International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

# Detection and Prevention of Wormhole attack in MANET

**Aakanksha Kadam[1], Niravkumar Patel[2], Vaishali Gaikwad[3]**

[1]*Student & Information Technology department, K.J.S.I.E.I.T, Mumbai, Maharashtra, India*
[2]*Student & Information Technology department, K.J.S.I.E.I.T, Mumbai, Maharashtra, India*
[3]*Assistant Professor, Dept. of Information Technology, K.J.S.I.E.I.T, Mumbai, Maharashtra, India*

---

**Abstract -** *The development in wireless technologies and the high availability of wireless equipment in everyday life have made infrastructure-less networks very popular. MANETs are becoming more and more common due to their ease of deployment. Unlike the wireless networks having a fixed infrastructure, a mobile ad hoc network or MANET does not depend on a static infrastructure for operations based on networking, because of this security is a very challenging issue in MANET, there is a high possibility that the intermediate nodes can be malicious and they might be a threat to the security. Wormhole is the most frequently occurring attack in ad hoc networks in which one malicious node tunnels the packets from its location to other defective nodes. If the source node chooses this fake route, the attacker has the alternative of delivering the packets or dropping them. In this paper we have surveyed some existing techniques for detection of wormhole and a method for detecting and preventing wormhole attack in MANET is proposed. The proposed approach is based on Smart Packet, wormhole infected nodes can be detected based on acceptance of the smart packets by the nodes in the network. All the simulation will be done on ns2 using AODV routing protocol.*

***Key Words***: MANET, Wormhole, AODV, Smart Packet.

## 1. INTRODUCTION

In this age of wireless devices, Mobile Ad-hoc Network (MANET) has become an important part for establishing communication between mobile devices. Therefore, research in the field of Mobile Ad-hoc Network has been growing since last few years. Mobile Ad-hoc Network (MANET) is a group of wireless mobile hosts without fixed network infrastructure and centralized administration. Multi-hop packets are used to establish communication in MANET. MANET is a challenging field: MANET consists of diverse resources; the line of defence is very uncertain; Nodes operate in shared wireless medium; Topology changes irregularly and very dynamically; Reliability in the radio link is an issue; connection breaks are frequent. Also, the density of nodes, number of nodes and mobility of these hosts may vary in different applications.

Security is an absolute service for wired and wireless network communication. This work is concerned with a very severe security attack that affects the ad hoc networks routing protocols, called "wormhole attack". A Wormhole attack is considered dangerous as it is free of MAC layer protocols and immune to cryptographic techniques. There are many solutions to trace and prevent this attack like packet leashes, cluster base, hop count analysis etc., but none of them is perfect solution. Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two extremely isolated regions of a MANET are directly connected through nodes that appear to be neighbours but are actually distant from one another. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.

In our system, we analyse wormhole attack nature in ad hoc and sensor networks and existing methods of the defending mechanism to detect wormhole attacks without the need of any specialized hardware. This analysis is able to provide a method to reduce the rate of refresh time and the response time to become more faster. We are primarily using Network Simulator version 2 for implementation.

The remaining parts of this paper are described as follows.

Section II gives Problem Definition of this project. Section III explains Wormhole attack. Section IV gives review of previous wormhole detection and prevention techniques. Section V explains proposed scheme. Section VI presents the conclusion.

## 2. PROBLEM DEFINITION

This project is a simulation for creating, detecting and preventing the Wormhole attack in MANET. A MANET is a mobile ad hoc network which is a collection of autonomous nodes that communicate with each other by maintaining radio connections in a decentralize manner. Security is a major issue for MANET due to its characteristics of open medium, flexibly changing topologies, reliance on cooperative algorithms, and absence of centralized monitoring points and lack of clear lines of defense. A defective node operating in the network receives packets at one location and tunnels them to another location in the network, where these packets are modified and resent into the network. The tunnel that is between two conspiring attackers is referred to as a wormhole.
The main scope of this project is to detect presence of a wormhole in the network and develop a method (algorithm)

or a technique so that other nodes realize what the compromised channel in the network is, and thus avoid that path for sending data. Transfer of smart packet through the network will trick the colluding malicious nodes to send a response for that packet, and thus we can know what the compromised path is. The project is based on ns2 only.
These days there is an immense need to be protected from malicious attacks on the network, which are constantly trying to steal user data. Since a lot of communication takes place through MANET, it is required to develop mechanisms to prevent these attacks.

## 3. WORMHOLE ATTACK

A Wormhole attack is a serious threat in MANET, it attacks the traffic of a network and either scan, change or drop the confidential message inside the packet when it is travelling over the wormhole tunnel. Generally wormhole puts their malicious nodes at powerful position within the network as compared to other nodes so it attacks maximum traffic of network and prevents other routes from being discovered instead of the wormhole, and thus creates a Denial-of-Service attack by dropping the entire data, or specifically discarding or modifying certain packets as needed.
The wormhole attack affects both the proactive and on demand routing protocols. Due to the wormhole, genuine nodes in the network are unable to predict the original network formation, required for safe communication. This causes severe damage in networks that is based on localization schemes and it may lead the genuine nodes to take wrong decisions while selecting a route for transferring data in the network.

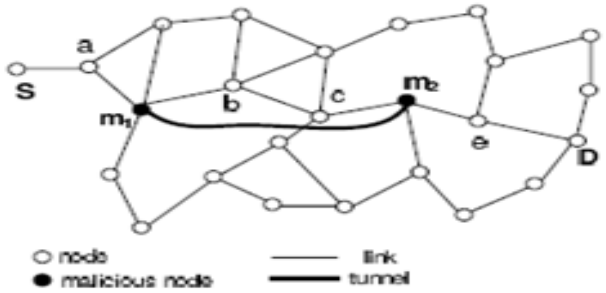


**Fig-1** : An example of wormhole attack

Figure 1 shows an example of typical wormhole attack in an ad hoc network. An attacker m1 colludes with another attacker m2 in order to deceive destination of a packet about the route and by including both m1 and m2 as the most efficient path towards the route. Since most routing protocols for ad hoc network select cost effective path, the path between m1 and m2may be chosen as the communication route from source to destination.

## 4. LITERATURE REVIEW

In the existing environment there are many solutions to detect and prevent this attack like packet leashes, cluster base, hop count analysis, Directional antennas etc., but none of them is perfect solution. This paper contains a postulate for new technique for wormhole avoidance. Proposed technique will be implemented with NS2 simulator over the AODV protocol. This technique for wormhole detection and avoidance addresses the malicious nodes and avoids the routes having wormhole nodes without affecting the performance of the network.
The proposed work [2], uses methodology of using a modified routing table that will help in the identification of malicious links. Since routing tables are used to maintain routes, they proposed a solution in which changes made to the routes and the full path from source to end are taken into account. By doing this we can instantly detect a potential wormhole link as soon as it is generated. This paper helps in detecting the wormhole only and does not provide any prevention mechanism.
The proposed work [3] is unable to detect false alarm and rescheduling of a packet propagating one hop is very high.
The proposed work [6] uses a packet leash technique for detection of wormhole attack. The leashes can be classified as geographical and temporal. But the problem with leashes is that all nodes should have knowledge of their own location in the network and insecure synchronized clock.
The proposed system is compared with the following existing systems as shown in table.
**Table -1:** System Comparison

| System | Features | Disadvantage |
|---|---|---|
| WADP[8] | RREP packet helps in checking the wormhole immediately. | Exposed wormhole attacks can be detected but hidden wormhole attacks are difficult to detect. |
| Wormhole Attack: A new detection technique[2] | Helps to detect malicious nodes quickly since the node which is mostly used is taken into account. | No prevention technique is mentioned. |
| Detection and prevention of wormholes in MANET using Hybrid Methodology[7] | Contains data about its 2 hops neighbours. | Sometimes it may assume the normal since confirmation technique is not applied. |
| Wormhole attack Avoidance Technique in MANET[4] | Helps to find out malicious nodes efficiently | DSR protocol increases the network load. |
| Wormhole attack mitigation | Two packets are used RREQ RREP for detection of wormhole. | Using one packet will be more efficient in which this method fails. |

## 5. METHODOLOGY

The proposed system shown in figure 1, aims at finding a safe path for sending packets for data communication. This technique focuses on the detection of misbehaving nodes and tries to prevent the wormhole attack on the network by preventing those nodes to use the current routing path and select an alternative path by again following the route discovery technique for the same. In this method of wormhole avoidance, existing AODV protocol is modified with the functionality of wormhole attack detection and prevention.

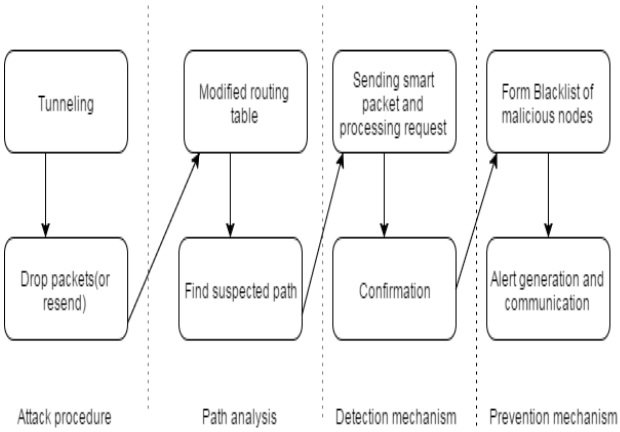


**Fig -2:** System Architecture

The steps in system architecture are as follows

**1. Attack Procedure:**

a) Tunneling: Two nodes are connected with one another with the help of a medium which is not available to normal nodes, with the help of this entirely different channel the nodes are able to communicate with one another over a range in which normal nodes cannot. The two defective nodes act in a way that they appear to be neighbors to all the other nodes.

b) Drop Packets: A malicious node receives packets at one place in the network and tunnels them to another place in the network, where these packets are again sent into the same network.

**2. Path Analysis:**

a) Modified Routing Table: The table will be modified to have an extra column consisting of full paths of each node besides the next hop. The modified routing table in two cases,

1. When no wormhole is present.
2. When wormhole is present.

b) Find Suspected Path: By modifying routing table we can identify suspicious wormhole links way before the attack actually takes place and starts disturbing the network. We can have a number of links within a routing table of a node that have high density, but it is least likely that the same two nodes be present in the routing table of a lot of nodes at the same time. Using this concept once a node has identified a potential wormhole link, it can confirm from its neighbors about the existence of same pattern in its routing table.

**3. Detection Mechanism:**

a) Sending smart packet & Processing Request: The smart packet is send to the neighboring nodes up-to two hops. This packet is supposed to be dropped by the authorized nodes. But if this packet is resend by any node, that node is supposed to be malicious and that node is to be checked further for confirming that the node is actually malicious.

b) Conformation:

1. First Process: When a node receives such a processing request, it will check its own table and if the same pattern exists, it will reply as true to the requesting node.
2. Second Process: the nodes at the two ends of wormhole send some encrypted messages to one another. Every privileged node on the path can be able to process those messages (we assume colluding nodes cannot decrypt and hence cannot process) and will add their signatures/stamps/flag to the encrypt packet pay load.
3. Third Process: When a destination node receives the encrypted message, it will look for signatures of all nodes along the path, if every node has added its signature to the encrypted payload; it will consider it as normal. If the signature of any node along the path is missing, it will consider it as a wormhole.

**4. Prevention Mechanism:**

a) Blacklist of Malicious Node: When the source node receives the encrypted reply and the wormhole existence is confirmed, we need to cut-off the malicious nodes so that no further communication takes place with them and hence they are black listed.

b) Alert Generation & Communication: Upon the confirmation of wormhole, both end nodes broadcasts a blacklisting message. This message contains list of malicious nodes to be excluded from communication and not to entertain any path update or any future request from them.

**Algorithm:**

AODV (Ad hoc on Demand distance vector routing) algorithm will be used primarily for developing detection as well as prevention algorithms for Wormholes encountered in the MANET. The AODV (Ad-Hoc On-Demand Distance Vector) routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. Routes are established on-demand, as they are needed. However, once established a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between the source and the destination only when the path is needed (i.e., if there are data to be exchanged between the source and the destination). An advantage of this approach is that the routing overhead is greatly reduced.

Step 1: First step is to create a MANET network in ns2.

Step 2: Creating a network in ns2, and creating wormhole using tunneling technique between the nodes (AODV algorithm will be used)

Step 3: Creating detection mechanism for detecting wormhole. Devising a suitable algorithm using AODV for detection.

Step 4: Sending "smart packet" through the network, which will detect the wormhole and the colluding nodes, since other nodes will drop that packet.

Step 5: That path will be avoided by other nodes. Generating algorithm for the same that is the prevention algorithm.

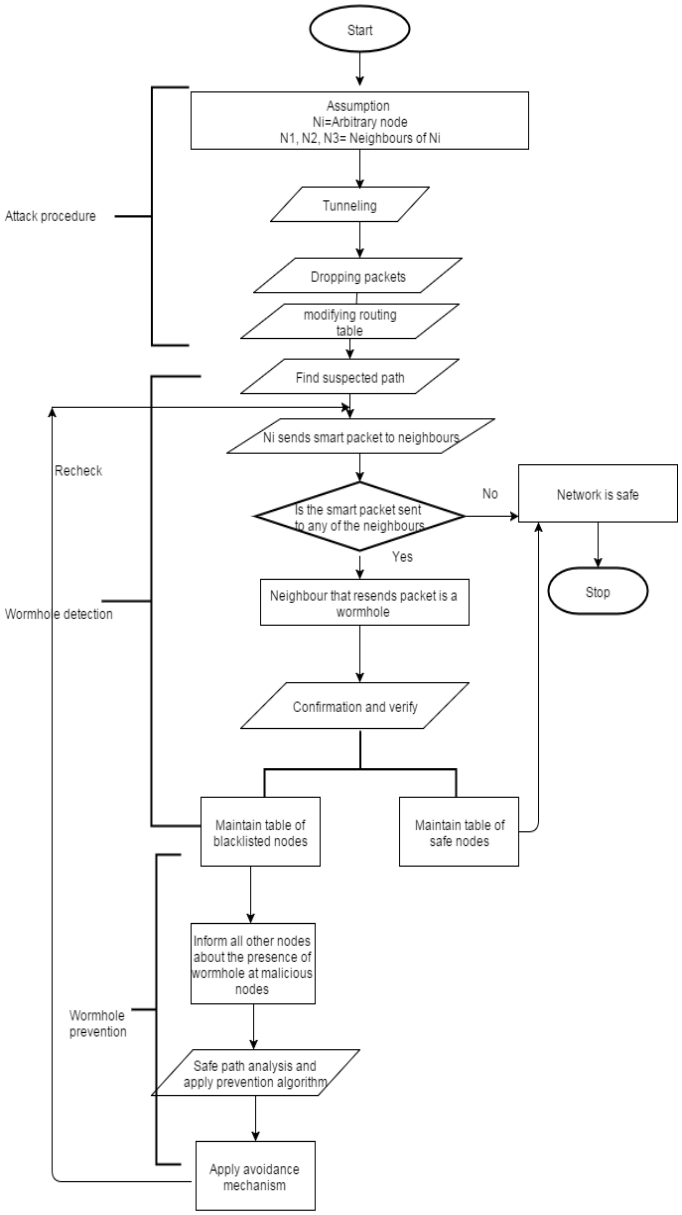


**Fig -3:** Design details of the system

The design details of the system contains of the following stages described in figure 2:

### 1) ATTACK PROCEDURE

Tunneling: Two nodes are connected with one another with the help of a medium which is not available to normal nodes, with the help of this out of band channel the nodes are able to communicate with one another over a range in which normal nodes cannot. The two colluding nodes act in a way that they appear to be neighbors to all the other nodes.
Drop Packets: A malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network.

A MANET is created in ns2, it consists of some Ni number of nodes (for Ni we can assume any value). Between any two nodes a wormhole is created using tunneling method. Packets are dropped in the network and the routing table is modified. With this out of band channel the nodes are able to communicate with one another over a range in which normal nodes cannot. The two colluding nodes act in a way that they appear to be neighbors to all the other nodes. A malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network.

### 2) WORMHOLE DETECTION

Sending smart packet & Processing Request: The smart packet is send to the neighboring nodes up-to two hops. This packet is supposed to be dropped by the authorized nodes. But if this packet is resend by any node, that node is supposed to be malicious and that node is to be checked further for confirming that the node is actually malicious.
Conformation:
First Process: When a node receives such a processing request, it will check its own table and if the same pattern exists, it will reply as true to the requesting node.
Second Process: The nodes at the two ends of wormhole send some encrypted messages to one another. Every legitimate node on the path will be able to process those messages (we assume that malicious nodes cannot decrypt and hence cannot process) and will add their signatures/stamps/flag to the encrypt packet pay load.
Third Process: When a destination node receives the encrypted message, it will look for signatures for all nodes along the path, if every node has added its signature to the encrypted payload; it will consider it as normal. If the signature of any node along the path is missing, it will consider it as a wormhole.
Once the suspected paths are identified, the local node first sends a smart packet to all of its neighbors to confirm the existence of the same path with high percentage of usage. When the smart packet is sent to neighbor nodes, and if the packet is dropped, we know that it is the safe path, and data can be sent through this network without the fear of intrusion. The legitimate node can send data by checking for digital signature/stamp of the previous legitimate node and while sending data it will also add its own signature/stamp in encrypted format. Colluder nodes cannot decrypt the

data/message. If the node accepts smart packet we know that it is a colluding node (malicious node) and the path between those two nodes is compromised and consists of wormhole.

### 3) WORMHOLE PREVENTION

Maintain a table of blacklisted nodes. When the source node receives the smart packet and the wormhole existence is confirmed, we need to isolate the malicious nodes from the network so that no further communication takes place with them and hence are black listed. Other nodes are informed about the malicious nodes and about the wormhole present between them. Safe path is analyzed by applying prevention algorithm and avoidance mechanism is applied.

## 6. CONCLUSION

Wormhole attacks in MANET can significantly degrade networks performance and threaten network security. In wormhole attacks as the adversaries usually replay the genuine data packets, detection of these attacks is quite complicated. In this paper we have discussed what a wormhole actually is and to detect them in the MANET. All the detection procedures have their own benefits and drawbacks. But there is no detection procedure which detects wormhole attack perfectly. Here we have studied all the existing approaches and tried to suggest our approach of using smart packet in order to eliminate the drawbacks encountered in earlier proposed works.

## ACKNOWLEDGEMENT

We would like to express our gratitude towards our Project guide, **Prof. Vaishali Gaikwad** for providing us inspiration, encouragement, help and valuable guidance that we needed for the project.

## REFERENCES

[1] Vaishali Mohite and Lata Ragha, "Cooperative security agents for MANET", IEEE -040, World Congress on Information and Communication Technology, Trivandram, India, pg 549 to 554, year 2012.

[2] Zubair Ahmed Khan, M. Hasan Islam, "Wormhole Attack: A new detection technique", Electrical & Computer Engineering Department, Center for Advanced Studies in Engineering (CASE), Islamabad, Pakistan.

[3]H.S. Chiu and K. Lui. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In Proceedings of Inter-national Symposium on Wireless Pervasive Computing, pp. 6-11, 2006.

[4] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, DheerDhwaj Barak, "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks" in 2012 Third International Conference on Advanced Computing & Communication Technologies.

[5] Motushi Sigh and Rupayan Das, "A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network", in October 2012. International Journal of Scientific & Engineering Research Volume 3.

[6] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", Rice University Department of Computer Science Technical Report TR01-384 December 17, 2001.

[7] Vikas Kumar Upadhay, Rajesh K Shukla and Rajshree Dubey, "Detection and Prevention of Wormholes in Mobile ad hoc networks using Hybrid methodology", Sagar Institute of Research and Technology, Bhopal Department of Computer science.

[8] Juhi Biswas, Ajay Gupta and Dayashankar Singh, "WADP: A Wormhole Attack Detection and prevention Technique in MANET using Modified AODV routing Protocol", Madan Mohan Malviya University of Technology
Gorakhpur, (UP) India, department of Computer science and Engineering.

[9] Reshmi Maulik and Nabendu Chaki, " A study of Wormhole attack in MANET", MeghnadSaha Institute of Technology, Techno Complex, Madurdaha, Kolkata 700150, India, Department of Computer science and Engineering.

[10] Norman A. Benjamin, Suresh Sankaranarayan. "Performance of Wireless Body Sensor based Mesh Network for Health Application", International Journal of Computer Information Systems and Industrial Management Applications, 2, pp. 20-28, 2010.

[11] R.H. Khokhar, Md. A.Ngadi, S. Manda. "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, 2 (3), pp. 18-29, 2008.

[12] D. Vivian, E.A.P. Alchieri, C.B. Westphall. "Evaluation of QoS Metrics in Ad Hoc Networks with the use of Secure Routing Protocols". In Network Operations and Management Symposium, pp. 1-14, 2006.

[13] N. Song, L. Qian, X. Li. "Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach". In Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, pp. 8-15, 2005.

[14] D.B. Roy, R. Chaki, N. Chaki. "A New Cluster-based Wormhole Intrusion Detection Algorithm for Mobile Ad-hoc Networks", IJNSA, 1 (1), pp. 44-52, 2009.

[15] D. Djenouri, O. Mahmoudi, D. Llewellyn-Jones, M. Merabti, "On Securing MANET Routing Protocol Against Control Packet Dropping". In IEEE International Conference on Pervasive Services, pp. 100-108, 2007.

[16] V. Mahajan, M. Natu, A. Sethi. "Analysis of wormhole intrusion attacks in MANETS". In IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.

[17] BounpadithKannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour. "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communication, 14 (5), pp. 85-91, 2007.