A Hybrid Approach to Modified AODV Protocol to Detect and Avoid Wormhole Effected Path over MANET

Neha Sahu
Department of Computer Science and Engineering,
Technocrats Institute of Technology, Bhopal

Deepak Singh Tomar
Department of Computer Science and Engineering,
Technocrats Institute of Technology, Bhopal

Neelam Pathak
Department of Computer Science and Engineering,
Technocrats Institute of Technology, Bhopal

ABSTRACT
In MANET mobile node is responsible for route establishment using wireless link where each node behave like both as a host and router. MANET encounter by number of security threat because of its open untrusted environment with little security arrangement, whether security over MANET is not to be enhance up to satisfactory level because of its characteristics. Among all of security threat worm hole is consider to be a very serious security threat over MANET. In worm hole two selfish node which is geographically very far away to each other, makes tunnel between each other to hide their actual location and try to believe that they are true neighbours and makes conversation through the wormhole tunnel. Recently research will focus over wormhole detection and avoiding path but existing technique having lower network overhead, lower battery power consumption in order to longer survival of network with fast response. This paper introduce a modified AODV protocol that detect and avoid wormhole path over MANET towards secure routing , which is based on an hybrid model that encapsulate location, neighbor node and hop count method.

Keywords
Ad-hoc network, wormhole, threshold, AODV

1. INTRODUCTION
The rapid growth of communication system the researchers pay attention to wireless communication approach. In this way the mobile ad-hoc network is one the best solution where communication takes place without any wired media.

Mobile ad-hoc network is a type of ad-hoc network which is created temporally. In these types of network the nodes have the special properties. This network has created with the wireless equipments. The major advantage of this network is- it is infrastructure less, it can be self-deploy and it doesn't need a centralized authority [1].along with that there are many important characteristic needs for the mobile node. Some of them discussed below:

- The node should be Wireless
- Hardware of the node should be consumption Low power
- The ability to route the packet
- No need of central co-ordinator
- Range of the node should be satisfactory
- Mobility of the node should be needed
- Node installation should be easy
- A node can be self healed
- Auto sleep mode
- The node should support the older protocols until extremely necessity of developing new protocols not occur.

It is not necessary that all these properties should be the node of mobile ad-hoc network. But up to a certain extend these properties are needed in the mobile node.

As far as the connecting media is concert, it is different from wired network so that, there is a need to use the different protocols to manage the network. Protocols designs for Mobile ad-hoc network are different from the protocols used in wired networks. Some time it seems to be that there protocol stuck in getting the correct decision because of the attacks.

The wormhole attack is a serious threat for mobile ad-hoc network that happen in the routing protocol for distracting the user for sending their data and it cannot be detected easily. Its present a illusion of shortest path between two end points in network. For detection of the wormhole attack in MANET a technique has been proposed. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network. In the reactive routing protocols such as AODV, the attackers can tunnel each route request packets to another attacker that is near to destination node [3, 4]. When the neighbours of the destination hear this RREQ, they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process.

Routing protocol over the dynamic link of MANET is responsible to select shortest and less traffic path but it is very challenging because of its mobile nodes and its very tedious job to maintain the accuracy over the network for long time .wormhole attacker node can use that greediness of shortest path, make a tunnel over the network and present an illusion of shortest path via wormhole node.

2. WORM HOLE ATTACK
As earlier we have discussed that wormhole is types of attack which is worked on the network layer [6, 7]. It creates the tunnel in order to forward the data from one wormhole node to another wormhole node. So it also confirms that there is a need of two nodes. Figure 4 shows the simple scenario of the wormhole. In this figure there are two networks having number of nodes. In both network two nodes act as wormhole node. Node N6 and P11 are the nodes with a tunnel in network 1 and network 2. Both nodes show that they have the shortest path to get the destination node in the different network. It might possible that both nodes can exist in the same network. It depends on the wormhole creator.

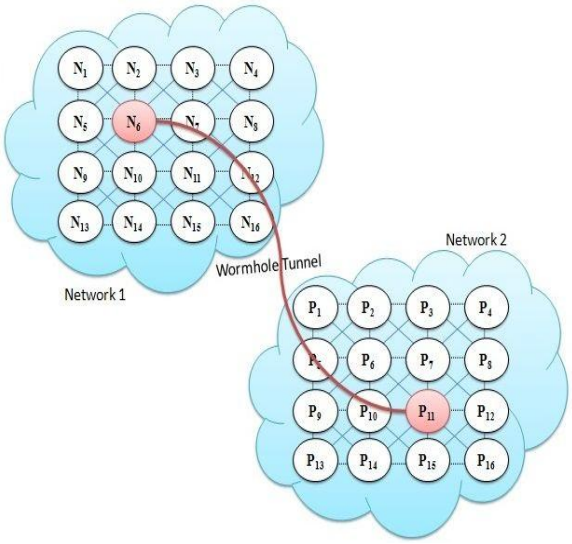

Figure 1: Illustration of a Wormhole attack

3. RELATED WORK

Maria A. Et al [8] has analysed on the wormhole attack and with respect to proactive protocols. The authors pay attention to the network traffic. The author tried to found the anomalous behaviour of nodes using timing analysis of routing traffic within the network. The proposed approach is far better than the previous approaches.

The proposed work [9] has developed the novel protocol in order to prevent the wormhole attack in the wireless environment. The author has used the symmetric and asymmetric key cryptography with Global positioning system. The protocol has tested on the both GPS node and non –GPS node. The author has tested the protocol with the ratios of GPS nodes to non-GPS nodes 30:20, 25:25, and 20:30, 15:35, 10:40 and 5:45 under a total network area of 100 by 100 meters. This gives the higher results.

The author [11] has proposed a protocol which doesn't uses any special hardware like directional antenna or synchronized clock. This protocol doesn't depend on the physical medium of the wireless network. In this approach the wormhole detection will take place after the discovery of route. Here the hope count techniques have also used between neighbours. The author has also applied the hound packet. The simulation results show that the WHOP is quite excellent in detecting wormhole of large tunnel lengths.

The wormhole is a major problem in mobile ad-hoc network. For the best result there are many protocols has developed. The two famous protocols are AODV and DSR. This paper gives the comparison result between these protocols. The parameter considered by the author are: packet delivery fraction, the average end-to-end delay, average jitter, throughput, number of frames tunneled, number of frames intercepted, number of frames dropped, number of frames replayed etc. the results shows that AODV is perfect protocol for the small network. Due to the routing overhead of AODV the performance will decrease in large network. But As the length of colluding link increases, the performance for DSR degrades compared to AODV.

The proposed methodology is based on the route request (RREQ). To find the wormhole in the network the author has suggested finding the possible routes by using the RREQ. There are three basic steps has used in this approach. These are routes redundancy, routes aggregation and calculating round-trip time (RTT) of all listed routes. The proposed results have compared with the AODV protocol and the previous approaches for the time based calculation. The parameter of packets dropping has decreased in this approach.

4. PROPOSED SOLUTION

This paper presents a hybrid approach that select an wormhole free path from source to destination. Proposed scheme work over the selection criteria of path reply from neighbor node, actually whenever any node S wants transmit a packet to D then its required a path for message transmission where routing algorithm (AODV) suggest a path for transmission such as node S broadcast a route request packet to all its neighbor or radio node for route towards destination D .All the neighbor node follow up the request forwards and replay an route replay packet to source node, then source node select shortest and less traffic path for transmission but because of that greediness some time source node select wormhole effected path for transmission. Proposed protocol hybrid approach enhances the performance of AODV by adding one more rule over selection criteria ie select wormhole free route.

Proposed protocol use location, hop count and neighbors node concept for wormhole detection in the routing path suggested by AODV. In proposed methodology every hops over the route responsible to find out, is there any worm hole between its next hop to its next to next hop over the route. For detection every hop evaluate an alternate route for their next to next hop over the route and if number of hop count in any of alternate route is greater than MHC(maximum hop count value) than that node reply wormhole detection signal between its next hop and its next to next hop and discard that path .

Algorithm(Wormhole detection)
Assumption

$S = Source\ node$

$D = Distination\ node$

$R_{(SD)}^{aodv}$ = *Route suggested by AODV from source to destination*

$n_0\ n_1\ n_2 \dots \dots \dots \dots \dots n_n\ n_{n+1}$

Where, n_o *=Source node*

n_{n+1} *=Destination node*

$TTL_{R(sd)}^{Max}$ = *Max TTL time/node in route R.*

(Intermediate node)

Nb_j^{ni} = *Nbj is the neighbor node of node ni*

Algo

Step 1:- Source node(s) call AODV protocol for route request towards destination D.

Step:2- AODV reply route reply packet with following message

$n_o\ n_1\ n_2 \dots \dots \dots \dots \dots n_n\ n_{n+1}$

Step3:-

For (i=0; i≤ n-1; i++)

For (j=0; j≤ m; j++)

n_i broadcast RRP for n_{i+2} via Nbi

$TTL(R^{Nbi}_{ni,ni+2})$

If (TTL ($R^{mi}_{ni,ni+2}$) >MHC)

Wormhole deduction message display and route discarded.

In proposed methodology the main consternation over the MHC value because all decision will carry out on the basis of that value. MHC means maximum number of hop count with any alternate route between any nodes to its neighbor of neighbor nodes ie any nodes to its second stage node. Where as if an routing protocol return an path S,A,B,G,H,D ie s is source and d is destination then node B must be neighbor of neighbor node of S via A and so on. But if B is not next to next node then alternate path defiantly return hop value greater than MHC value.

For calculating MHC each and every node of network find the largest number of hop count required for its next to next node with any alternate route over the network. And consider average of its as MHC value

Algorithm for MHC

Assumption

HC=Hop count

N = total number of node in network

X = number of neighbor node

MHC=Maximum hop count

Algorithm

For (I=1; I<=N ; I++)

{

For (J=1; J<=X ; J++)

{

Step 1. Si send an route request message to all its neighbor node for its next to next node NNjSi

Step 2. All the neighbor node reply the Route through route Reply packet to Si in term of number of hop count 'Y'

Step 3. if (Y>HC)

HC=Y

}

MHC= MHC+ HC

}

MHC = MHC/N

5. SIMULATION AND RESULT ANALYSIS

In order to authenticate the proposed methodology for wormhole detection verity of simulation experiments have been performed by using NS-2

For performance validation of proposed technique take different numbers of nodes in each scenario and consider a wormhole tunnels between any two nodes of that scenario for the simulation test. For experimental verification proposed technique run over three different scenarios with 140,160,180 and 200 node densities with same assumptions. As show in figure 1 false negative rate ie rate of wormhole detection is depend network density whereas MHC that is considered as keyhole for wormhole detection also depends on the network density.

Time Taken to Detect the Wormhole

Wormhole detection is perform by any node in between their next node and next to next node,whether this section describe time required to generate wormhole detection signal by any node successfully.

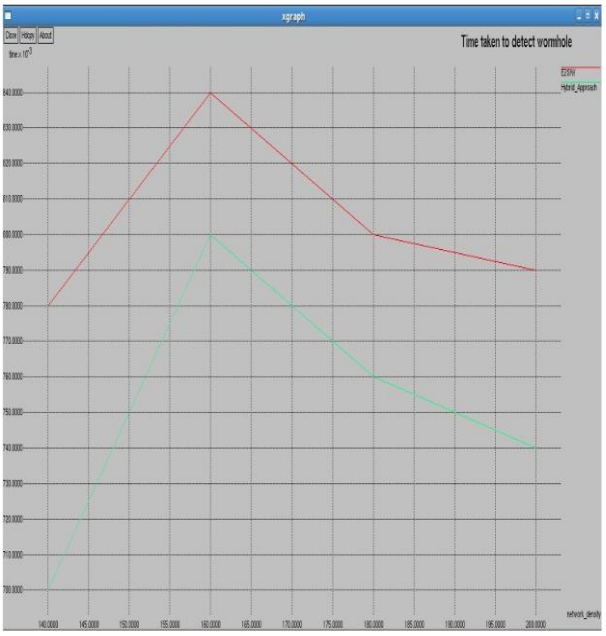

Figure 2: Time taken to detect wormhole

As show in figure 2 times required to detect wormhole by hybrid approach is significantly very less as compare to E2SIW. The average time taken to detect a wormhole by the E2SIW is 790 mili second, whereas it is 560 mili second in the case of hybrid approach.

Battery Power Consumption

E2SIW use GPS system for gathering the location of node ie used 1 joule of energy per node to gather it location whereas there is not any requirement of GPS system in hybrid approach. One joule energy is 33% of energy used per node in E2SIW so proposed hybrid approach degrades the energy requirement by 33%.

Network Overhead

With consider the algorithm 2 for MHC proposed technique is compared with the existing E2SIW in many different factors like network overhead and number for control packet responsible for route hunting and handshaking over different node of network. Proposed technique decrease the possibility of packet

retransmission so ultimately decrease the routing overhead as show in figure 4. Along with that proposed technique used number of control packet for wormhole verification over each node so proposed technique having larger number of control packet as compare to AODV.

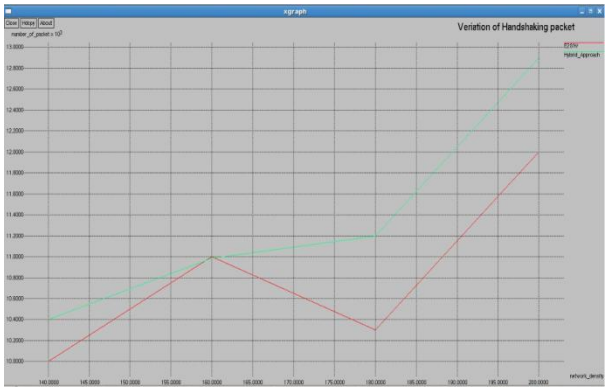

Figure 3: Comparison between Proposed hybrid approach and E2SIW over Handshaking

The above observation shows that the detection technique works efficiently but having some overhead, control packet is also increases in the graph, but the benefit of this technique is that it detects the wormhole, and will serve as an advantage when added to the existing AODV protocol.

6. CONCLUSIONS

In this paper a hybrid methodology for detecting and avoiding wormhole affected path in mobile ad hoc network is presented. This method encapsulate advantage of two different predefine method in order to overcome their limitation. The performance of proposed technique is depending upon network density, having lower response time with lower power consumption.

In order to detect wormhole proposed technique use larger number of control packet in future we will try negotiates that effect.

7. ACKNOWLEDGEMENT

I would like to say thanks to my guide prof Deepak Singh Tomar and prof Neelam Pathak who gives their knowledge and time in order to complete this paper. This paper will never complete without the support facility member CSE department TIT Bhopal.

8. REFERENCES

[1] Maulik, R. ; Chaki, N., "A comprehensive review on wormhole attacks in MANET" IEEE 2010, Page 233-238.

[2] Jian Yin, Sanjay Madria, "A hierarchical secure routing protocol against black hole attack in sensor networks", IEEE SUTC, 2006.

[3] Xiangyang Li "Wireless Ad Hoc and Sensor Networks: Theory and Applications" Cambridge University Press 978-0-521-86523-4

[4] Sebastian Terence J , "Secure Route Discovery against Wormhole Attack in Sensor Networks using Mobile Agents", IEEE 2011, pp 110-115.

[5] C. Perkins, E. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," The Internet Society 2003.

[6] Sang-min Lee, Keecheon Kim "An Effective Path Recovery Mechanism for AODV Using Candidate Node" springerlink, vol. 4331/2006, 2006.

[7] Mahajan, V. ; Natu, M. ; Sethi, A. , "Analysis of wormhole intrusion attacks in MANETS", IEEE 2008, Page 1-7.

[8] Keer, S. ; Suryavanshi, A., "To prevent wormhole attacks using wireless protocol in MANET" IEEE 2010, Page 159-163.

[9] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, "A secure routing protocol for ad hoc networks," in Proc. of IEEE ICNP, 2002.

[10] Dang Quan Nguyen ; Lamont, L., "A Simple and Efficient Detection of Wormhole Attacks", IEEE 2008, Page 1-5.

[11] Katrin Hoeper, Guang Gong, "Pre-Authentication and Authentication Models in Ad Hoc Networks," Signals and Communication Technology, pp. 65-82, 2007.

[12] Kanika Lakhani, Himani bathla, Rajesh Yadav "A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET" IJCSNS International Journal of Computer Science and Network Security, vol. 10 No.5, May 2010.