Worm Secure Protocol for Wormhole Protection in AODV Routing Protocol

Vijay Kumar
Dept. of Computer Science
Guru Nanak Khalsa College Karnal – India

Ashwani Kush
Dept. of Computer Science, University College
Kurukshetra University, Kurukshetra - India

ABSTRACT
A Mobile Adhoc Network (MANET) is characterized by mobile nodes, multihop wireless connectivity, Non infrastructural environment and dynamic topology. In Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Stable Routing, Security and Power efficiency are the major concerns in this field. The ad hoc environment is accessible to both legitimate network users and malicious attackers. The proposed scheme named as worm_secure is intended to incorporate security aspect on existing protocols .This paper checks one of the common attack on MANET as wormhole and tries solving the situation. Scheme has been incorporated on AODV and results have been calculated using NS2.

Keywords
Ad hoc Networks, Modified AODV, AODV, Performance evaluation

I. INTRODUCTION
An Ad hoc wireless network [1,2] is a collection of mobile devices equipped with interfaces and networking capability. It is adaptive in nature and is self organizing. A formed network can be deformed and again formed on the fly and this can be done without the help of system administration. Each node may be capable of acting as a router. Applications include but are not limited to virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in exhibitions, conferences and meetings, in battle field among soldiers to coordinate defence or attack, at airport terminals for workers to share files etc. Although security has long been an active research topic in wired networks, the unique characteristics of Ad Hoc networks present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic topology. Some of the main security attributes [1,2] that are used to inspect the security state of the mobile adhoc network are : Availability, Integrity, Confidentiality, Authenticity, Non repudiation, Authorization, Anonymity. The wormhole attack is one of the most powerful attacks since it involves the cooperation between two malicious nodes that participate in the network. In this paper a new scheme called worm_secure has been used to take care of wormhole attack. Rest of the paper is organized as: Section 2 describes wormhole detection, recent studies have been discussed in Section 3, proposed scheme has been elaborated in Section 4, working and detection has beend escribed in section 5, simulation results have been explained in Section 6 and Conclusions end the paper.

2. WORMHOLE ATTACK
The wormhole attack is one of the most powerful attacks since it involves the cooperation between two malicious nodes that participate in the network. One attacker, say node A, captures routing traffic at one point of the network and tunnels them to another point in the network, say to node B, that shares a private communication link with A. Node B then selectively injects tunnelled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. For case study wormhole has been introduced in AODV [9,10,11] Wormhole attack is not that difficult to set up, but still can be immensely harmful for a MANET. Moreover, finding better techniques for detection of wormhole attacks and securing AODV against them still remains a big challenge in Mobile Ad-hoc Networks. Working of AODV in the presence of wormhole attack is described using Figure1.

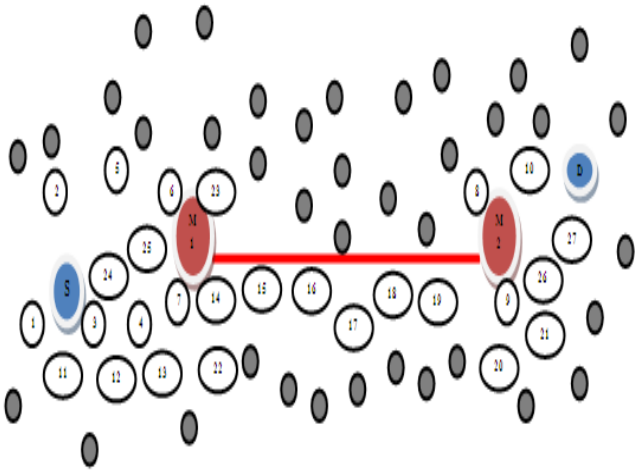

Figure1. Wormhole attack in AODV

In Figure 1 during path discovery process, sender "S" broadcasts RREQ to a destination node D. Thus 24, 1, 2 and 3 neighbours of S, receive RREQ and forward RREQ to their neighbours. Now the malicious node M1 that receives RREQ forwarded by 25 records and tunnels the RREQ via the high-speed wormhole link to its partner M2. Malicious node M2 forwards RREQ to its neighbour 10, 9 and 26. Finally 26 forwards it to 27 and it will forward it to destination D. Thus, RREQ is forwarded via S-24-25-26-27-D. On the other hand, other RREQ packet is also forwarded through the path S-4-13-22-14-15-16-17-18-19-20-21-27-D. However, as M1 and M2 are connected via a high speed bus, RREQ from S-24-25-26-27-D reaches first to D. The wormhole attack exits in the route

selected in AODV according to shortest path S-24-25-26-27-D. After getting the route requests to destination from the sender destination it will unicast a route reply packet to source "S" using shortest path. Source will select the shortest path as best route from source to destination for transmitting the data and other routes will be discarded. In above example destination "D" ignores the RREQ that reaches later and chooses D-27-26-25-24-S to unicast an RREP packet to the source node S. As a result, S chooses S-24-25-26-27-D route to send data that indeed passes through malicious M1 and M2 nodes that are very well placed in comparison to other nodes in the network.

3. RECENT WORK

MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured with ease. To address these concerns, several secure routing protocols have been studied. Dahill et al. proposed ARAN [3], it assumes managed-open environment, where there is a possibility for pre-deployment of infrastructure. It consists of two distinct stages. The first stage is the certification and end-to-end authentication stage. In this, source gets a certificate from the trusted certification server and then using this certificate signs the request packet. Each intermediate node in turn signs the request with its certificate. The destination then verifies each of the certificates, thus the source gets authenticated and so do the intermediate nodes. The destination node then sends the reply along the route reverse to the one in the request; reply signed using the certificate of the destination. The second stage is a non-mandatory stage which is used to discover the shortest path to the destination but this stage is computationally expensive. It is prone to reply attacks using error messages unless the nodes have time synchronization. Papadimitratos and Haas [4] proposed a protocol SRP that can be applied to several existing routing protocols. This protocol assumes a security association between source and destination nodes. Intermediate nodes do not need to cryptographically validate the control traffic. It adds a SRP header to the base routing protocol, DSR or AODV, request packet. SRP header has three important fields QSEQ which helps prevent replay of old outdated requests, QID and random number which helps prevent fabrication of requests and a SRP MAC which ensures integrity of the packets in transit. SRP requires that, for every route discovery, source and destination must have a security association between them. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected and any malicious node can just forge error messages with other nodes as source. ARIADNE [5], is based on DSR [6] and TESLA [7]. It prevents attackers/compromised nodes from disrupting uncompromised routes comprising of benign nodes. It uses highly efficient symmetric key cryptography. It does not guard against passive attackers eavesdropping on the network traffic. It does not prevent an attacker from inserting data packets. It is vulnerable to active-1-1 attacker that lies along the discovered route, who does not forward packets and does not generate ERROR if it encounters a broken link. It also requires clock synchronization, which we consider to be an unrealistic requirement for adhoc networks. Perlman proposed a link state routing protocol [8] that achieves Byzantine Robustness. Although the protocol is highly robust, it requires a very high overhead associated with public key encryption. Zhou and Haas [9] primarily discussed key management. They devote a section to secure routing, but essentially conclude that "nodes can protect routing information in the same way they protect data traffic". They also observe that denial-of-service attacks against routing will be treated as damage and routed around. Some work has been done to secure adhoc networks by using misbehavior detection schemes [10]. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving; and second has no real means to guarantee the integrity and authentication of the routing messages. Looking at the work that has been done in this area previously, it seems that the security needs for adhoc networks has not been yet satisfied. Most of the work done around using Hashing techniques is around authenticating messages and route table entries. Bayya et al. [11] demonstrate the use of hashing as part of password based authenticated key exchange. The problems in this protocol are the need of a strong shared secret and the need to constantly change the shared secret which in turn may prove to be computationally expensive. Yih-Chun Hu et al. [12] used symmetric cryptography to secure adhoc networks by using one way hash chains or Markle hash tree as part of SEAD protocol for proactive routing. The problems identified with SEAD protocol are no provision of a secure initial key distribution, greater network traffic and count-to-infinity problem. Zapata [13] in its proposed protocol uses a new one-way hash chain for each Route Discovery to secure the metric field in an RREQ packet. It also uses asymmetric cryptography to initially authenticate participating nodes.

4 WORM_SECURE

The following assumptions are taken in order to design the proposed algorithm.

1. A node interacts with its 1-hop neighbours directly and with other nodes via intermediate nodes using multi-hop packet forwarding.
2. Every node has a unique id in the network, which is assigned to a new node collaboratively by existing nodes.
3. The network is considered to be layered.
4. Source and Destination node will not be wormhole node.

Steps of Worm_Secure Algorithm

1. *Source node sends route request*
2. *Intermediate node forward request*
3. *If intermediate node is wormhole it tunnels the packet to next end*
4. *If packet reaches destination it send reply to source*
5. *If wormhole receive reply then it tunnels to another wormhole end*
6. *Reply reaches source node and start transmitting data packet through shortest path*
7. *Then source node send path message to all intermediate node upto destination*
8. *Intermediate node receive path message and select 2nd hop path node as target node*
9. *It sends route message to one hop neighbour along with other nodes in path*
10. *One hop neighbour receive route message and find alternate path to target node*
11. *If hop count of alternate path > hop count threshold*
12. *Then previous hop node of target is detected as wormhole node*
13. *Else no wormhole present.*

5. WORMHOLE DETECTION

The basic idea of the Worm_Secure protocol is to detect the wormhole node using the algorithm to find alternative routes to a target node that does not pass through the wormhole. In Worm_Secure protocol after getting the route from the source to destination in routing table sender will set a second hop

node as a target node from the route which is stored in routing table. Sender will send "hello" message to its one hop neighbour node after getting "hello" message from one hop neighbour node, reply will be received by sender. All the details of neighbour and target hop node like node id, hop_count from target to sender are stored in the neighbour table at sender node. Now check whether the wormhole node exist or not in the path from sender to target node. Longest route alternate route will be checked if the number of hop_count > threshold value (i.e 7 in our proposed plan) then there exists a wormhole node in the path. Because in the general scenario of MANET a target node must be reached with 1 to 4 hop_count nodes. If it is greater than this, it is assumed that there is a wormhole attack. To reduce the false positive occurrences, threshold value will be fixed. Once wormhole node is detected, a worm_message is sent to all nodes in where all nodes get the node id of the wormhole nodes. After getting the information about wormhole nodes the route will be removed from the routing table and new alternative route will be selected.

WORKING OF WORM_SECURE

For describing the working of Worm_Secure four steps are discussed as Route Request, Route Reply, Wormhole nodes Detection and Route Maintenance:

I. *Route Request (RREQ)*

Sender "S" broadcast route request to search the shortest route to destination. Route request will be broadcasted in the manner of multi node hops. In Figure 2 during path discovery process, sender "S" broadcasts RREQ to its neighbouring nodes i.e. 24, 1, 2 and 3. The neighbouring nodes will forward RREQ further to their neighbours. Now the malicious node M1 that receives RREQ forwarded by node 25 records and tunnels the RREQ via the high-speed wormhole link to its partner M2. Malicious node M2 forwards RREQ to its neighbour 10, 9 and 26. Finally node 26 forwards it to 27 and it will forward it to destination D. Thus, RREQ is forwarded via S-24-25-26-27-D.

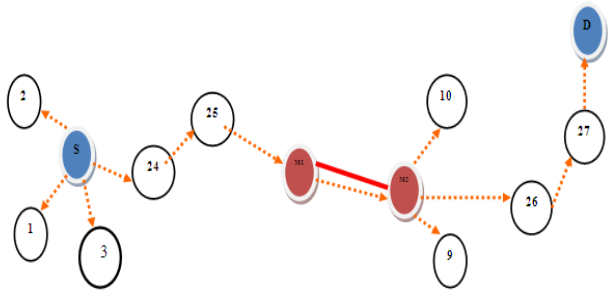

Figure 2 Route Request Process

II. *Route Reply (RREP)*

After getting the route request to destination from the sender, destination will unicast a route reply packet to source "S". Source will select the shortest path as best route from source to destination for transmitting the data and other routes will be discarded. In our example destination D ignores the RREQ that reaches later and chooses D-27-26-25-24-S to unicast an RREP packet to the source node S. As a result, S chooses S-24-25-26-27-D route to send data that indeed passes through malicious M1 and M2 nodes that are very well placed compared to other nodes in the network.

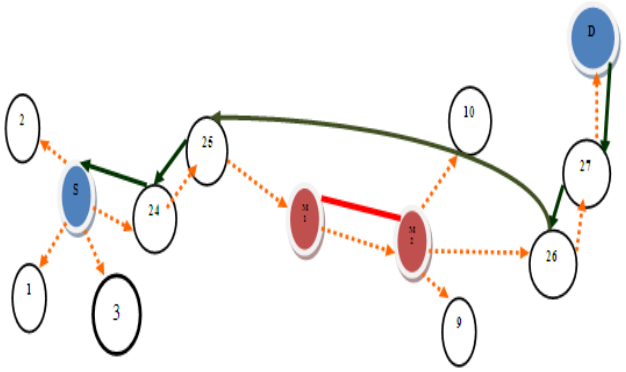

Figure 3 Route Reply Process

III. *Wormhole Node Detection*

In Figure 4 the sender node *S* wants to communicate with node *D* using the shortest path (*S-24*-25-26-27-*D*). Note that there are five hops to the destination. Obviously this route passes through the wormhole and nodes *25* and 26 are connected through the wormhole nodes *M*1 and *M*2 without being aware of this fact.

Step(1): Node *S* will set the target node *i.e. 25 as a second hop.*

Step(2): Node *S* will broadcast a "hello" message to its one hop neighbours.

Step(3): Node *S* will receive replies from one hop neighbour nodes 24, *1*, *2*, and *3* and add them to its one-hop neighbours' list.

Step(4): Node *S* will broadcast its neighbours' list and ask nodes *1*, *2*, and *3* to find a route to the target node 25, which does not go through any node from the neighbours' list. Nodes *1*, *2*, and *3* are required to find a route to 25 that does not go through nodes *S*, 24, *1*, *2* and *3*. In our example nodes *1*, *2*, and *3* will find routes to 25 as shown in Figure 4 (*1-11-12-4-*25), (*2-5-25*), (*3-4-25*) and they will inform the sender *S* that the lengths of the routes to *25* are 4, 2, and 2 hops, respectively. The sender will pick the longest route as the "selected route" with 4 hops here, and compares it with 2 hops.

Step(5): In this example the length of the selected route 4 which is not greater than the sensitivity parameter. Thus, no wormhole is detected.

Step(6): The next hop – node 24 – will become the new "sender" (there is now a new target as well – node 26).

Step(7): Steps numbered 1 to 6 will be repeated by the new sender until either a wormhole is detected or the destination node is reached.

In Figure 4 node *24* will pick nodes *3* and *4*. The routes from nodes *3* and *4* to *26* (excluding nodes *S*, *3*, *4* and 25) will be (*3-12-13-7-*26) and (*4-13-7-*26) respectively. The selected route 4 which is again not greater than 7. Thus the wormhole is still not detected and the new sender will be the next hop, node 25. Node 25 will have nodes *24*, *4*, *6*, *7*, *8*, *9*, *10*, and 26 in its one-hop neighbours list. Note that the replies from nodes 26, *8*, *9*, and *10* are transmitted by *M*1. Nodes *4*, *6*, *7*, *8*, *9*, and *10* will all try to find routes to node 27 that do not pass through the one-hop neighbours' list of node 25. Since all the nodes that are within the range of *M*2 (nodes *26*, *8*, *9* and *10*) cannot be in the route to the target node, any route from nodes *4*, *6*, or *7* will not pass through the wormhole and it will be long enough to detect the wormhole. The selected route will be from node *4* that is (*4*, *13*, *22*, *14*, *15*, *16*, *17*, *18*, *19*, *20*, *21 and 27*) which has 11 hops. Thus in this case we have 11

which are greater than 7 and consequently node *25* will inform node *S* that a wormhole has been detected.

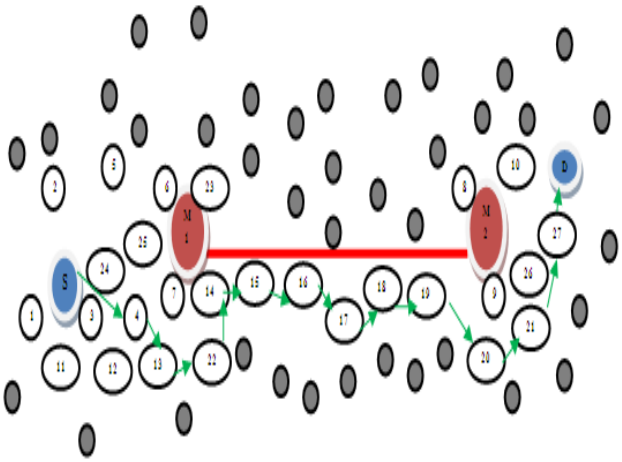

Figure 4 Route Establishing Process

IV. *Route Maintenance*

Whenever a node detects a link break from link layer acknowledgements or HELLO beacons, the source and end nodes are notified by propagating an RERR packet similar to DSR. One optimization possible in AODV route maintenance is to use an expanding ring to search and control the flood of RREQ and discover routes to unknown destinations. The main advantage of AODV is that it avoids source routing thereby reducing the routing overload in large networks. Further, it also provides destination sequence numbers which allows the nodes to have more up-to-date routes. However, AODV requires bidirectional links and periodic link layer acknowledgements to detect broken links. Further, it has to maintain routing tables for route maintenance unlike DSR.

6. PROPOSED ALGORITHM ANALYSIS

The working of routing largely depends upon successful transmission of packets to the destination. This requires proper selection of Routing path and algorithm. AODV and Modified AODV have been used in this paper for routing solutions. All the simulations have been performed using Network Simulator NS-2.32 [2] on the platform Fedora 13. The traffic sources are CBR (continuous bit–rate). The source-destination pairs are spread randomly over the network. The mobility model uses 'random waypoint model' [9] in area 1000m x 750m with 25, 50, 75 and 100 nodes. During the simulation, each node starts its journey from a random spot to a random chosen destination. Once the destination is reached, the node takes a rest period of time in second and another random destination is chosen after that pause time. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. Different network scenario for different number of nodes and different node transmission range are generated.

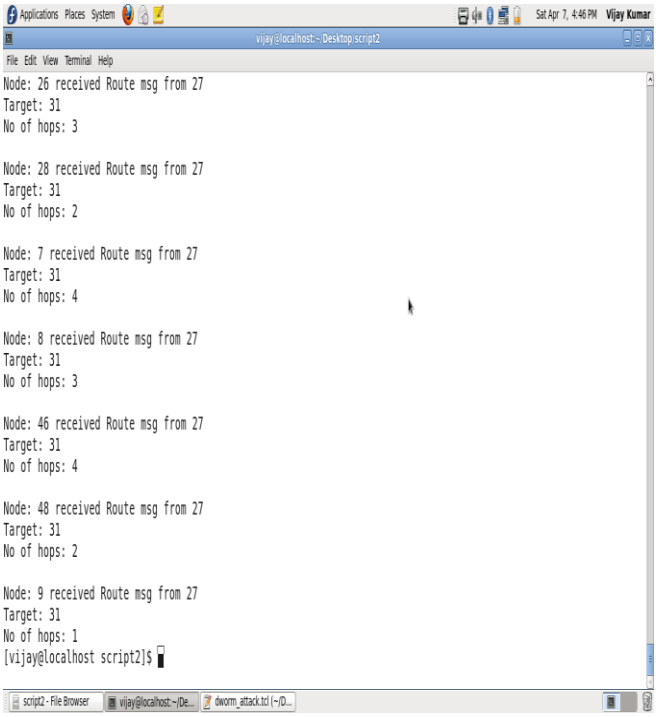

Figure 5: Snapshot of TCL script without Worm hole Attack

Figure 5 shows the snapshot of running TCL script's output with Worm_Secure without any wormhole attack. In the above snapshot the number of hops is less than 7.

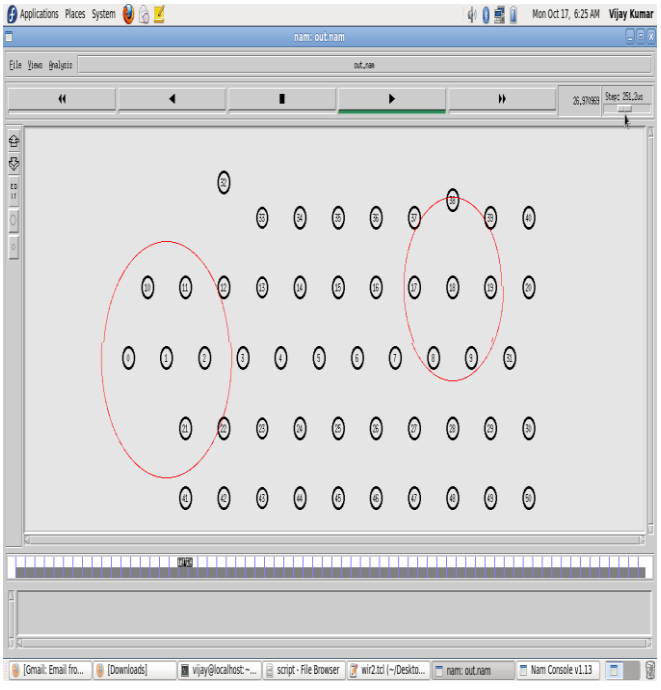

Figure 6: Snapshot of NAM without Worm hole Attack

Figure 6 shows the snapshot of running .NAM output of Worm_Secure without any wormhole attack.

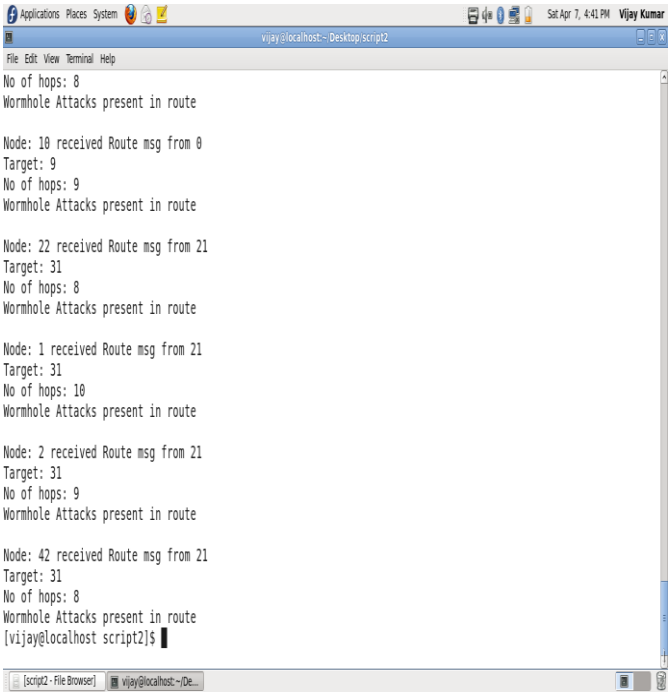

Figure 7: Snapshot of TCL output with Worm hole Attack

Figure 7 shows the snapshot of running TCL script of Worm_Secure with wormhole attack. In the above snapshot the where number of hops is greater than 7 the proposed Worm_Secure detect the wormhole attack and display the massage about the wormhole attack. After detection the wormhole attack it will change the route without any wormhole node in the route.

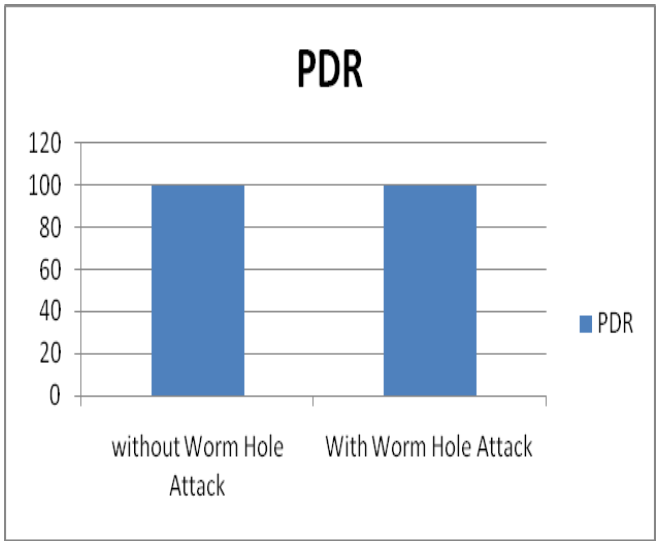

Figure 8: PDR with and without wormhole attack

Figure 8 shows the performance of Worm_Secure on the metric Packet Delivery Ratio. In this figure the result of PDR is same in the case of wormhole attack and without wormhole attack. This figure proves that solution of detection and stop the working of wormhole attack in MANET is working effectively.

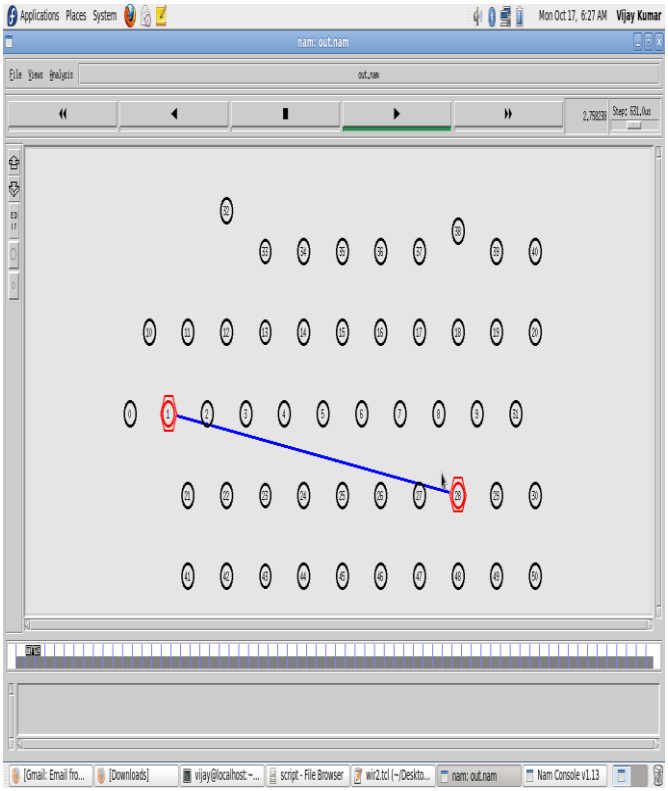

Figure 9: Snapshot of NAM output with Worm hole Attack

Figure 9 shows the snapshot of two wormhole nodes are working as an attacker. Node 1 and Node 28 are malicious nodes. A tunnel is also established between both wormhole nodes.

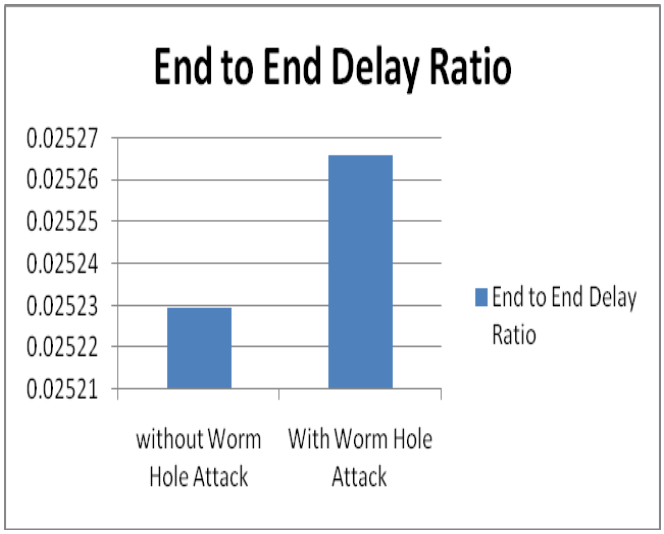

Figure 10: End to End Delay with or without wormhole attack

Figure 10 shows the performance of Worm_Secure on the metric end to end delay Ratio. In this figure the result of end to end delay ratio is high in the case of with wormhole attack. The main reason of that in case of wormhole attack proposed algorithm will detect the wormhole attack and the route. This route will be long route compare to the existing normal route without wormhole attack.

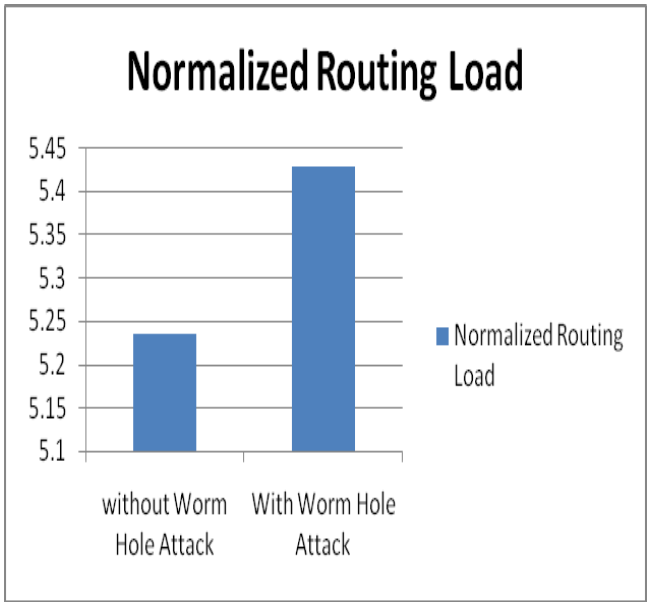

Figure 11: Normalized Routing Load with or without wormhole attack

Figure 11 shows the performance of Worm_Secure via the metric Normalized Routing Load. In this figure the Normalized Routing Load is high in the case of with wormhole attack in the comparison of without wormhole attack.

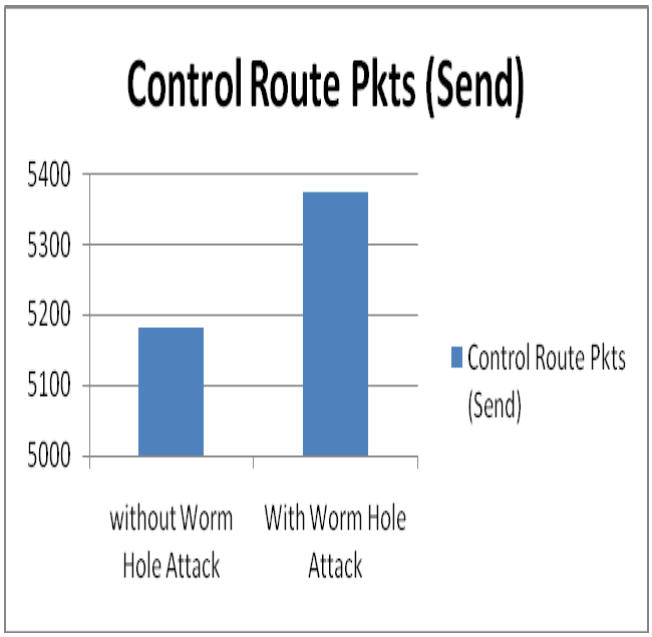

Figure 12: Control Packets Sent with and without wormhole attack

Figure 12 shows the performance of Worm_Secure on the metric Control Route Packets (Send). In this figure the Control Route Packets (Send) is high in the case of with wormhole attack in the comparison of without wormhole attack.

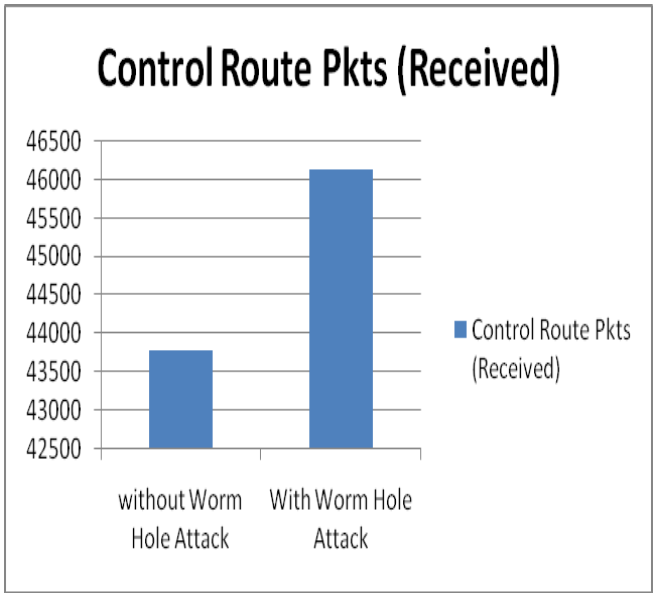

Figure 13: Control Packets Received with and without wormhole attack

Figure 13 shows the performance of Worm_Secure on the metric Control Route Packets (Received). In this figure the Control Route Packets (Received) is high in the case of with wormhole attack in the comparison of without wormhole attack.

7. CONCLUSIONS

A new algorithm has been proposed in this paper named as Modi_AODV. This algorithm is basically the enhanced or better algorithm in comparison to existing AODV. Here NS2.32 simulator on Fedora 13 is used for the measurement of the results between existing AODV and Modi_AODV. The results shows clearly that the PDR, end to end delay ratio and throughput is better and giving stable performance in the proposed Worm_Secure but it will increase the overhead control packets. The propose algorithm is capable of not only detecting the wormhole attack but also it will deactivate the participation of the wormhole nodes in MANET.

8. REFERENCES

[1] Kush, Ashwani June 2009 Security and Reputation Schemes in Ad-Hoc Networks Routing, International Journal of Information Technology and Knowledge Management, Volume 2, No. 1, pp. 185-189.

[2] Kush, A. March 2009 Security Aspects in AD hoc Routing, Computer Society of India Communications, Vol. no 32 Issue 11, pp. 29-33.

[3] Bouam S. and Othman J. B. Sept. 7-10, 2003 Data Security in Ad hoc Networks using MultiPath Routing, in Proc. of the 14th IEEE PIMRC, pp. 1331-1335.

[4] Ghazizadeh S., Ilghami O., Sirin E., and Yaman F. Nov. 6-8,2002 Security-Aware Adaptive Dynamic Source Routing Protocol, In Proc. of 27th Conference on Local Computer Networks, pp. 751-760.

[5] D. B. J., Yih-Chun Hu, Perrig Adrian, Sept. 2002 Ariadne: A secure on-demand routing protocol for ad-hoc networks, Proceedings of the Eighth Annual

International Conference on Mobile Computing and Networking (MobiCom 2002).

[6] Inkinen Kai 2004-04-26/27 New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes, Helsinki University of Technology T-110.551, Seminar on Internetworking.

[7] Wenjia Li, Joshi Anupam 2008 Security Issues in Mobile Ad Hoc Networks- A Survey, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, http://www.cs.umbc.edu/~wenjia1/ 699_report.pdf.

[8] Qian L., Song N., and Li X. Marh 2005 Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path, In Proc. IEEE Wireless Communications & Netwoking Conference (IEEE WCNC), New Orleans, USA..

[9] Lazos L., Poovendan R., Meadows C., Syverson P., and Chang L.W. March 2005 Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach, In Proc. IEEE Wireless Communications & Netwoking Conference (IEEE WCNC), New Orleans, USA.

[10] Khalil I., Bagchi S., and Shroff N.B. July 2005 LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks, In Proc. International Conference on Dependable System and Networks (DSN), Yokohama, Japan.

[11] Chiu H.S. and Lui K.S. January 2006 DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks, In Proc. International Symposium on Wireless Pervasive Computing, Phuket, Thailand.

[12] Hu Y.C., Perrig A. and Johnson D.B. February 2006 Wormhole Attacks in Wireless Networks, In IEEE JSAC, Vol. 24, No. 2, pp. 370-380.

[13] Hu Y.C., Perrig A., & Johnson D. 2006 Wormhole attacks in wireless networks, IEEE Journal on Selected Areas in Communications , 370-380.

[14] Jen S.M., Laih,C.S. and Kuo W.C. 2009 A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET sensors, 5022-5039.

[15] Lazos L., Poovendran R., Meadows C., Syverson P. and Chang L. 2005 Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach, Wireless Communications and Networking) Washington: IEEE Conference, pp. 1193 – 1199.

[16] Zhu S., Setia S. and Jajodia S. 2003 LEAP: efficient security mechanisms for large-scale distributed sensor networks, Proceedings of the 10th ACM conference on Computer and communications security New York: ACM, pp. 62 - 72.

[17] Wang X. and Wong J. 2007 An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks, 31st Annual International Computer Software and Applications Conference, Washington, DC, USA: IEEE Computer Society, (p.8).