A Secure Approach to Prevent Packet Dropping and Message Tampering Attacks on AODV-based MANETs

Arpana Akash Morey [1], Dr. Jagdish W. Bakal[2]

[1] *Information Technology Department, PIIT, Panvel, Maharashtra,India*
[2] *Principal, SSJCOE, Dombivali (E), Maharashtra, India*

Abstract-*In Mobile wireless communication and computing technologies, Mobile Adhoc Networks (MANETs) has growing demands in various applications which has also caused high and complicated security issues in transmission communication wireless networks are sensitive to problems like data tampering and dropping attacks less focused and addressed. This paper has enhanced the accepted protocol due to its ability to adapt rapidly in dynamic network environment with minimum overhead and small management packet size protocol named AODV with ADEHSAM. Our proposed work addresses the main issue breaking links in MANET caused by attacks by outperforming ADEHSAM in terms of normalizing overhead required in many other method to avoid attacks and throughput as well as number of broken links which shows ADEHSAM better than EHSAM.*

Keywords—*MANETs, malicious nodes, simulation, AODV, security, packet dropping attacks, message tampering attacks.*

I. INTRODUCTION

Distributed collaborations and information sharing are considered to be essential are considered to be the important operations in MANET to achieve the deployment goals such as sensing and event monitoring and type of wireless networks which are easily deployable because there is no requirement for setting up an infrastructure for their operational purposes. Collaboration will be productive only if all participants operate in a trustworthy manner. MANETs are usually deployed in harsh or uncontrolled environment, thereby heightening the probability of compromises and manufacturing as there is no centralized control unit to monitor the node operations on dynamic topology. These characteristics force a component node to be cautious when collaborating/communicating with other nodes as the behavior of node change with time and environmental conditions. Therefore establishing and quantifying behavior for ensuring proper operation of MANET. Focusing on operations to ensure that data cannot be tampered or dropped by malicious nodes or misbehaved links.

When routing operations are performed between a source and destination node pair in an AODV –based MANET, in this paper we address the problem of packet tampering and dropping attacks in MANETs. We follow up investigation of recently proposed solution to this problem (EHSAM [1]). As pointed out in [1], EHSAM evaluated experimentally using a network simulator showing considerable increase in end to end delays in less network density. A more efficient approach to secure the routes where mock packets are sent between sender and destination nodes in lieu of actual data chunks is used. In EHSAM the source node only sends RREQ packet and after receiving RREQ, it replies RREP and records sent and receive time but not maintaining each node's next hop node id and count value. In doing so, our enhanced ADEHSAM scheme each node maintains next hop node id and count value and source node or any intermediate node starts timer while forwarding the frame, Source node or any intermediate node overhears to next hop whether frame is forwarded or not. If overhearing message does not come within timer then increase the count while improving performance of ADEHSAM scheme.

The remainder of the paper is organized as follows. Section II discusses some related work on security schemes for MANETs targeted towards data dropping attacks and tampering attacks. In section III, the proposed ADEHSAM scheme for detecting and preventing malicious nodes against message tempering and packet dropping attacks in MANETs is described and contracted against the EHSAM scheme. In section IV, simulation results are presented. Finally in section V, we conclude the work and some future research directions.

II. RELATED WORK

In this section we present related work that have been dealing with detecting and/or preventing malicious nodes in MANETs that tamper or drop the routed data packets while in transit to the destination.

In [1], Mohammad S. Obaidat and Tssac Woungang, have proposed the EHASAM approach to secure the routes, where mock packets are sent between sender and destination nodes in lieu of actual data chunks, but not maintaining communication in intermediate nodes. Most of the above mentioned solutions against packet dropping or message tampering attacks in MANET deal with

specific individual type s of network layer attacks. None of them presented a mechanism to tackle different types of such attacks in parallel. An attempt to do so was recently proposed in [1] (called EHSAM scheme).

In [2], Gonzalez et al. has presented a method that detects a forwarding misbehavior of a malicious node by dropping a significant percentage of packets when participating in routing operation. The method that they used to ensure that a well behaved node is not falsely accused was based on a threshold value, which in turn determined the acceptable level of node's misbehavior. However, the problem of finding the optimal misbehavior threshold was not addressed. In [3] Dhanalakshmi and Rajaram have proposed a scheme that detects and isolates malicious nodes in MANETs, and then prevent them from dropping data packets. However, the complexity of their proposed algorithms was not disclosed.

In [4], Choi et al. proposed an approach that detects wormhole attack in MANETs, which is a DSR-based approach. This approach consisted of neighbor node monitoring technique and a worm hole rout detection method. This resulted in a scheme that does not rely on any specific hardware for node's location or time synchronization. However their approach was built on several unrealistic assumptions such as taking for granted that at the link layer, a node would always be able to monitor the ongoing transmissions even in case it is not the intended receiver. In [5], Nasser et al. addressed the weakness of watchdog protocol and proposed an intrusion detection scheme called ExWatchdog for wireless ad hoc networks. The scheme identifies the malicious nodes that can partition network by attempting to falsely reporting other nodes as misbehaving. Their approach was shown to greatly decrease overhead, but failed to increase throughput.

In [6],Yu et al. proposed a scheme that detects and defends byzantine attacks, which are the internal attacks on routing in MANETs. Their approach was based on using message and route redundancy during the route discovery phase. However, the resulting routing overhead was not investigated. In [7], Raj and Swadas proposed the DPRAODV scheme that provides detection and prevention against black-hole attacks in MANETs. For identifying the malicious nodes in their scheme the ALARM packets were used. Similarly, in [8],Li et al. introduced a method that employed ALARM packets to detect the nodes in wireless ad hoc networks that maliciously drop the packets during the routing operation. A subset of neighbors of each node was selected as observer to monitor the node's message forwarding behavior.

In [9], a scheme to prevent blackhole attacks on Expected Transmission Count (ETX)-based routing in MANETs was proposed, where the nodes were allowed to measure their neighbor's delivery ratio directly. However the efficiency of this scheme on other routing metrics was not investigated. In [10], Dhurandher et al. have proposed a solution to mitigate wormhole attacks in MANETs called an energy-efficient AODV-based scheme (so called E2SIW). In their scheme to detect presence of a wormhole in selected route, location information of nodes was used.

In [11], Jain et al. proposed a solution to problem of packet forwarding misbehavior in MANETs which is an AODV based scheme that detects and removes a chin of malicious nodes which attempted to drop a significant fraction of packets during routing operation. Similarly in [12], Tsou et al. proposed a DSR-based mechanism called CBDS that can detect malicious nodes launching black hole or grayhole attacks. The address of an adjacent node of a given node was used as the bait destination address to bait malicious nodes to reply to RREP messages, forcing their identification and isolation.

In [13], liu et al. proposed a message security scheme that was based on neural network. This technique deals with data integrity check while performing routing operation.

In this paper we propose an enhancement to the EHSAM protocol (referred to as ADEHSAM).

III. PROPOSED ADEHSAM PROTOCOL

The ADEHSAM scheme is designed to enhance the EHSAM scheme [1], which can find malicious node and ultimately broken links caused by malicious node and same time giving quality of service parameters better than EHSAM and preventing message tampering and packet dropping attacks at the network layer.

A. EHSAM

There is slight modification done in EHSAM as compared to HSAM. The EHSAM protocol sends packets from the source to destination nodes. The data packets at source node are split into 48 byte chunks and sent to the destination node in EHSAM algorithm [1].The data chunks may still contain in part, sensitive and private information which can be stolen or tampered by intermediate malicious nodes before the route is actually discarded.

In EHSAM protocol in an attempt to eliminate the possibility of unwanted data manipulation or data copy mock packets is sent in lieu of actual data chunks. The data chunks contain a filler content that is not the part of original data packet. Therefore, if an attack occurred, the actual data packet will not be compromised. The result of EHSAM shows that the number of mock packets sent is obtained by dividing the payload size of the

actual packet by 48. In order to obtain the reliable limit of tolerance, there needs to be sufficient number of cpkt and cmiss (counters). For smaller data packet sizes, the packet should be split accordingly in order to gather enough cpkt and cmiss (rather than just a few cpkt and cmiss) that would yield a more reliable ratio. The difference between HSAM and EHSAM scheme lies in manner in which the routes that contain malicious nodes can be avoided. Instead of using a self developed method as in H-SAM [1] to avoid such routes, EHSAM utilizes a mechanism similar to that used by AODV for sending a RERR control packet back to the sender node. The suspicious route (SR1) will be discarded by this mechanism and the next hop to the source will be added to a blacklist. Additionally, when the source sends another RREQ, the hop that is blacklisted from SR1 will not receive will not receive a RREP within that prescribed allotted time, the packet is assumed to be lost. The track of number of packets lost is kept by a counter (cmiss), and the principle of flow conservation is used to help deterring whether a selected route is misbehaving or not. This principle states that the input to a system must either be absorbed by that system or passed along to another system. For example, if a packet enters the system and does not leave the system, the system is either lying or the nodes are lying about the packet. A ratio (cmiss/cpkt) is calculated to determine a limit of tolerance, which is set to less than 20% for 'good' routes. The route is said to misbehave, if the ratio exceeds that limit.

In case of EHSAM [1] scheme there is possibility that the malicious nodes record the packets while still meeting above mentioned allotted maximum threshold time constraint. Further if the packets are just recorded, the hash values have not changed, thereby bypassing the security mechanism.

The above drawbacks suggest that different timing constraints can be tested to create more aggressive timings that are still acceptable within the normal AODV operations, leading to a more secured approach. Our proposed ADEHSAM scheme exploits this idea.

B. ADEHSAM Protocol

The major drawback of EHSAM is that it not maintaining track of intermediate nodes. It is only focusing on source and destination node communication. In our proposed approach of AEHSAM, we have maintained status of each packet for each intermediate node with next hop node id and count value. This statistics gives better control flow mechanism against attacks.

ADEHSAM also construct mock data frames by analyzing actual data to be sent with Source node address, destination node address, and message to be sent and hash code. Whenever either source node or any intermediate node has to forward any data frame, it always initializes timer keeping sending while forwarding the frame. Then source node or any intermediate node overhears to next hop whether frame is forwarded or not. This is main difference between our approach and EHSAM. Next successive is also responsible to acknowledge whatever data packets are received from corresponding nodes. This approach gives assurance to sender node which can be any node i.e. source or intermediate node. At same time we have also kept expecting time for overhear message within which receiver node has send to send overhear message back to sender node. If overhearing message does not come within timer set for it then source node increase the count. The count value maintained by every forwarding node for not receiving overhear message, is exceeding than threshold value set, then ADEHSAM protocol will warn topology about this misbehavior of node. So our protocol will send alarm message sent to source node with misbehaving node id. Alarm message sent such way the RERR is sent to Source. Source node maintains the node black list of such misbehaving nodes. So whenever any source node present in network wants to start or use existing routing table entries for next route discovery process, it will check first black list. If any entry found regarding node or path in blacklist, it remove path which having these nodes. Any intermediate node checks for destination address and it is not, then forwards to next hop. When it matches with destination node, packets gets reconstructed by validating hash value proves the path is OK i.e. malicious node free path and accordingly acknowledge packets goes to source node for informing same. If it is not matched then ADEHSAM maintain that path as broken link path.

The pseudo-code of the ADEHSAM algorithm is given in Fig.1.

-A RREQ is sent by the source (S)
-Source S receives RREP from the destination (D)
-Route from S to D through regular AODV protocol
-Each node maintain table
-Mock packets are sent before sending actual data packets to check the path is malicious or not
-Mock data packets are split into 48 bytes chunk
1. Source node S creates mock packets of 18 bytes
2. for each packet t
    2.1 Construct mock data frame.
    2.2 Source node or any intermediate node starts timer while forwarding the frame.
3. Node n overhears to next hop.
    3.1 If OverhearingMessageArriTime>ThreTimer then increase the count
    3.2 End if
4. If CountValue>T0hretimer
    4.1 Then send alarm message to source node

4.2 Send misbehaving node id
4.3 Send RERR is sent to Source node.
5. Source node maintain node black list
5.1 When next route discovery phase starts then
Source node remove path which having these nodes
6. Intermediate node D checks for destination address
6.1 If D is matched
6.2 then it forwards frame to next hop.
6.3 Packets are reconstructed at destination.
6.4 hash value is computed.
7. If hash matched
7.1 then path is ok
7.2 else then path is broken path
7.3 destination node D sends acknowledgement to source node

Fig.1. ADEHSAM algorithm

IV. PERFORMANCE EVALUATION

Ns2 is used as the simulation tool to evaluate the performance of the proposed ADEHSAM SCHEME. We simulated a black hole attack in which the integrity of data packets that traverse through the MANET is compromised. Simulation files contain topology of 10 nodes with mobility speed. Node 0 is chosen as source node and Node 7 is chosen destination node. Node 1 is chosen to be malicious node designed intentionally to compromise the integrity of the data packets and to misbehavior to perform broken link attack against our approach. The malicious node is also in communication range of the source and destination nodes in order to ensure that some of the data packets will go through them. In the ADEHSAM scheme, if the nodes are sending overhear message within the expected time i.e. threshold time, whole system will work as that used in AODV.RERR control packets are used to signal the source that route should no longer be used and for broken link consideration if hash value is not matched coming in order form source to destination. The routing table sequence number will then be incremented and the next available route will be chosen for routing.
Other simulation parameters are captured in Table 1.

Table 1: Simulation Parameters

Terrain dimension	**1000m×1000m**
Number of nodes	**10,20,30,40,50,60,70**
MAC protocol	**IEEE 802.11**
Traffic Type	**CBR**
Network layer routing protocol	**AODV**
Simulation Time	**150 minutes**
Mobility model	**Random way point**
Max movement speed	**10-90m/s with 10m/s increments**
Packet Size	**2048**

The performance of the proposed ADEHSAM scheme was compared against the EHSAM scheme by varying the node's mobility speed, on the basis of the following performance metrics: (1) Throughput, i.e. the average rate of successful message delivery over a communication channel(measured as bits per second(bps)). (2)Packet delivery ratio, i.e. the ratio between the number of packets delivered to the destination node and the number of packets originated from the source node. (3) Normalized Routing Load: the total number of routing packet transmitted per data packet. It is calculated by dividing total number of routing packets sent (includes forwarded routing packets as well) by the total number of data packets received. (4) Number of broken links: if the hash value is compromised, the link will be deemed to be broken and the source node will be choosing the next available route.

The first parameter used to analyze the performance of EHSAM and ADEHSAM is throughput shown in figure2. The result shows significant improvement in throughput as compared to EHSAM. In EHSAM because of sporadic fluctuations be due to the fact that some of the node might be out of range at the time of delivery, the throughput is not getting better than HSAM, but our ADEHSAM shows improvement in this bandwidth utilization.

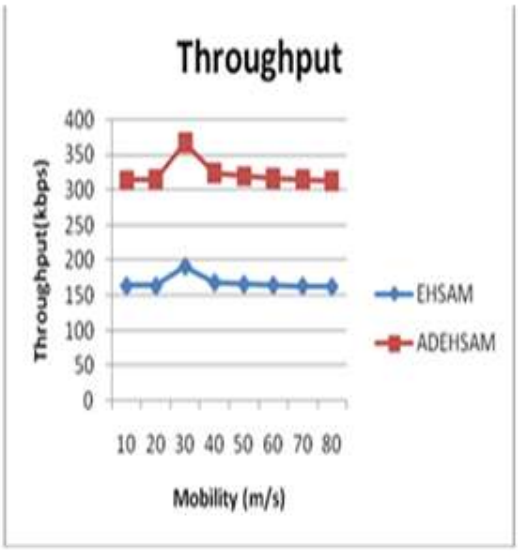

Fig.2 Throughput to destination vs. Mobility rate

The next performance metric used in the analysis of our scheme is the number of packets received at the destination. Figure3 depicts the effect of this parameter on the node mobility in the network. It can be observed that ADEHSAM generates more received packets at destination than the HSAM scheme does. From the graphs it can be said that our ADEHSAM approach is able to find malicious node and preventing the same from being part of path and reroute the attacked packets using the next available trusted route. On the other hand, HSAM continuously keeps sending and using packets to same route identified by malicious node and hence packets dropping take place which is affecting on packet delivery ratio. It is also observed that in both schemes, the number of packets received at the destination steadily decreases as the mobility rate increases. This is due to the fact that as nodes moved around quicker, there is a great chance that connections fail since it may occur that nodes become out of range. But, at higher mobility speed both the schemes gives better performance again.

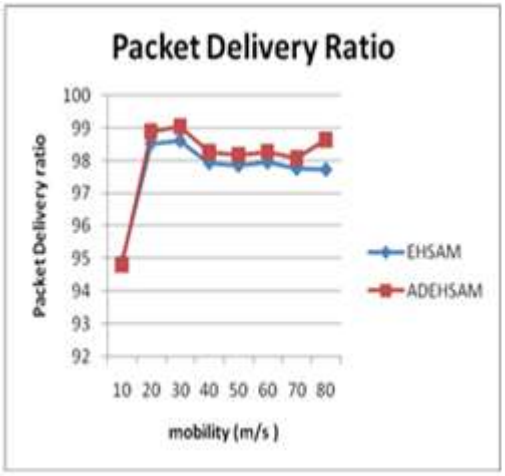

Fig.3 Packet Delivery Ratio vs. Mobility rate

The next performance metric is normalized routing load (NRL) which is defined as total number of routing packet transmitted per data packet. EHSAM approach has put extra routing information which causing extra load on delivery of packet and it is consuming bandwidth for extra feature in packet header which we have avoided in ADEHSAM. So in ADEHSAM NRL performance is better than EHSAM. As topology density differs NRL performance also gets affected as in sparse area, it is decreasing in both the schemes and higher in low and high density.

Next parameter is number of broken links detected during the delivery of packets. As we have already discussed that EHSAM sends only RERR control packets. Once the packet has been compromised, the route is assumed to be misbehaving. So it is assumed that the link will be broken and hence, will no longer be used and the next available recommended route will be chosen, but in ADEHSAM the broken link will be decided when packets come to destination and hash sequence is not matching with source with effect of node's mobility, in presence of malicious nodes.

It is observed that the number of broken links is reflective of the node movement within the specified terrain. So the number of broken links is high vs. the mobility rate increases, indicating the higher chance of lost connections due to mobility. In our ADEHSAM scheme, the higher number of broken links compared to that of EHSAM scheme. This is obvious because, in EHSAM, RERR control packets are used to decide link as broken which many times finds follows infected path having malicious node. But ADEHSAM sends overhear message back to sender which ultimately finds more links infected.

V. CONCLUSION

In this paper we proposed the ADEHSAM scheme, which is an enhancement of highly secured approach against attacks on MANETs (EHSAM) scheme. Simulation results showed that: (1) ADEHSAM performs better than EHSAM in terms of packet delivery ratio; (2) ADEHSAM finds a higher number of broken links, hence packets that went through the malicious nodes were redirected using alternate routes as opposed of being completely dropped. In future, we plan to adopt ADEHSAM against other well-known methods for preventing/avoiding misrouting and routing table overflowing causing non-existent node data is sent in the network, more ever computing and degrading the rate and creating so many routes to nodes that do not exist in the network.

REFERENCES

[1] Mohammad S.,Isaac Woungang,, Sanjay Kumar Dhurandher (2013) "Preventing Packet Dropping and Message Tampering Attacks on AODV-based Mobile Ad Hoc Networks" IEEE 2012.

[2] O. F. Gonzalez, G. Ansa, M. Howarth, G. Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering, Vol. 2, No. 1, pp. 181-192, June 2008.

[3] S. Dhanalakshmi, M. Rajaram, "A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET", IJCSNS International Journal of Computer Science and Network Security, Vol. 8, No.10, Oct., 2008.

[4] S. Choi, D-Y. Kim, D-H Lee, J-I.Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", International Conference on Sensor Networks, Ubiquitous, & Trustworthy

Computing, (SUTC' 08), June 11-13, Taichung, Taiwan, pp.343-348, 2008.
[5] N., Nasser and C. Yunfeng, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks", IEEE Intl. Conference on Communications, Vol. 07, No. 24-28 June, pp. 1154-1159, 2007.
[6] M. Yu, M. Zhou; W. Su, "A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Vol. 58, No. 1, Jan., pp.449 – 460, 2009
[7] P. N. Raj and P. B. Swadas, " DPRAODV: A Dynamic learning system against blackhole attack in AODV based MANET", Intl. Journal of Computer ScienceIssues, Vol. 2, 2009
[8] X. Li, R. Lu, X. Liang, X. Shen, "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks", Proc. of IEEE Intl. Conference on Communications (ICC'11), Kyoto, Japan, June 5-9, 2011.
[9] K. Osathanunkul, N. Zhang, "A countermeasure to black hole attacks in mobile ad hoc networks", Proc. of Intl. Conference on Networking, Sensing and Control, Delft, Netherlands, Apr. 11-13, pp. 508-513, 2011
[10] S. K. Dhurandher, I. Woungang, A, Gupta, B. Bhargava, "E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks", Accepted Nov. 29, 2011,To appear in the proc. of the 8th Intl. Workshop on Heterogeneous Wireless Networks (HWISE'12), in conjunction with AINA-2012, March 26-29, 2012, Fukuoka, Japan.
[11] S. Jain, M. Jain, H. Kandwal, "Advanced algorithm for detection and prevention of cooperative black and grayhole attacks in mobile ad Hoc networks", Intl. Journal of Computer Applications, Vol. 1, No. 7, pp. 37– 42, Feb. 2010.
[12] P-C Tsou, C. J-M Chang, Y-H Lin, H-C Chao, J-L Chen, "Developing a BDSR scheme to avoid blackhole attack based on proactive and reactive architecture in MANETs", ICACT 2011, Feb. 13~16, Korea, 2011 .
[13] C. Liu, I. Woungang, H-C Chao, S. K. Dhurandher, T-Y Chi, M. S. Obaidat, "Message Security in Multipath Ad Hoc Networks using a Neural Network-Based Cipher", To appear in the Proc. of the IEEE GLOBECOM 2011, Dec. 5-9, Houston. Texas, USA, 2011.
[14] G. S. Mamatha and S. C. Sharma, "A highly secured approach against attacks in MANETs", Intl. Journal of Computer Theory and Engineering, Vol. 2, No. 5, Oct. 2010.
[15] Global Mobile Information Systems Simulation Library (GloMoSim), http://pcl.cs.ucla.edu/projects/glomosim/ (Last visited Dec. 3, 2011).