. Wormhole attacks aim to attack a fragile MANET by using two or more malicious nodes to fool a source node, which is trying to send the data. Typically, the malicious node uses a fake route which presents itself as the shortest route to the destination node [3]. Usually, two nodes are involved: one is used to record the data and the other is used to forward the data back into the original network [4]. Contrary to malicious attacks, it was suggested [5] that if a wormhole attack is not used for malicious means (for instance, the case where it is created by security personnel to test a network), the performance of the network can be improved.

AODV and Message Delivery Protocol

AODV [6] is a routing protocol which has been designed to wait for requests before attempting to find the most optimal route for use by one node (source) to send messages to another node (destination). The most optimal route is determined by the distance or the number of hops between nodes. There are two types of message delivery protocols; namely, unicast and multicast. Unicast message delivery [7] is a type of message passing mechanism used in AODV. Unicast involves two nodes of interest, one node wanting to send a message and another node that will receive the message. Therefore, unicast is commonly known as `one-to-one' message transmission. Multicast message delivery [8] is another type of message delivery scheme. Unlike unicast, multicast can involve two or more nodes of interest. Therefore, multicast is commonly known as `one-to-many' message transmission. For example, after a source node receives a RREP from different destination nodes of interest, it sends the data simultaneously to all the targeted destination nodes. In this thesis, only unicast transmission is used.

II. LITERATURE REVIEW

Khalil et.al.[9] proposed a protocol (so-called LiteWorp) to discover and prevent wormhole attacks in a static network. LiteWorp works by instructing each node involved to obtain 2-hop routing information from their immediate neighbours. The proposed technique is an extension of their original protocol in which each node only keeps 1-hop routing information. Therefore, analyzing the routing information on routes which are 2-hops away will aid wormhole detection. In addition, nodes will also monitor their own neighbour nodes and potentially become guard nodes for a pair of nodes which are maximum 2-hops apart. Guard nodes are designed to monitor neighbouring nodes activity to aid wormhole detection. However, the LiteWorp idea was only designed for static networks and is impractical for a mobile network such as MANETs.

Hu.et.al.[4] introduced a way to prevent wormhole attacks. Their idea of using packet leashes consists of information in a commuting packet that detects and prevents abnormal transmission. In doing so, some timings are inserted in the packet when it is forwarded by the sending node to a receiving node (not necessarily from source to destination). Next, the receiver compares its own timings with the sender's timings resulting in a calculated latency between the two nodes. The authors pointed out a limitation to this technique since it is possible that two malicious nodes collude together to break their scheme while still being within an acceptable distance.

Mamatha et.al.[11] proposed an AODV-based scheme for preventing wormhole attacks in MANETs in which the hash identifier of the original packet is inserted in the data as it gets forwarded from node to node.

Singh and Vaisla [10] introduced an approach to detect wormhole attacks, where time is considered as a key parameter. In their scheme, during the RREQ broadcast phase of route discovery, each node will save a TREQ (time of request) which will record the time it takes for the current node to forward a RREQ to its neighbour node. Once the RREQ reaches the destination, a RREP is sent by the destination node to the sender and a TREP (time of reply) is recorded at each node as the algorithm retraces its steps back to the sender. Finally, a RTT (round trip time) of each successive intermediate node is calculated as the difference between the TREP and the TREQ (RTT = TREP - TREQ). The RTT is calculated at each node to check if the value is higher or lower than other RTT values calculated along the route.

Choi.et.al. [12] proposed a method which is based on the DSR routing protocol to detect wormholes in MANETs. Their method consists of a neighbour node monitoring technique and a wormhole route detection method controlled by means of a timer (so called wormhole prevention timer). This scheme does not rely on any specific hardware for node location or time synchronization.

Hayajneh.et.al [13] proposed a technique called DeWorm which utilizes discrepancies in routing between neighbours of nodes that are along a route of a selected path between the source and destination nodes. DeWorm takes advantage of the fact that a wormhole link attempts to attract a large amount of traffic to itself. Moreover, the routes through the wormhole link are shorter than that of legitimate nodes within the network. Each node along the route, after being selected during the route discovery phase, will initiate the DeWorm algorithm which relies on the acquisition of different routes to a target node.

III. METHODOLOGY

Prevention against Single Wormhole Attacks - Single Wormhole: Method 1

In this scenario, we simulate two different single wormhole attacks. In order to do this, we must define the two colluding or malicious nodes. In this simulation, we use nodes 6 and 10 as the two colluding nodes. The idea is to get these two nodes to have direct communication with each other. For example, if node 10 gets an RREQ packet, the next hop should be to the other malicious node, namely node 6 and vice versa. It is important to note that the radio power of the two colluding nodes is higher than that of normal nodes. The reason for increasing the power of the two nodes is part of what is called a long range wireless attack. Since the two nodes have a higher range, the number of neighbours to the nodes will increase, thus reducing the number of hops required to get to the destination node. Malicious node 10 drops data packets as they are tunneled through the wormhole.

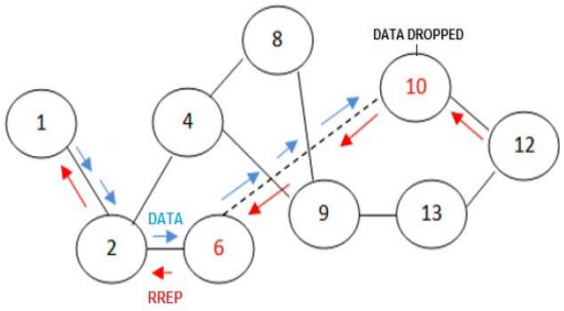


Figure 1. Single Wormhole Attack – Method 1

Single Wormhole: Method 2

In this simulation, we also use nodes 6 and 10 as the two colluding nodes. This scenario is slightly different than that in method 1. Although malicious nodes 6 and 10 are colluding nodes, packets are only forwarded from node 6 to node 10 but not the other way around. Node 10 will not forward any packets to node 6 as in the first method. Another important constraint of this scenario is that one of the colluding nodes must be a direct neighbour of the source node (here, malicious node 6) and the other node must be a direct neighbour of the destination node (here, malicious node 10). As with method 1, the radio power of the two malicious nodes is higher than that of normal nodes. Finally, the attack scenario of this method is the same as in method 1; that is, data packets are dropped by the malicious node 10.

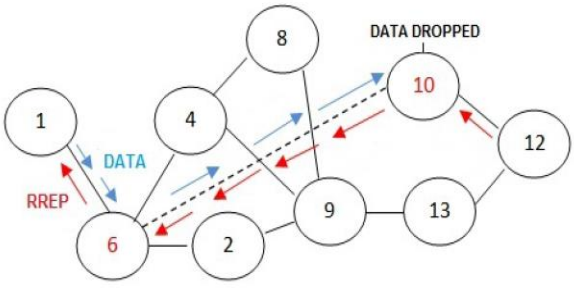


Figure 2. Single Wormhole Attack – Method 2

Enhanced HSAM Scheme

The implementation of E-HSAM is similar to that of HSAM; however, the major difference is found in the

sending of packets. HSAM splits the data packets into 48 byte chunks and sends them to the destination. However, it takes a reactive approach to securing the routes. Data chunks may still contain, in part, sensitive data which can still be stolen or tampered by intermediate malicious nodes before the route is discarded. In an attempt to eliminate any chance of unwanted data manipulation or data copy, we propose that mock packets be sent instead of the actual data chunks. The mock chunks contain fuller content which is not part of the original data packet. Therefore, if an attack occurred, the actual data packet will not be compromised. In our simulation, the number of mock packets sent is obtained by dividing the payload size of the actual packet by a split value of 48. The reasoning behind this comes from our treatment of the size of data packets. In order to obtain a reliable Limit of Tolerance, there is a need to obtain a sufficient number of cpkt and cmiss. For smaller data packet sizes, the packet should be split accordingly in order to gather enough cpkt and cmiss to provide a reliable ratio (rather than just a few cpkt and cmiss). The next difference is how routes will be avoided by the method. Instead of using a self-developed method to avoid the route containing malicious nodes, E-HSAM method utilizes a mechanism similar to that used by AODV for the sending of a RERR packet back to the sender. This mechanism will discard the suspicious route and automatically increment the routing table sequence number, then choose the next route. This slight modification to the RERR mechanism effectively avoids the route in question when data the integrity is compromised and the next available route is to be used.

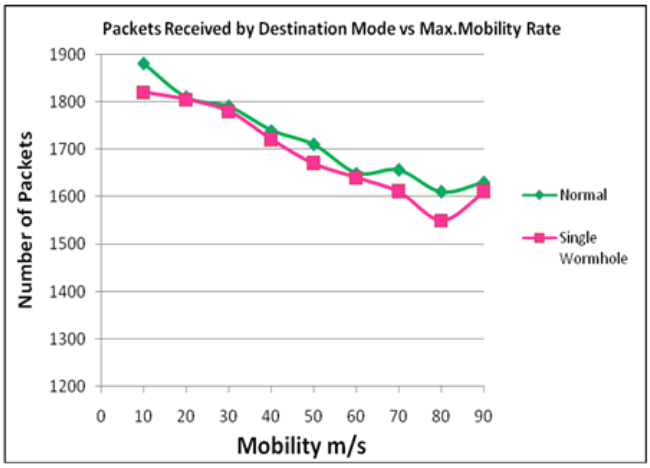
IV. RESULTS

Results on Single Wormhole Attacks

In this experiment, we have measured the performance metrics with respect to mobility of nodes. First, we observe the number of packets which are received by the destination node.

	No. of Packets	
Mobility	Normal	Single Wormhole
10	1880	1820
20	1810	1805
30	1790	1780
40	1740	1720
50	1710	1670
60	1650	1640
70	1656	1610
80	1610	1550
90	1630	1610

Table 1. Number of Packets received by Destination Mode (Normal & Single Wormhole)



Graph 1. Number of packets vs Mobility (Normal and Single Wormhole)

As depicted in Graph 1, the number of packets reaching the destination node in most of the trials is lower when the network is experiencing a single wormhole.

The Results we implement E-HSAM and compare it against HSAM under scenario 1. As discussed earlier, E-HSAM replaces the data chunks from the original method with mock packets containing no original data from the real payload. Moreover, as an attempt to increase efficiency, we modify how the sender is

notified of discovery of malicious routes. HSAM uses a similar procedure used in AODV to send notifications to the sender of a message. Consequently, we treat a wormhole link as a broken link and at the same time, we update our blacklist. Moreover, the HSAM method resends all the data packet chunks again with a new route whereas E-HSAM continues the next mock packet chunk with another route obtained from the routing tables, thereby increasing efficiency and reducing redundancy. First, we examine the number of packets received by the destination node as well as the packet delivery ratio.

Simulation Parameters

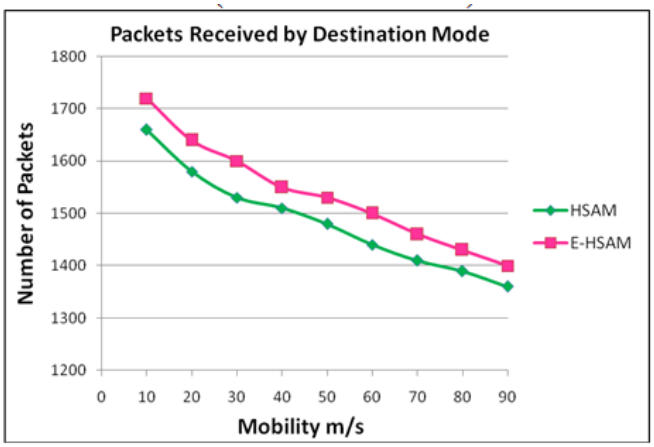
Table 2. outlines the main parameters for HSAM, E-HSAM and E-HSAM-AES:

Routing Protocol	AODV
Traffic Type	CBR
MAC Protocol	IEEE 802.11
Mobility Model	Random Way point
Number of Nodes	50
Default Wireless power (txpower_dBm)	15 dBm
Malicious Wireless power (txpower_dBm)	50 dBm
Max Movement Speed	10-90 m/s with 10 m/s increments
Simulation Terrain (m x m)	1000 x 1000
Simulation Time	120 mins
Packet Size	2048 Bytes (512 and 1024 can be used)

Table 2. Parameters for HSAM and E-HSAM

	No. of Packets	
Mobility	**HSAM**	**E-HSAM**
10	1660	1720
20	1580	1640
30	1530	1600
40	1510	1550
50	1480	1530
60	1440	1500
70	1410	1460
80	1390	1430
90	1360	1400

Table 3. Number of Packets received by Destination Mode (HSAM and E-HSAM)



Graph 2. Number of packets vs Mobility (HSAM and E-HSAM)

In Graph 2, it is observed that the number of packets which the destination receives is higher in E-HSAM compared to HSAM. This is understandable since E-HSAM automatically re-route the packets using the next available route and mock packet chunks are not dropped completely. On the other hand, HSAM drops the data packet chunks if there is a discrepancy with the data packet (i.e. if the hash value is no longer valid).

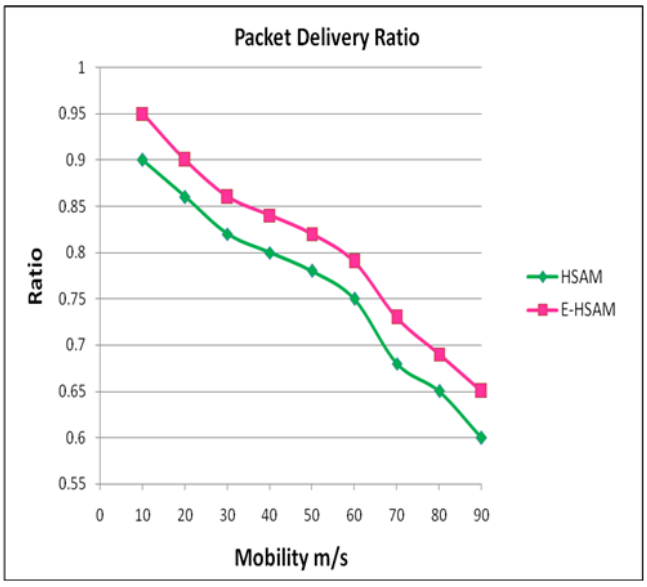
A similar observation is cascaded in Graph 3, where E-HSAM is shown to have a higher packet delivery

ratio compared to HSAM. As expected, the number of packets delivered as well as the packet delivery ratio steadily decreases as the mobility rate increases. This might be due to the fact that as nodes move around the simulated terrain with increased speed, connections have greater chance of failing since nodes can be out of range at any given time.

Next, we examine the number of broken links in both E-HSAM and HSAM. The results
are captured in Graph 4

	No. of Packets	
Mobility	HSAM	E-HSAM
10	0.9	0.95
20	0.86	0.9
30	0.82	0.86
40	0.8	0.84
50	0.78	0.82
60	0.75	0.79
70	0.68	0.73
80	0.65	0.69
90	0.6	0.65

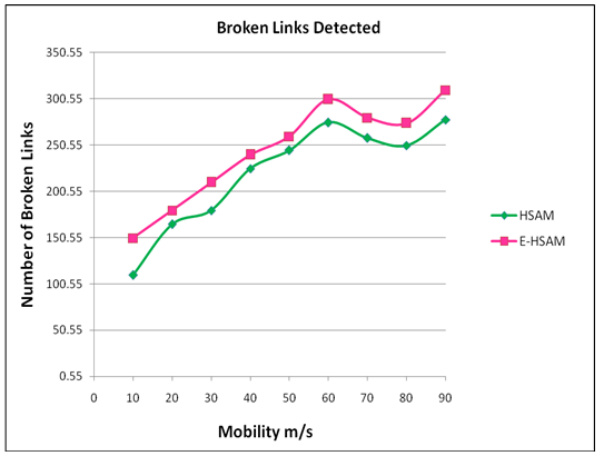
Table 4. Number of Packets received by Destination Mode (HSAM and E-HSAM)



Graph 3. Number of packets vs Mobility (HSAM and E-HSAM)

	No. of Broken links detected	
Mobility	HSAM	E-HSAM
10	110	150
20	165	180
30	180	210
40	225	240
50	245	260
60	275	300
70	258	280
80	250	274
90	278	310

Table 5. Number of Packets received by Destination Mode (HSAM and E-HSAM)



Graph 4. Number of packets vs Mobility (HSAM and E-HSAM)

V. CONCLUSION

In this, (1) enhanced HSAM with E-HSAM which improves the security of HSAM as well as its performance, Addressing the potential security weaknesses of HSAM leads to the design of E-HSAM. By replacing the actual data packets with mock packet chunks, E-HSAM can safely analyze the routes without worrying about data chunks being

copied. Moreover, we are able to increase the efficiency of the HSAM and make the algorithm adaptable to collaborative wormhole attacks.

VI. REFERENCES

[1]. R Jhaveri, A. Patel, J. Parmar, and B. Shah, \MANET Routing Protocols and Wormhole Attack against AODV," International Journal of Computer Science and Network Security, vol. 10, pp. 12{18, April 2010.

[2]. V Mahajan, M. Natu, and A. Sethi, \Analysis of wormhole intrusion attacks in manets," in IEEE Military Communications Conference (MILCOM 2008), San Diego, California, USA, pp. 1 {7, November 17-19, 2008.

[3]. F Nait-Abdesselam, \Detecting and avoiding wormhole attacks in wireless ad hoc networks," IEEE Communications Magazine, vol. 46, pp. 127 {133, April 2008.

[4]. Y-C. Hu, A. Perrig, and D. Johnson, \Packet leashes: a defense against wormhole attacks in wireless networks," in the 22nd Annual Joint Conference of the IEEE Com- puter and Communications (INFOCOM 2003), San Francisco, California, USA, vol.3, pp. 1976 { 1986, April 1-3, 2003.

[5]. C. H. Vu and A. Soneye, \Collaborative Attacks on MANETs: An Analysis of Collaborative Attacks on Mobile Ad hoc Networks". LAP Lambert Academic Publishing, Germany, 2010.

[6]. A Mtibaa and F. Kamoun, \Mmdv: Multipath and mpr based aodv routing protocol," in the IFIP 5th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2006), Lipari, Sicily, Italy, pp. 137{144, June 14-17, 2006.

[7]. H Xu, X.Wu, H. Sadjadpour, and J. Garcia-Luna-Aceves, \A uni_ed analysis of routing protocols in manets," IEEE Transactions on Communications, vol. 58, pp. 911 {922, March 2010.

[8]. N Meghanathan, \A manet multicast routing protocol for stable trees based on the inverse of link expiration times," in IEEE Consumer Communications and Networking Conference (CCNC 2012), Jackson, MS, USA, pp. 947 {951, January 14-17, 2012.

[9]. I. Khalil, S. Bagchi, and N. Shro_, \Liteworp: a lightweight countermeasure for the wormhole attack in multihop wireless networks," in International Conference on Dependable Systems and Networks (DSN 2005), West Lafayette, Indiana, USA, pp. 612 { 621, June 28 - July 1, 2005.

[10]. A. Singh and K. Vaisla, \A mechanism for detecting wormhole attacks on wireless ad hoc network," International Journal of Computer Science and Network Security, vol. 2, pp. 27{31, September 2010.

[11]. G. Mamatha and D. S. C. Sharma, \A Highly Secured Approach against Attacks in MANETS," International Journal of Computer Theory and Engineering, vol. 2, pp. 815{ 819, October 2010.

[12]. S. Choi, D. young Kim, D.-H. Lee, and J.-I. Jung, \Wap: Wormhole attack prevention algorithm in mobile ad hoc networks," in Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC 2008), Taichung, Taiwan, pp. 343 {348, June 11-13, 2008.

[13]. T. Hayajneh, P. Krishnamurthy, and D. Tipper, \Deworm: A simple protocol to detect wormhole attacks in wireless ad hoc networks," in Proceedings of the 3rd International Conference on Network and System Security (NSS 2009), Gold Coast, Queensland, Australia, pp. 73{80, October 19-21, 2009.

[14]. Bhandare A.S., Patil S.B. and Patil B.S., Modified AODV Protocol To Prevent MANET Against Black Hole Attack And Its Performance Analysis, International Journal of Advanced Scientific and Technical Research, Issue 3 volume 4, July-August 2013

[15]. Bhandare A.S., Patil S.B. and Patil B.S., Securing Manet Against Insider Attack-A Black Hole Attack & Its Performance Analysis, International

Journal of Computer Application, Issue 3, Volume 4 (July-August 2013)