An Enhanced Integrated Solution for Identification and Elimination of Wormhole Attack in MANET

Kapil Raghuwanshi
Department of CSE
Truba Institute of Engineering & Information Technology Bhopal, India

Amit Saxena
Department of CSE
Truba Institute of Engineering & Information Technology Bhopal, India

Manish Manoria, Ph.D
Department of CSE
Truba Institute of Engineering & Information Technology Bhopal, India

ABSTRACT

‘Mobile ad hoc network (MANET)’ is an infrastructure less, self controlled wireless network it doesn’t need any centralized control so it can form and deform anywhere. Several freely movable mobile nodes with wireless connectivity can construct this type of network anywhere in no time, open connectivity and lack of central infrastructure enables the mobile nodes to freely exchange information and data with each other using radio signals. With this type of open connectivity and absence of centralized control MANET is vulnerable to many kinds of attacks and ‘wormhole attack’ is also present in those attacks. It is the most powerful attack and very difficult to detect in ‘wormhole attack’ two collaborating attacker nodes occupy strong strategic locations in two different ends of the network. By occupying dominant positions these two nodes can cover complete network and advertise to have the smallest route for transmitting data. The two attacker nodes are linked with a high speed wireless transmission link which is called wormhole tunnel. A very efficient solution of ‘wormhole attack’ is discussed in this paper. The objective of our research work is to discover the alternative paths between the two communicating nodes. Then after calculating length of every alternative path we found that the length of alternative path is much larger than the path including wormhole tunnel.

Keywords

AODV, MANET, Malicious node, Packet drop ratio, Wormhole Attack.

1. INTRODUCTION

“A Mobile Ad-hoc network [1], [2] is an aggregation of mobile devices which have some sort of wireless networking capabilities”. It is robust in nature and is self organizing. It is an infrastructure less network. A formed network can deform and again formed as many time we want without the help of any central administration. Every node works like a router in this type of networks. there are many applications of ad-hoc networks such as in the virtual classrooms among the students for connectivity, in military organizations and battle fields where the enemy movements and the other confidential information and high risk data are exchange between all the divisions and the individual soldiers, in disaster situation where the existing infrastructure and wired networks are not applicable then these type of network works very effectively in the disaster relief operations, in hospitals and many private & government organizations for better connectivity to exchange various reports and files etc. with these all the useful applications a major drawback for this network is its vulnerability towards many types of attacks. Because it doesn’t need any centralized structure to control and maintains the information sharing so security has a serious issue in mobile ad-hoc network. The open characteristic, self organized behavior and highly dynamic ‘‘network topology,’’ of these networks creates many complications to design the specific and effective security solution. According to [1], [2] “Availability, Integrity, Confidentiality, Authenticity, Non repudiation, Authorization, Anonymity,” is the basic security attributes which are always kept in mind to develop the various security strategies. Generally Mobile ad-hoc network is vulnerable to many attacks but wormhole attack is one the most powerful and severe attack, because it is a collaborative attack which can be organized by a pair of malicious nodes which works in collaboration to form a secret tunnel between them which is known as wormhole tunnel, and then they force the network and participating nodes to divert there traffic towards this tunnel by advertising smallest route every time in this way this tunnel consumes all the active traffic of the entire network. In this paper we are projecting a new Mechanism called effective “hop count analysis” for minimizing the threat of Wormhole attack. To achieve this solution we made some small changes in the source files of AODV Protocol and obtain a new protocol which we called Modified AODV (MADOV) in this work. The basic architecture of mobile ad-hoc network is depicts in the figure below. Where see the peer-to peer connectivity between each mobile node without the help of any central administration or access point.

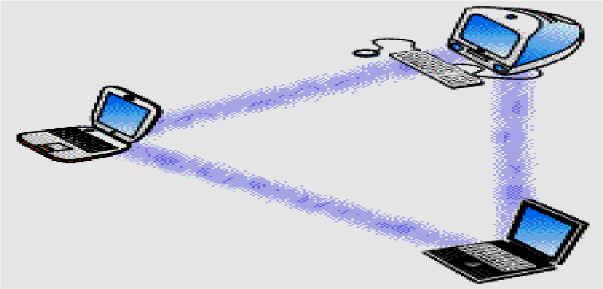

Fig 1: Basic Architecture of MANET

2. AODV ROUTING PROTOCOL

AODV stands for “Ad hoc on-demand distance vector routing Protocol”. It establishes routes only in on-demand basis. It means route between nodes only establishes when it is required. AODV routing strategy is specially suited for dynamic self-configured networks like MANET. It provides loop free routes along with route management for broken links. In AODV Bandwidth requirement for mobile nodes is comparatively less than other protocols as AODV doesn’t require periodic route advertisements [3]. Nodes which are communicating or intermediate nodes on active route only maintain routing information. Nodes which present along with established path are not necessary to mange routing information and doesn’t required to exchange routing table on each time interval. Furthermore, routes only established and maintained between the two communicating parties only whenever they required or when they are acting as a supporting cast or “intermediate nodes” in others communication. AODV is a variant or polished version of DSDV protocol because it creates routes in on demand basis so it can minimizes the broadcast counts, routes are created whenever they required. But DSDV maintains a route list already in its buffer. In AODV generally two messages are used one is RREQ which stands for route request and the other is RREP which is for Route response. When any node wants to send any information to other communicating node in the network then it launches a route discovery for this it will invoke a broadcast RREQ query through-out the network. This RREQ broadcast message will be received by each node. According to [4] every node preserves some information in their routing table, which includes “destination internet address, destination sequence no., next hop id, hop count value and lifetime”. A route is determined when this RREQ reaches itself to the target node or the other nodes which are nearer to the destination or which have a brand new & valid path for the destination. A route is finally established when a RREP message is unicasted to the initiator of the RREQ. Every intermediate node which is present in this active route to the direction of source keeps track the path related information. So by using this RREP reaches to the initiator node. After that this route is become activated and ready for the transmission.

3. WORMHOLE ATTACK

The wormhole attack is the most severe attacks of MANET. It is a sort of DOS attack which is very effective in network layer. It affects network routing and especially location based security of Ad-hoc is compromised by this attack [5]. “Wormhole attack” is a co-operative attack because it needs two nodes which act’s in co-operation. In this attack two collaborating attacker nodes occupy strong strategic locations in two different ends of the network. By occupying dominant positions in a network these nodes can cover complete network and advertise to have the smallest path for transmitting data. These two attacker nodes are linked with a direct wireless link which is called wormhole tunnel. At one end of wormhole tunnel, one node collects the packets in its local area and then transmits those packets to the other node which are present on the other end of tunnel then this node plays again with those packets. The tunnel which connects these nodes was created using a high speed transmission links such as Ethernet cables or wireless optical links. If this pair forwards every packet legitimately then in a way they are supporting the faster communication and routing within the network. However, this is not the case as these attacker node, either drop every packets which are intended to them, alter those packets or selectively transfer some packets.

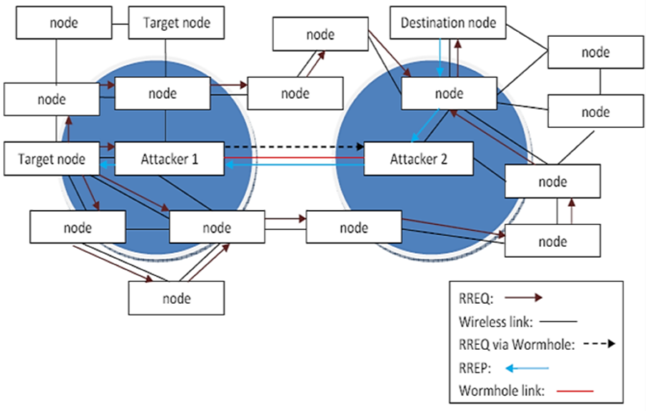

Fig 2: Wormhole Attack

In Figure 2 the two attackers placed themselves in a strong strategic location and the target node invokes its route finding mechanism by sending RREQ query packets throughout the network just to discover a valid and legitimate route towards destination. As the attacker 1 node which is the one hop neighbor of the sender node receives these packets then it forwards these packets to the attacker 2 node using wormhole tunnel. After reaching at the attacker 2 node these RREQ packets are then forwarded to the destination node. Then the destination node on its behalf directs a RREP message for the target node which is first received by the second attacker node then using the wormhole tunnel again these RREP forwarded to the first attacker node. Which is then lastly reaches to the initiator node. So this way these colluding malicious nodes establishes a legitimate path between source and destination. And then they capture the whole data set. Either drop every intended packets or altering them or to delay them before reaching to the receiving end.

3.1 Types of Wormhole Attack:

- Wormhole using Out of Band channel
- Wormhole using packet encapsulation
- Wormhole using high-power transmission lines
- Wormhole using packet relay

4. RELATED WORK

Y. C. Hu et al., (2003) [6] proposed a protective scheme for wormhole detection by using packet leashing. They proposed a new authentication protocol “TIK (*TESLA with Instant Key disclosure*) which is an enhanced version of the ‘TESLA’ broadcast authentication protocol”. TIK protocol employs “temporal leashes” and it is based upon old symmetric cryptography rules and requires an accurate time management between all communicating parties. The proposed TIK protocol when used with fixed timestamps & accurate clock synchronization can protect against wormhole attacks that cause the signal to travel a distance longer than the minimum range of the radio, or any other range that might be specified. To achieve an exact clock synchronization commercial GPS receivers are used. A MAC layer protocol using TIK authentication protocol doesn’t require significant additional processing overhead. D. B. Roy et al., [7] presented an intrusion detection Mechanism in which entire network is branched into many clusters. And the participation of a wormhole attack is noticed by the two layer technique. This approach uses AODV routing protocol. Using a layered approach reduces the load of processing on each cluster heads and it also reduces the chances of compromising cluster heads. A “guard node” is used for monitoring the malicious activity. The technique which is basically based on “round trip time calculation” is used by the guard node to expose the existence of wormhole. If any sign of wormhole is noticed by this node then it informs the cluster head of the corresponding layer. Cluster Head of outer layer broadcast this information to all other cluster heads at layer 1. Cluster heads at layer 1 inform their respective cluster members. Y. C. Hu et al., [8], [9] presents the design of two protocols which is capable of recognizing wormhole attack at the receiver. “The Slot Authenticated MAC protocol and the TIK protocol” are presented. Both protocols are depending on tight time synchronization. Slot Authenticated MAC is a simple, resource-efficient approach based on a TDMA MAC, whereas TIK is a practical, unique technique that has somewhat higher network overhead and resource requirements, but features significantly reduced latency. Since TIK key disclosure occurs as the data in same packets, protected packets can be immediately verified resulting in reduced latency and packet overhead. L. Qian et al., [10] proposed a new mechanism called "Statistical Analysis of Multi-path (SAM)" for the detection and identification of the attacking nodes. By Using statistically analyzed information which was collected by multipath routing is helped to detect wormhole attack and also identifies the attacking nodes. No additional overhead required in this approach and no security enhancement is needed in the existing routing protocol. The main concept of this mechanism is to detect routing anomaly on the basis of the changes which are occurred in the previously discovered routes of routing protocols in the existence of the wormhole attack. X. Su and R. Boppana [11] proposed a distributed technique which is based on the propagation speeds of requests and statistical profiling. They implemented the technique in Ariadne. Practically this technique reduces RREQ delays and statistical profiling of RREQ or RREP delays to prevent creation of in-band wormholes. They presented packet filtering techniques to filter RREQs or RREPs that have excessively large delays. Since different RREQs take varying number of hops, the upper most on per hop time of RREQ/RREP packets is calculated so that most normal packets are retained and most falsified packets are filtered. A. Vani and D. Rao [12] proposed a combination of three different techniques which are hop count value, decision anomaly and neighbor list count methods. In hop count examination method if the value of hop count between any two routes of the same destination node are extensively grater then some defined threshold value then the sender node automatically presumes that a wormhole exist. In anomaly detection, existence of wormhole will be decided by all the neighbors of a wormhole node because wormhole node generally shows very desperation in active routing and they give tough competition to all participating nodes in route discovery. In Neighbor List count method secure neighbor discovery from sender to receiver is obtained by neighbor list and detect the anomaly if attack is present. R. Maheshwari et al., [13] in their work created a new algorithm that uses connectivity information and look for prohibited substructures in connectivity graph. If any wormhole node present in the network it deviates the real formation of the connectivity graph. Because wormhole nodes generally create a long distance directional link between them so the existence of these nodes deviate the resulting configuration of the connected graph from its real configuration or structure. local connectivity information is used in this algorithm which means that every node looks into connectivity of its k-hop neighbors. Hu and Evans [14] in their scheme used the directional antennas to avoid wormhole attack. They present cooperative protocol called neighbor discovery protocol in which all nodes share direction related information to every other node so the creation of wormhole end-nodes is very difficult in this scheme. Wormhole prevention is totally relies on the ability of the nodes how they create & maintains accurate sets of authentic neighbors list. A node heavily relies on the incoming signals to getting actual direction related information and guidance. This is the main property of the directional antennas. So the network assumption will be accomplished by using this information. As directional information is combined with effective protocols, minimizes the occurrence of attacks significantly and reduces the success ratio of attacks. Kumar & Kush [15] developed a protocol known as "Worm Secure protocol". The objective of the proposed solution is to find an alternative route which bypasses the wormhole infected route. This method relies on hop count analysis approach. In this protocol after getting the entire route from sender node to receiver node in routing table the sender will set a second hop node as a target node. From using the previously stored route in the routing table, one hop neighbors find alternate paths to target node, if the alternative path has a greater hop count than threshold then it is infected with wormhole. K. Win [16] presented algorithm that path has a greater hop count than threshold then it is infected with wormhole. K. Win [16] presented algorithm that combines method uses in DaW –Defence against Wormhole security model, monitoring nodes and calculation of trust for wormhole detection. Frequency analysis of all the links of every available route is to be done in the time of routing. Whenever any link found suspicious, then the existing trust information is used to check if the link is that of a wormhole. In this trust model, Packet drop pattern is used instead of measure of dropped packets by the nodes to monitor their neighbours. Hu et al., [17] describes a "wormhole geographic distributed detection (WGDD) algorithm" for wireless sensor networks. This algorithm uses hop count scheme, reconstruct local structures in every node and then it uses a diameter feature to recognise the abnormal behaviour which is induced by wormhole. This scheme provides the approximate location of wormhole nodes. W. Ahad and M. Sharma [18] presented a multipath algorithm to sense "wormhole attacks". To detect wormhole, a target node is selected at random and path to any destination node is saved in routing protocol. When all alternate paths are stored, if the hop count for any path abruptly decreases then at least any one node is malicious. T. V. Phuong et al., [19], [20] proposed a "transmission time based mechanism (TTM)" for wormhole detection. In this mechanism first they calculate the average transmission time between each successive node which are presents in the active established path and then uses this average time value for wormhole detection. It detects wormhole during initial route setup stage. According to this scheme average transmission time between wormhole nodes is greater than the real neighbours.

5. PROPOSED WORK

The objective of this research was to solve or minimizes the impact of wormhole & device a solution which can sense the presence wormhole in the initial route setup stage. To achieve this goal we present an efficient solution which is applicable for reactive AODV routing protocol. Our solution is typically relies on the "hop count study" approach. In this scheme we uses hop count as a parameter to distinguish paths containing wormhole tunnel. Figure 4 present the basic planning and idea of this research. Mostly the routes contain larger hop count value for example the value is 5 and 6 in the following network shown in figure, to establish connection between sender node and destination node. While the hop value of the path going through wormhole tunnel will be much smaller, in this case the value is only 2. Consider two nodes wishes to communicate with each other, in which one is source and the other one is destination, which are highlighted in green color in the following figure. If source node communicates via wormhole tunnel then it encounters only 2 hops. But the other possible alternative routes comprise 5 or 6 hops to transfer a packet from the same set of nodes. So the basic approach behind this technique is that the route path having small hop value or the route which have lower no. Of hops may be unsafe. So the proposed mechanism says that the path having too short "hop count value" is unsafe.

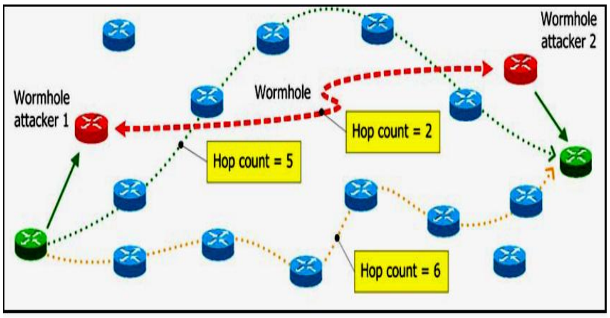

Fig 3: Compare hop count values of available routes

In this detection technique hop count of all the available routes is calculated first. Source node then verifies the one hop neighbors and accordingly a threshold value is set, which is used for comparing the hop count of the present route with the next available route. If the preferred route which is followed by the AODV differs widely with the next available route in terms of length, then there will be high probability of having wormhole in this route.

5.1 Proposed Algorithm

In this proposed mechanism, any node not necessarily source node, which is set in detect mode uses this hop count based technique for wormhole avoidance. Whenever any node sends RREQ packets and in turn start receiving RREP packets, it follows the below mentioned algorithm using the *checkpath( )* function module which is employed in the source file of AODV in ns-2. This algorithm is repeatedly executed in ns-2 in every 0.1 seconds. The purpose of repeatedly checking the routes is to ensure that the wormhole attacker nodes should not get included in our picked path for packet transmission from sender to destination because wormhole nodes always very eager to take participate in active routing. This is possible because these nodes set the maximum sequence number & lowest hop count which is one in the RREP packet.

5.2 Hop-count Analysis Algorithm

1. In AODV, all the available paths to the receiver are checked one by one through routing table for wormhole detection.
2. To check the paths, AODV determines number of hops and each one-hop neighbor is verified.
3. If there is one hop neighbor, it is legitimate and threshold is increased by 1 every time, otherwise it is decremented. This way a threshold value is set.
4. Then the next alternative path is checked in similar manner and number of hops is calculated which again defines a new threshold value.
5. Source node compares length of selected route with alternative path by comparing hop count and threshold.
6. If the hop count value of the considered route is larger than the set threshold, then symptoms of wormhole is detected.
7. On detecting malicious route, the corresponding next hop entry is deleted, so that now that suspected neighbor is not used for routing.
8. Similarly other paths are examined using the step 5 – 10.

6. SIMULATION RESULT ANALYSIS

In this Proposed technique Network Simulator (NS-2) version 2.34 (NS-2.34) has been used for the Simulation of AODV, AODV under Wormhole Attack and MAODV. Simulation can be performed on the basis of several performance matrices, such as Average End-to-End delay, Average Throughput & Packet Delivery Ratio.

6.1 Simulation Parameter

Table 6.1 Simulation Parameters

Channel	Channel/Wireless
Propagation	Propagation/TwoRay Ground
Network Interface	Phy/Wireless Phy
Platform	Ubuntu 12.04
NS Version	Ns-allinone-2.34
MAC	Mac/802_11
Interface Queue	Queue/ Drop tail / Pre queue
Link Layer	LL
Antenna	Antenna/Omni Antenna
Interface Queue Length	50
No. of Nodes	5,10,15,20,25
Simulation area size	750*550
Traffic Pattern	CBR Sessions
CBR Packet Size	512 bytes
Simulation Duration	32 Seconds

6.2 Simulation Result

6.2.1 Packet Delivery Ratio Comparison

This subsection depicts “packet delivery ratio” of the three routing protocols, calculated for different nodes Scenarios PDR in accordance with the different nodes value is depicted in the table below. Saw the variation in packet delivery.

Table 6.2 PDR Comparison table of AODV, AODV under wormhole attack & MAODV

No. of Nodes	AODV	AODV under wormhole attack	Modified AODV
5	99.4%	1.13%	76.8%
10	98.54%	1.46%	55.12%
15	98.66%	0.89%	47.32%
20	87.85%	0.81%	39.27%
25	86.97%	0.57%	42.21%

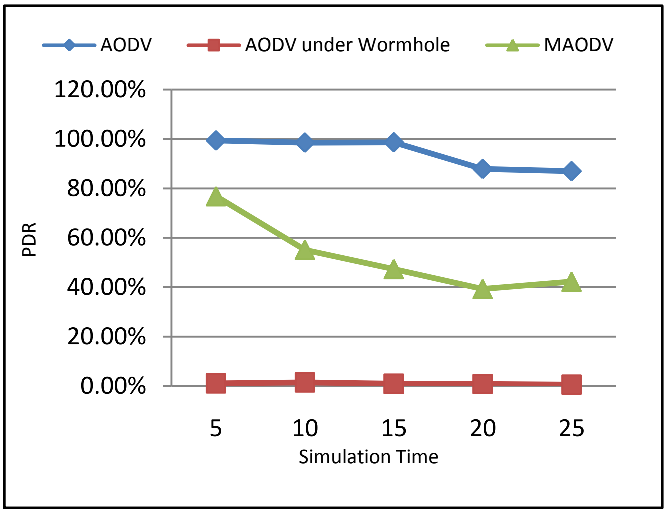

Fig 4: PDR Comparison

6.2.2 Average End to End Delay Comparison

End-to-end delay for each received packets is calculated first and then averaged. This subsection shows the average delay of each routing protocol. The comparison of each protocol in the form of "end to end delay" is given in the table below.

Table 6.2: Average end to end delay (in m sec) Comparison table

No. of Nodes	AODV	AODV under wormhole attack	Modified AODV
5	62.67	20.12	96.68
10	15.77	8.58	8.70
15	12.55	41.68	36.27
20	67.8	38.67	40.76
25	252.78	50.62	68.65

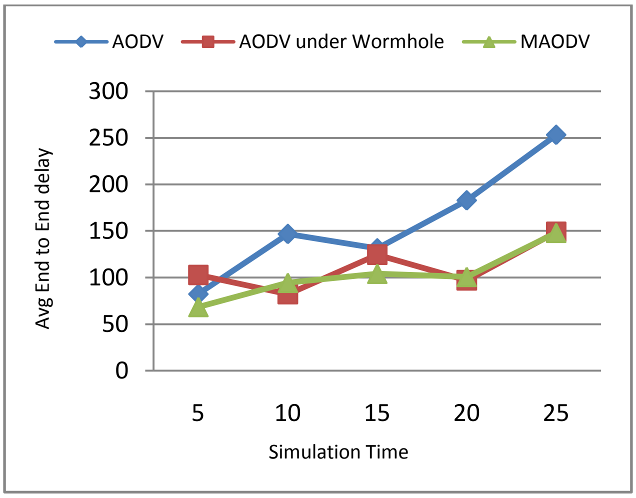

Fig 5: Average. End to End Delay comparison

6.2.3 Average Throughput comparison

Throughput of the whole network is calculated at all the destination nodes by including all the links. In this subsection, "Throughput" of the three routing protocols, calculated for different nodes scenarios. Throughput for various nodes is shown in Table 6.3.

Table 6.3 Average Throughput (in kbps) Comparison table

No. Of Nodes	AODV	AODV under wormhole attack	Modified AODV
5	82.27	102.67	68.45
10	146.71	82.10	94.39
5	131.28	124.43	104.15
20	182.74	96.89	100.75
25	252.98	148.87	148.07

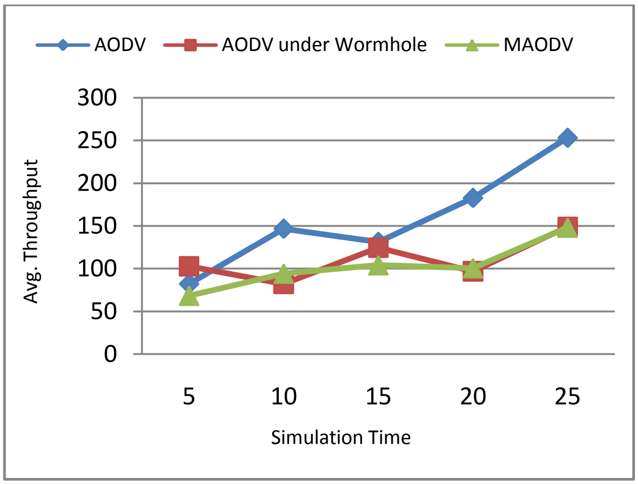

Fig 6: Avg. Throughput comparison

7. CONCLUSION

This research carried out the detailed study and examination of AODV routing protocol and the wormhole attack. In our work we proposed a technique namely hop-count analysis to identify the malicious nodes which causes wormhole tunnel. We had done Simulation of our proposed solution in the presence of wormhole attack in different node and traffic scenarios. Simulation of security strategies provides the facility to select a good security solution for routing protocols and gives the knowledge how to use this scheme in hostile and compromised environments. According to simulation results proposed technique shows superior performance as PDR and throughput increases however, "average end-to-end delay" also increases. In the analyzed scenario, it is found that the MAODV has a superior performance then AODV. Modified AODV is suitable for detection and prevention of wormhole attack. It improves the Packet delivery ratio under attack conditions, with a minimal decrease in throughput and acceptable increase in end-to-end delay.

8. FUTURE WORK

One of the leading issues in MANET communication is security. Security in MANET can be compromised by many ways and attacks. Lots of other ways to attack the networking that could be subject to further studies

1. Many other ways are also available to initiate a wormhole attack such as packet leashing. Thus more techniques are required to detect them.

2. Measurement of computing complexity.
3. Energy efficiency is also a very prime topic of concern for mobile nodes in MANET. Because they use batteries.

9. ACKNOWLEDGEMENT

Firstly I am very thankful to my guide Mr. Amit Saxena Sir for their unconditional support and views on each aspects of this project. And then I specially thank my brother for supporting me and guiding me to successfully complete this research work.

10. REFERENCES

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

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

[3] K. Toh, "Ad Hoc Wireless Networks".

[4] S. K. Sarkar, T. G. Basavaraju and C. Puttamadappa, "Ad Hoc Mobile Wireless Networks".

[5] Z. Danailov, "Attacks on Mobile Ad hoc Netwoks", Seminar Report, Integrated Information Systems, Ruhr University, Bochum, Germany, 2012.

[6] Y. C. Hu, A. Perrig and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols", in Proceedings of the ACM Workshop on Wireless Security, pp 30–40, 2003.

[7] D.B. Roy, R.Chaki and N. Chaki, "A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks" International Journal of Network Security & Its Applications (IJNSA), Vol. 1, No.1, 2009.

[8] Y.C. Hu, A. Perrig and D. B. Johnson, "Wormhole Detection in Wireless Ad Hoc Networks", Technical Report TR01-384, Rice University Department of Computer Science, 2002.

[9] Y.C. Hu, A. Perrig and D. B. Johnson, "Wormhole attacks in wireless networks", IEEE journal on selected areas in communications, Vol. 24, No. 2, 2006.

[10] L. Qian, N. Song and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path"

[11] Xu Su Rajendra V. Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks", in proceedings of IEEE Communications Society, ICC 2007.

[12] A.VANI and D. S. Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing in Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3, No. 6, 2011.

[13] R. Maheshwari, J. Gao and S. R Das, "Detecting Wormhole Attacks in Wireless Networks using Connectivity Information",

[14] L. Hu and D. Evans "Using Directional Antennas to Prevent Wormhole Attacks" In Network and Distributed System Security Symposium (NDSS 2004), San Diego, California, USA. February 2004.

[15] V. Kumar and A. Kush, "Worm Secure Protocol for Wormhole Protection in AODV Routing Protocol", International Journal of Computer Applications, Vol. 44, No.4, 2012.

[16] K. Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 24, 2008.

[17] Y. Xu, G. Chen, J. Ford and F. Makedon, "Detecting Wormhole Attacks in Wireless Sensor Networks",

[18] W. Ahad and M. Sharma, "Efficient Multipath Algorithm in MANETs to Prevent Wormhole Attack", CT International Journal of Information & Communication Technology, Vol. 1, Issue 1, pp 5-8, 2013.

[19] P. V. Tran, L. X. Hung, Y. K. Lee, S. Lee and H. Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", IEEE, pp 593-598, 2007.

[20] T. V. Phuong, N. T. Canh, Y.K. Lee, S. Lee, and H. Lee, "Transmission Time-based Mechanism to Detect Wormhole Attacks", IEEE Asia-Pacific Services Computing Conference, IEEE Computer Society, pp 172-178, 2007.