# A Novel Approach to Detect and Defend against Wormhole Attack in Mobile Ad-hoc Network

**Ankita Jain[1] and Megha Kamble[2]**
*[1]M-tech Scholar, [2]Assistant Professor*

***Abstract - the Mobile Ad Hoc Network (MANET) more vulnerable to attack in comparison with the wired network. Hence difficult to have a secure and authentic communication in wireless network. This paper focus on study of wormhole attack and the performance of wormhole attack on Ad-hoc on Demand Distance Vector routing protocol and MANET. In this paper we represent a mechanism of Delphi for detection and digital mark scheme for prevention of the wormhole attack in Manet. Delphi mechanism allow the sender to check whether there are any malicious node trying to launch wormhole attacks in the network or not. In this method we collect number of hop count and delay information and digital mark scheme is prevent the network against wormhole attack. In this scheme receiving node verified and compare the digital mark of previous node. The proposed work is simulated using Opnet simulator to evaluate the wormhole attack impact on AODV and MANET and measure certain parameters such as number of hops, traffic received and sent packets, delay and route discovery time.***

***Keywords - MANET, Wormhole, AODV, Digital mark, DelPHI***.

## 1. INTRODUCTION

Ad hoc in Latin means for this purpose only, MANET is a collection of mobile node which will act like router also that can communicate with each other wirelessly and having no predefined infrastructure. Each node acts like a router also. Major advantage is easy deployable and low cost. Applications of MANETs are in military, disaster relief, personal area network, and civilian network [12].The main thing of mobile Ad Hoc Networks is increasing rapidly with advances in technology and also result in smaller, economic due to cheaper, and power-efficient devices . There is no

Preexisting infrastructure so nodes can freely move and self-organize into a network topology [9].

MANET is subjected to various kinds of security attacks. One of them is wormhole attack. To launch a wormhole attack, an adversary establishes a direct link referred as wormhole link between two points in the network. A direct link can be established via a wire line, along-range wireless transmission, or an optical link. Once the wormhole link is operational, the adversary eavesdrop messages at one end, referred as the origin point, tunnels them through the wormhole link and replays them in a timely fashion at the other end, referred as the destination point [13].

The main purpose of study is to providing a novel approach mechanism for detecting and preventing against wormhole attack occur in the mobile ad-hoc network. This approach is provide a solution against wormhole attack caused for unauthorized access in ad-hoc network using delay per hop mechanism and digital mark scheme. Delay per hop scheme is able to detect wormhole attack as expected after applying detection algorithm while digital mark scheme is able to works properly as expected by applying prevention algorithm for prevent the network from the wormhole attack. The outcome of the study is to provide a graph based solution on different scenario for detecting and preventing against wormhole attack occur in the network. Perform on the basis of various parameters of AODV and MANET we analyse the result. AODV is used for establish a route to communicate with nodes in the network.

AODV (Ad Hoc On-Demand Vector Routing Protocol) In AODV, when a node wants to communicate with another node and there is no valid route in its routing table, it broadcasts a route request packet (RREQ). A node receiving a RREQ for the first time will setup a reverse route to the source node in its routing table. If the node is the destination or has a valid route to the destination, it will unicast a route reply RREP along the reverse route back to the source node. Otherwise, it will increase the hop count in the RREQ by one and forward the RREQ to other nodes [11].

## 2. SYSTEM MODEL

Research is mainly based on two tasks, one is based on theoretical study with the help of literature survey and fundamental and the other one is based on the implementation and experiments that we perform in certain ways. Simulation and result is performed in Optimized Network Engineering Tool (OPNET) simulation environment. Working of OPNET generally divided into four parts, design of the model , applying various required statistics, run the simulation and view the results in the form of graphs and to analyze the results , if the results are not correct then it has to be re-modeled and then to apply new statistics. In this environment we used it to create network models, design a scenario based on three different condition. They are normal network condition, network in attack condition and network in secured condition. In our experiments, the ad-hoc network includes eighteen mobile nodes placed randomly in square field campus of 20*20 kilometer area. Collect statistics directly from each network object, execute a simulation and view results. Now a day OPNET is very powerful and useful software in research fields.

## 3. PREVIOUS WORK

Several works has been proposed for the problem of wormhole attack by detecting or preventing in MANET. In this section we mentioned some work that has been done for the wormhole attack.

Yih-Chun Hu, Adrian Perrig and David B.Johnson [1] uses the method packet leash to prevent wormhole attack. The idea behind packet leashes is to limit the transmission distance tone hop. Leashes are divided in two category, namely geographical leashes and temporal leashes. In geographical leash, all nodes must have the knowledge of its own location in the network. In temporal leashes, all nodes calculate the expiration time of each packet and also add this expiration time in the packet’s header. This allows estimating the distance from the sender to receiver. In temporal leash, the packet creation time is encrypted and included with the packet. Shortcoming of using packet leashes method is that its provide the solution for hidden attack based observation only and Temporal leash requires nodes to have tightly synchronized clock but geographical leashes is better that temporal leashes because it’s not require tightly synchronized clock.

Hon Sun Chiu, Wong Lui and King-Shan Lui [3] described an efficient algorithm, they call it DelPHI. We know DelPHI is an effective technique to detect wormhole attacks. Wormhole attacks classifies as hidden attack and exposed attack. Thus DelPHI mechanism helps in providing solution for both kinds of classification. But they cannot pinpoint the wormhole location. Because lengths of paths are changed by every node so wormhole nodes could change the path length in a certain way to make them unable to be detected. They evaluate the performance of DelPHI by conducting various simulation using the ns simulator. This mechanism find delay per hop in every path. The message overhead of DelPHI also shown in this paper. They use AODV protocol to compare it.

Reshmi Maulik and Nabendu Chaki [9] proposed a simulation for MANET using AODV and DSR routing protocols and also simulated the effect of the presence of wormhole. They consider Significant QoS parameters such as throughput, delay, node density, and packet delivery ratio and power consumption. Their main aim is to focuses on how QoS is affected under wormhole attack in a network.

Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Sung young Lee, and Heejo Lee [11] proposed an efficient mechanism known as TTM a transmission time based mechanism against wormhole attack in Wireless Ad Hoc Networks. TTM is able to detect both hidden & exposed wormhole attacks also locating the wormhole with no special requirement of hardware. TTM performance good with little overhead. TTM specifically design for Ad Hoc On-Demand Vector Routing Protocol (AODV) but it can be extended to work with other routing protocols.

Ravinder Ahuja, Alisha Banga Ahuja and Pawan Ahuja [12] determines the performance of AODV and DSR routing protocol under wormhole attack and also compare the performance of these protocol without wormhole attack. Three parameter taken in this paper are ratio of packet delivery, throughput and average of the end to end delay. The performance of routing protocol decreases under the wormhole attack. So good solution need to be find out to detect and defend against wormhole attack. In this paper the routing performance is measured but only shows the effect of worm hole in AODV routing protocol and DSR routing protocol.

## 4. PROPOSED METHODOLOGY

Proposed mechanism is mainly based on two tasks, one is concern with theoretical study with the help of literature survey and fundamental and the other one is based on the implementation and experiments of the Mobile Ad-Hoc Network. In this proposed mechanisms a novel approach is presented to detect and prevent against wormhole attack using AODV protocol in MANET. We proposed a graph based simulation on different network parameters. This approach is able to detect the wormhole attack in network and also prevent the network against wormhole attack. We create scenario in normal network, attacked network and secured network and performing graph based solution for this approach. The normal network scenario is prepared by applying various attribute of mobile node according to the requirement of study. The network attack scenario is prepared by applying various attribute of mobile node according to the requirement. Detection algorithm is applied in this scenario to detect malicious node. In Secured network we applied the proposed algorithm. Prevention of wormhole attack through digital mark scheme which is an efficient method for doing this. Proposed mechanism is done by two method: first is Detection Method and second is Prevention Method

### *4.1 Detection Method*

Detection mechanism uses delay per hop indication method to detect wormhole attack in adhoc network. This mechanism allow the sender to check whether there are any malicious node trying to launch wormhole attacks in the network or not. In this method we collect number of hop count and delay information. To improve and check the reliability of information collected, the process of data collection is repeated more than one times. Analysis the number of hop using different path and calculate average number of hop. Now delay/hop indication mechanism is used for analysis the average no. of hop. Value by calculating round trip time and then computing delay per hop indication method. Suppose that the sender initiates the detection which means is route request packet is broadcasting at time $t_{req}$ and receives a route reply packet from a neighbor node i at time $t_{rep}$, then the round trip time of the path through node i is given by

$$RTT_i = t_{rep} - t_{req}. \; [3]$$

If the hop count field in the RREP from node i is hi, then the delay per hop value of the path to the receiver through node i is given by:

$$DPH_i = \frac{RTT_i}{2h_i} = \frac{t_{rep} - t_{req\_}}{2h_i} \quad [3]$$

### *4.2 Detection Algorithm*

Input: no. of nodes n, source node s, destination node d

Terms: Rq – route request packet, Rp- route reply packet, AODV- adhoc on demand distance vector, Delphi-delay per hop indication, RTT- round trip time.

```
Algo (wormhole_attack_detection)
Begin
Deploy mobile nodes randomly to form a network
Establish a route, invoke AODV
Define source node and destination node
Broadcast Rq
At source
If (source send any packet)
Add information of in node id column of packet header
Hop count starts its value by one in the hop count column
At intermediate
If (received Rq during the process of broadcasting)
Increase no. of hop count by the value one until reach to d
At destination
If (packet received)
A scheme is used called Delphi at destination node d
Destination node d received all Rq reached by using different path in a certain period of time

For (select a route)
1 Analyse number of hops used by different path.
2 Choose a route for unicast the Rp which have average number of hop count.
3 Route having less no. of hop count value than the average no. of hop may have malicious nodes
For (analyse average no. of hops)
1 Delay/hop is computed by using the values of RTT
2 Delay/hop of the shortest path is chosen because shortest path refers under wormhole attack
3 The minimum average no. of delay is taken from all the shortest path Rp and analyse average no. of hops for detecting attack due to their tunnelling property
End
```

### *4.3 Prevention Method*

A digital mark prevention scheme is a mechanism for provide authentication and prevent network from security threats that is wormhole attack. In this scheme receiving node verified and compare the digital mark of previous node because it is consider that all good node in the network must have their own digital mark. The verification of digital mark uses a bits concept. We add digital mark in the digital mark column of route request (Rq) packet header .To prevent the wormhole attack by encrypting the packet at each level by sharing the digital mark with the neighbouring nodes and ensuring secured delivery via decrypting the packet at the receiving node and matching the digital mark in MANET in AODV protocol environment.

### *4.4 Prevention Algorithm*

```
Input: no. of nodes n, source node s, destination node d
Terms: Rq – route request packet, Rp- route reply packet
Algo (wormhole_attack_prevention)
Begin
Deploy mobile nodes randomly to form a network
Call AODV routing protocol for establish a path
Define source node and destination node
Broadcast Rq packet
The header of Rq packet have
a. Data of node id in the information column
b. Data of the number of visiting nodes using in the path contains in hop count column
c. Digital mark information of the packet is contains in digital mark column
At source
If (broadcast a packet)
Add information of every visiting node i.e. node id in the information column of Rq header
Add information of Hop count column in the Rq header
Hop count starts its value by one in the hop count column
All nodes of the network also start sharing the digital mark with each node a route have.
At intermediate
If (received a Rq packet during broadcasting)
No. of hop count get by the value one until reach to the d
At destination
If (on receiving packet _ verify authentication)
Rp packet header have data of node id and digital mark data of each visiting node
Compare value of digital mark of previous node
If (digital mark found identical)
Unicast reply to next node
Repeat process again and again till meet to s
Establish an authenticated and secure way between s and d
If (digital mark not found identical)
Presence of malicious node in packet header of any previous node noticed
Received packet found that malicious node contains
a. Duplicate mark b. Blank space
Node discard the Rp to next node
Inform about malicious node in the network
Node update their database
End
```

## 5. SIMULATION/EXPERIMENTAL RESULTS

The simulation parameters along with their values are listed in table1.Simulation results are evaluated on the basis of performance parameters which are shown below.

**Table-1: SIMULATION PARAMETERS**

| **Parameters** | **Values** |
|---|---|
| Simulation tool | Opnet modeler |
| Routing protocol | AODV |
| Simulation time | 1000 sec |
| Simulation area | 20*20 kilometer |
| Numbers of mobile nodes | 18 |
| Data packet size | 1024 Bytes |
| Data rate | 10 Kbps |
| Speed of node | 08 Km/h |
| Number of malicious nodes | 2 |

### *5.1 Number Of Hops Per Route*

Graph shows the average numbers of hop per route for AODV protocol. In normal network scenario all nodes working properly without affecting the network. In attack network scenario, the average no. of hopes per route is goes down. Because When Wormhole attack occurs in the network than due to tunneling property, wormhole affected node start sending packet by using the tunnel created by attacker without using intermediate nodes so number of hopes reduces. In secure network scenario we applied DMPS mechanism to secure the network from wormhole attack. This improve the average no. of hop value to normal condition.

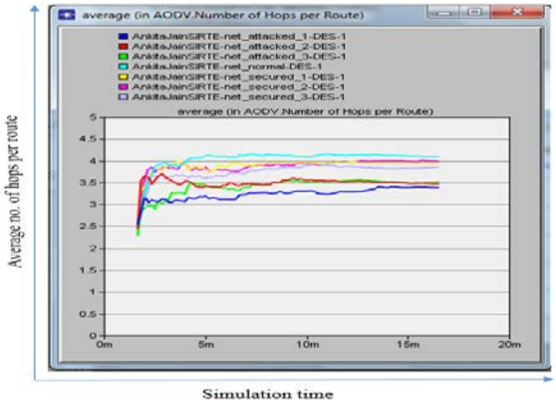

Fig.1. Average (in AODV Number of Hops per Route).

### 5.2 Route Discovery Time

Graphs shows the average route discovery time for AODV protocol. In the graph three condition of network is shown. No attack in network that is under normal condition where all nodes works as expected. In attack network the average route discovery time is reduces because under the presence of the wormhole attack, wormhole affected route will be selected most of the times. When applied the secured scheme in the network we can see that there is much better performance of network for the route discovery time that the attack network and it is near to normal condition.

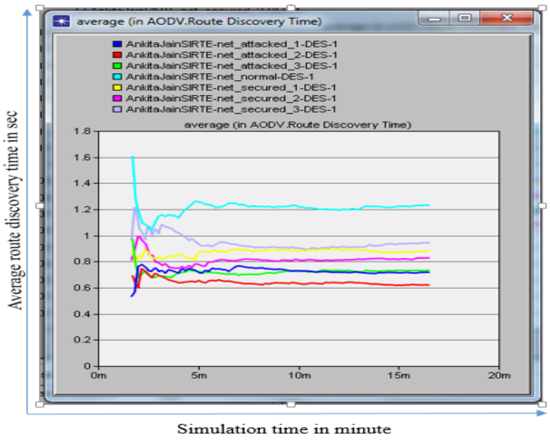

Fig.2. Average (in AODV Route Discovery Time).

### 5.3 Traffic Received Packets

Graph shows the average traffic received during the transmission. X direction shows the Simulation time and Y direction shows the number of packets received. Through the graph, we analyzing the average traffic received in MANET.

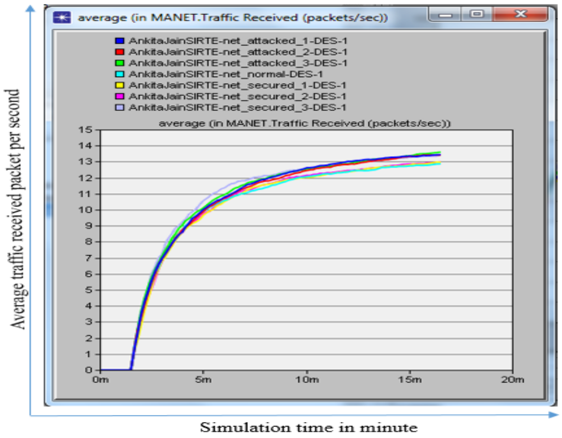

Fig.3. Average (in MANET Traffic Received).

### 5.4 Traffic Sent Packet

Graph shows the average traffic sent during the transmission, based on MANET. We simulate the result in attack network the packet received is high. In secured network, the packet sent by the attacker node is work properly as expected

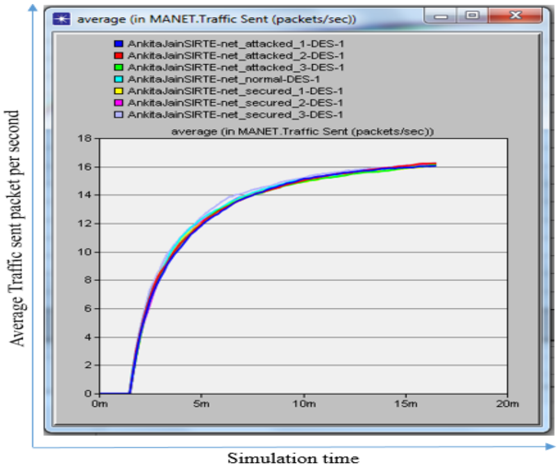

Fig.4. Average (in MANET Traffic Sent).

### 5.5 Delay

Graph shows the average delay per second for wormhole attack, normal condition and secured condition. Graph shows the average delay in MANET. When the attack present in the network the value is goes down because wormhole attack reduces the delay because without use of intermediate nodes the data are delivered.

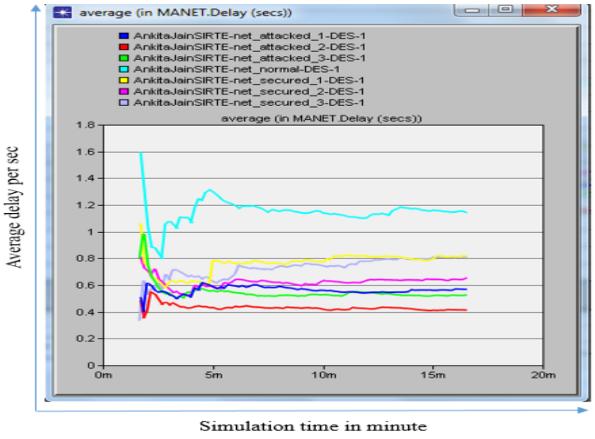

Fig.5. Average (in MANET Delay)

## 6. CONCLUSION

In this paper, we described a mechanism which is able to detect and defend the wormhole attack in mobile ad hoc networks.we created a scenario with wormhole attack and without wormhole attack and analyse the result on the basis of various parameters of AODV and MANET .The proposed method is able to detect wormhole attack in mobile ad-hoc network by collecting and analysing the value of no. of hop count and delay information. The proposed method using digital mark scheme is working as expected to prevent wormhole attack that occur in the network. The wormhole attack is prevented by encrypting the packet at each level by sharing the digital mark with the neighbouring nodes and ensuring secured delivery via decrypting the packet at the receiving node and matching the digital mark of previous node.

## 7. FUTURE SCOPES

Some existing solutions cannot work well in the presence of more than one malicious node, while some other needs hardware. So, there is still a hope and scope of research to provide security, authentication to the MANETs.

## REFERENCES

[1] Hon Sun Chiu, Wong Lui and King-Shan Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Network", IEEE the 1st International Symposium on Wireless Pervasive Computing, Phuket, Thailand, 16-18 January 2006.

[2] Yih-Chun Hu, Adrian Perrig and David B.Johnson, "Wormhole Attacks In Wireless Networks", IEEE Journal On Selected Areas In Communication, Vol 24 ,No.2,February 2006.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", Proc. IEEE INFOCOM, 2003..

[4] Majid Khabbazian, Hugues Mercier and Vijay K. Bhargava, "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad-Hoc Networks", IEEE Wireless Communication, Vol 8, No.2, February 2009.

[5] Dezun Dong, MoLi, Yunhao Liu, Xiang-Yang Li, and Xiangke Liao "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks", IEEE/ACM Transactions On Networking, Vol. 19, No. 6, December 2011.

[6] T. Sakthivel and R. M. Chandrasekaran, "Detection and Prevention of Wormhole Attacks in MANETs using Path Tracing Approach", European Journal of Scientific Research ISSN 1450-216X Vol.76 No.2 (2012).

[7] Jyoti Thalor, Ms. Monika, "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review", IJARCSSE ISSN: 2277 128X Volume 3, Issue 2, February 2013.

[8] Hosny M. Ibrahim, Nagwa M. Omar and Ebram K. William, "A Lightweight Technique to Prevent Wormhole Attacks in AODV", International Journal of Computer Applications (0975 – 8887) Volume 104 – No.6, October 2014.

[9] Reshmi Maulik and Nabendu Chaki,"A Study on Wormhole Attacks in MANET", International journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279.

[10] Xia Wang, Johnny Wong, "An End-to-end Detection of Wormhole Attack in Wireless Adhoc Networks", 2007proceedingsofannual ICSAS, Department of Computer Science, Iowa State University, Ames, Iowa 50011.

[11] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee, and Heejo Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", 1-4244-0667, 2007 IEEE.

[12] Ravinder Ahuja, Alisha Banga Ahuja and Pawan Ahuja, "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANET sunder Wormhole Attack", 978-1-4673-6101-9/13/$31.00 ©2013 IEEE.

[13] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. W. Chang, "Preventing wormhole attack on wireless adhoc networks: a graph theoretical approach " ,University of Washington, Seattle, Washington, Naval Research Laboratory, Washington, DC.

[14] Achint Gupta, dr. Priyanka v j and SaurabhUpadhyay, "Analysis of Wormhole Attack in Aodv Based Manet Using Opnet Simulator", issn 2319-2720 volume 1, no.2, September – October 2012 ijccn.