# Wormhole Attack Avoidance Technique in Mobile Adhoc Networks

Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak
UIET, MD University,
Rohtak, India
dr.yudhvirs@gmail.com

***Abstract*—Security is an essential service for wired and wireless network communication. This work concerned with a particularly sever security attack that affects the ad hoc networks routing protocols, called "wormhole attack". There are many solutions to detect and prevent this attack like packet leashes, cluster base, hop count analysis etc., but none of them is perfect solution. This paper contains a proposal for new technique for wormhole avoidance. Proposed technique has been implemented with NS2 simulator over the DSR protocol. This technique for wormhole avoidance addresses the malicious nodes and avoids the routes having wormhole nodes without affecting the overall performance of the network. The performance metrics used for evaluating network performance are jitter, throughput and end to end delay. The performance of proposed techniques is good.**

***Keywords - MANET, Wormhole, DSR, Network Security.***

## I. INTRODUCTION

With the rapid development in wireless technology, ad hoc networks have emerged in many forms. These networks operate in the license free frequency band and do not require any investment in infrastructure, making them attractive for military and selected commercial applications. However, there are many unsolved problems in ad hoc networks; securing the network being one of the major concerns. Ad hoc networks are vulnerable to attacks due to many reasons; amongst them are lack of secure boundaries, threats from compromised nodes inside the network, lack of centralized management facility, restricted power supply, scalability etc.

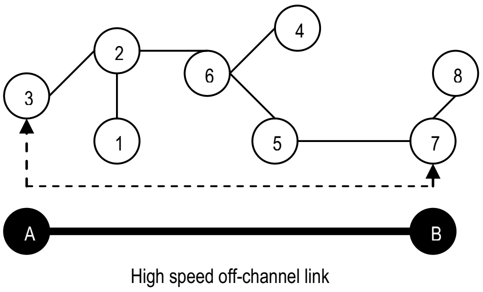


Figure 1. Fig.1 Example of wormhole

A particularly severe security attack is the wormhole attack. During the attack a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally. The tunnel can be established in many ways, such as through an out-of-band hidden channel (e.g., a wired link), packet encapsulation, or high powered transmission. This tunnel makes the tunneled packet arrive either sooner or with less number of hops compared to the packets transmitted over normal multihop routes. It creates the illusion that the two end points of the tunnel are very close to each other. [6] [15]

Here Fig.1 shows an example of wormhole attack. A network under a wormhole attack. Intruders A and B are connected by an off-channel link (i.e. wired or satellite link), which they use to tunnel network data from one end of the network to the other. Without a wormhole, nodes 7 and 3 are 4 hops apart, - their messages to each other should go through nodes 2, 6, and 5. When intruders A and B activate a wormhole, nodes 7 and 3 are able to directly overhear each others' messages, and are lead to believe they are immediate neighbors. Once this happens, all further communications between nodes 3 and 7 will be going through the wormhole link introduced by A and B.

## II. RELATED WORK

Unfortunately, the wormhole attack can not be defeated by crypto-graphical measures, as wormhole attackers do not create separate packets - they simply replay packets already existing on the network, which pass all cryptographic checks. Since wormhole attack such a severe thread to ad hoc network security, several researchers have worked on preventing or detecting wormhole attacks specifically [14].

### *A. Problem Statement*

This section describes wormhole attacks nature and problem statement. A wormhole attack is a particularly severe attack on MANET routing where two attackers connected by a high speed off-channel link called the wormhole link. The wormhole link can be established by using a network cable and any form of "wired" link technology or a long-range wireless transmission in a different band. The end-point of this link (wormhole nodes) is equipped with radio transceivers compatible with the ad hoc or sensor network to be attacked.

Once the wormhole link is established, the adversary record the wireless data they overhear, forward it to each other, and replays the packets through the wormhole link at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbors, and force all communications between affected nodes to go though them. We can think of wormhole attack as a two phase process launched by one or several malicious nodes. In the first phase, these malicious nodes, called wormhole nodes, try to lure legitimate nodes to send data to other nodes via them. In the second phase, wormhole nodes could exploit the data in variety of ways. [5] [14]

978-0-7695-4941-5/13 $26.00 © 2013 IEEE
DOI 10.1109/ACCT.2013.68

### B. General Approaches

Several solutions have been proposed for the wormhole attack avoidance, the solutions can be categorized into location based, time based, key based, statistics, and graph based solutions etc. Wormhole attack has different modes, classification and threats to network. There are different solutions to detect and prevent this attack based on the environment like packet lashes (geographical and temporal), time of flight, node monitoring, directional antenna etc. GPS-based solutions are particularly interesting. But GPS-based wormhole combating techniques can not be used where GPS does not work. Whereas temporal leashes require much tighter clock synchronization but do not rely on GPS information. The level of time synchronization required for temporal leashes (on the order of nanoseconds) not currently practical and impossible in wireless ad hoc networks. Cluster based, hop count analysis and statistical analysis, neighbor node monitoring techniques are unlike of some of its predecessors does not require any specialized hardware for detecting attack but to some extent. Statistical analysis works only with multi-path on demand protocols. Where hop count analysis is an interesting solution but causes a high load on the network since routing messages must be flooded over the network several times during one single route discovery process. In spite of many solutions, this attack is a particularly sever security attack that affects the ad hoc networks routing protocols, hence prevention of this attack is a major issue in MANETs security.

### C. DSR in MANET

The proposed approach have been implemented by considering DSR (Dynamic Source Routing) protocol. Existing DSR working has been modified in order to detect and prevent wormhole nodes in an adhoc network. The Dynamic Source Routing (DSR) specifically designed for use in multi-hop wireless ad hoc network. The DSR protocol does not require any existing network infrastructure or central administration and is completely self organizing and self-configuring. This protocol basically consists of two mechanisms: Route Discovery and Route Maintenance, where the route discovery mechanism handles the establishment of routes and the route maintenance mechanism keeps update the route information.

DSR is an on demand routing protocol, which means that no data is sent periodically and therefore it scales routing traffic and avoid the overhead package. The entire route in this routing protocol is known before the beginning of packet transmission and it stores the route information in a route cache[19].

When a node A sends a packet to the destination node C, it first searches its route cache for a suitable route. If no route from A to node C exists in the route cache, node A initiates Route Discovery by sending out a ROUTE REQUEST(RREQ) message in order to find a route to C. The sending node is referred as the initiator and the destination node, as the target. It is also necessary to maintain the route that are stored in the Route Cache since nodes move in and out of the transmission range of the other nodes in the adhoc network, and thereby creates and break routes.

## III. Proposed Solution

### A. Proposed Technique

Research methodologies for the proposed technique are related to the analysis of the misbehaving nodes which are responsible for the wormhole attacks in the MANET. Mainly in the Wormhole attack, traffics for the network are redirected to the mobile node in the network which not at all exists in the network. Thus in this case the network traffic is redirected into the one of the special mobile node such node is called as *wormhole node*. The wormhole attack has two characteristics: first one, the misbehave node advertise itself regarding to the information that it has shortest route to the destination with the intention of dropping the packets or intercepting packets in the routing protocols like DSR, AODV. Intercepted packets then consumed by the node: this is the second characteristics. For the simulation of the wormhole attack, the proposed technique works on the misbehaving nodes simulation on the DSR protocol and prevention of it using ns2 simulator and red hat Linux 5.0 environment.

The proposed technique is focused on the detection of the misbehaving nodes and tries to prevent doing wormhole attack on the network by preventing those nodes from the current routing paths and select the alternative path by again doing the route discovery procedure for the same. In this technique of wormhole avoidance, existing DSR protocol is modified with the functionality of wormhole attack detection and prevention. It fires the message of wormhole node detection in the path without affecting the overall performance of the network. Proposed DSR detects such nodes and the routes which contains the misbehaving nodes, are simply dropped and not added into the routing table of the DSR so that in future that routes are not used in any communication. For evaluating the network performance three parameters jitter, throughput, and delay has been used.

### B. Simulation Environment

Simulation is a fundamental tool in the development of routing protocols, because the difficulty to deploy and debug them in real networks. The simulation eases the analyzing and the verification of the protocols, mainly in large-scale systems. Network Simulator-Version 2, widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors.

To visualize the result it is possible to use a Network Animator (NAM) in NS2 environment. But in the NAM, wireless network simulation is not visualize properly as there is no extensive support in the NAM for the wireless simulation. Thus for the wireless simulation one more tool was developed which is called as *iNSpect tool*. For iNSpect tools, trace file output is needed as the input which is generated from the simulation script. Trace file contains the simulation results. This trace file is generated by the NS which contains the information related to the topology, nodes movement, routes, packets received, drops etc. For implementing proposed technique, we are considering a network of 5 nodes. The iNSpect visualization screen for such a network is shown in Fig. 2.

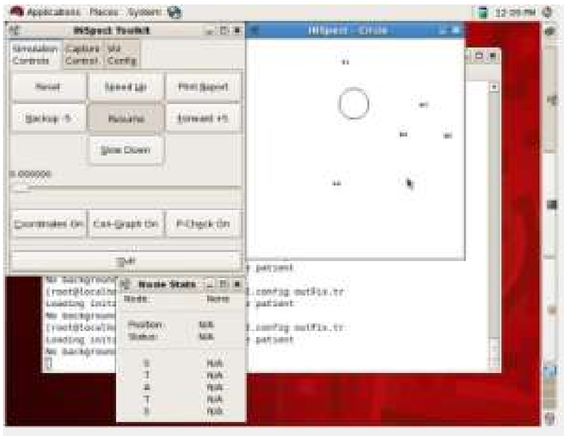


Figure 2. Fig.2 iNSpect simulation results for the 5 nodes simulation

As the proposed approach have been implemented with NS2 simulator. The experimental setup of the network parameters which has been used for simulation are shown in Table1.

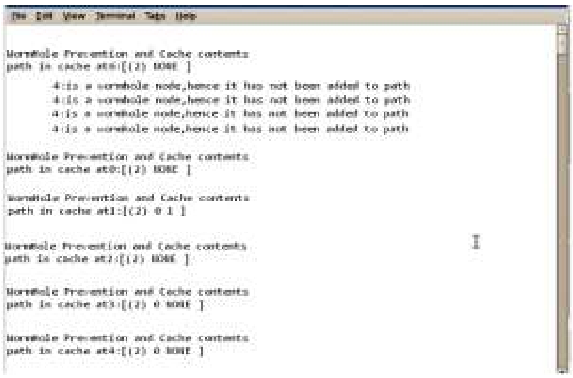
TABLE I. TABLE1. NETWORK PARAMETERS

| Parameter | Value | Description |
|---|---|---|
| Simulation time | 600Sec | Maximum execution time |
| Terrain Dimensions | 1000, 1000 | Physical area in which the nodes are placed in meters |
| Number of Nodes | 5 | Nodes participating in the network |
| Traffic Model | CBR | Constant Bit Rate link used |
| Network Model | Random waypoint | Node placement policy |
| Routing Protocol | DSR | Routing protocol used |
| Transport | UDP / TCP | For transport the packet |
| Mobility | 100 (m/s) | Speed of node with which they are moving |

## IV. RESULT AND ANALYSIS

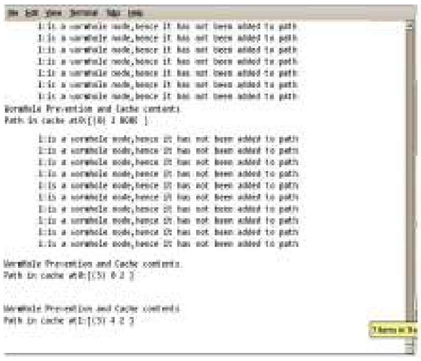
### A. Simulation script result

We have taken the simulation scenario of 5 nodes in which nodes 1 and 4 are the wormhole nodes. After running simulation script with 5 nodes, nodes 1 and 4 detected as the misbehaving nodes. From the output on the command prompt, it shows the detection of such nodes and then later they are prevented by taking the other routes for the communication of the same. As shown in Fig 3, it's clear that node 4 in the network is wormhole and then whenever during simulation, node 4 comes in the routing path, then that node is removed from the path and take another route for the same in order to successful transmission of the data from source node to destination. The same is the case when node 1 acting as wormhole as shown in Fig. 4.



```
WormHole Prevention and Cache contents
path in cache at6:[(2) NONE ]
        4:is a wormhole node,hence it has not been added to path
        4:is a wormhole node,hence it has not been added to path
        4:is a wormhole node,hence it has not been added to path
        4:is a wormhole node,hence it has not been added to path

WormHole Prevention and Cache contents
path in cache at0:[(2) NONE ]

WormHole Prevention and Cache contents
path in cache at1:[(2) 0 1 ]

WormHole Prevention and Cache contents
path in cache at2:[(2) NONE ]

WormHole Prevention and Cache contents
path in cache at3:[(2) 0 NONE ]

WormHole Prevention and Cache contents
path in cache at4:[(2) 0 NONE ]
```

Fig.3 Node 4 acting as wormhole



```
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
WormHole Prevention and Cache contents
Path in cache at0:[(0) 1 NONE ]

        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path
        1:is a wormhole node,hence it has not been added to path

WormHole Prevention and Cache contents
Path in cache at0:[(3) 0 2 ]


WormHole Prevention and Cache contents
Path in cache at1:[(3) 4 2 ]
```

Figure 3. Fig.4 Node 1 acting as wormhole

Following are overall scenario for the existing DSR

Average End to end delay: 0.0011 sec

Average Throughput: 380 packets/TTL

Average Jitter: 0.00026 Sec

Following are overall scenario for the modified DSR

Average End to end delay: 0.0012

Average Throughput: 375 packets/TTL

Average Jitter: 0.00015 Sec

Thus results shows that for jitter and throughput, on the average both existing and proposed approaches have minor difference in their values as shown in table 2. and for end to end delay both existing and proposed approach have almost similar values. These small variation is due to wormhole attack detection and new route discovery. Thus without affecting the overall performance of the network new technique for wormhole avoidance have been implemented.

TABLE II. TABLE 2: COMPARISON OF EXISTING DSR AND MODIFIED DSR

| Techniques | No. of nodes | Throughput | Delay | Jitter |
|---|---|---|---|---|
| Modified DSR | 5 | 375 packets/TTL | 0.0012 sec | 0.00015 Sec |
| Existing DSR | 5 | 380 packets/TTL | 0.0011 sec | 0.00026 Sec |

## V. COMPARISON CHARTS

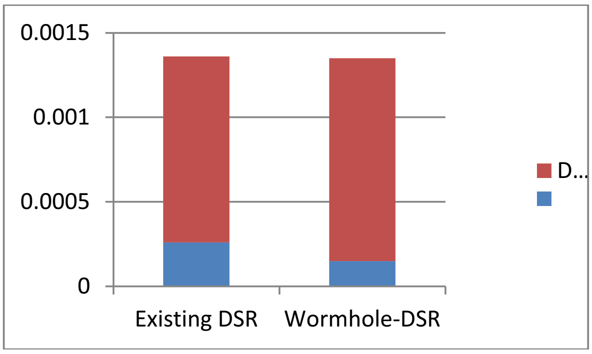


Figure 4. Fig.5 Comparison of existing DSR and modified DSR (for wormhole prevention) for parameters Jitter and Delay

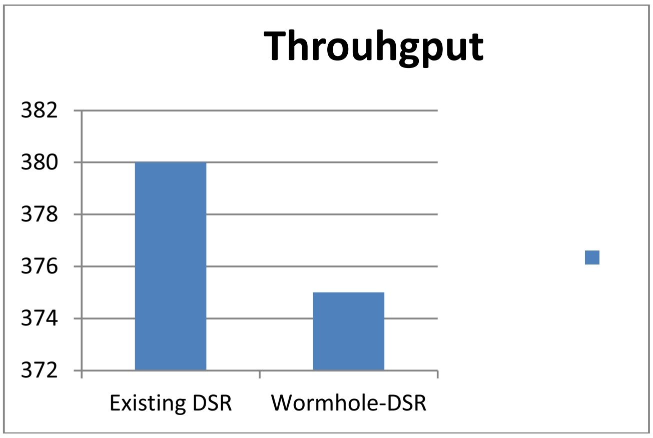


Figure 5. Fig.6 Comparison of existing DSR and modified DSR (for wormhole prevention) for parameter Throughput

Comparison charts shown in Fig.5 and Fig.6 shows negligible change in performance metrics (jitter, delay and throughput) after implementing the modified DSR for wormhole avoidance, which does not disturb the network performance but detects the wormhole nodes successfully in the path and the routes having such nodes are simply dropped and not taken in the future. As the number of nodes and network size grows, this performance level goes to the equal performance for both existing DSR and modified DSR system. Thus the proposed approach is showing security enhancement while maintaining the performance level and overall system lifetime.

## VI. CONCLUSION

Presence of the attacks in the network or misbehaving nodes in the network is one of the major security issues for the MANET. This work concerned with a particularly sever security attack that affects the ad hoc networks routing protocols, called wormhole attack. The proposed approach simulates the wormhole nodes and misbehaving nodes and finds the ways to detect and prevent it. The routing protocols which is used here is the dynamic source routing protocol (DSR), which is modified in order to prevent wormhole attack in MANETs. Simulations results shows how selfish nodes or malicious nodes comes into the routing and when they are found in any routing path, proposed DSR detects such nodes and the routes which contains the misbehaving nodes, are simply dropped and not added into the routing table of the DSR so that in future that routes are not used in any communication. It fires the message of wormhole node detection without disturbing the network performance for parameters jitter, throughput and end to end delay.

This type of wormhole analysis is important to account for possible new dangers and variations of this attack. Furthermore, it can help in putting some constraints on the network topology to design a robust network for such attacks, and in the design of new and more powerful attack countermeasures.

## Acknowledgment

Financial assistance provided by UGC, New Delhi in form of major research project to Dr Yudhvir Singh, PI is acknowledged with thanks.

## References

[1] Abhishek Seth, “Seminar Report on Security Issues in MANETs”, Proceedings of abstract uation of wireless ad hoc, sensor, and ubiquitous networks, pp-69–78, 2004.

[2] B. Wu, J. Chen, J. Wu, M. Cardei, “A Survey on Attack and Countermeasures in Mobile ad hoc Networks”, Dept. of computer science and engineering, Florida Atlantic University, under review at Wiley Journal Wireless Communication and Mobile Computing (WCMC), 2006.

[3] D. Barman Roy, R. Chaki, N. Chaki, “A new cluster-Based Wormhole Intrusion Prevention Algorithm for Mobile Ad-Hoc Networks”, International journal of network security and its application, vol.1, pp-44-52, 2009.

[4] **Yudhvir Singh**, Yogesh Chaba, “Security & Network Performance Evaluation of KK’ Cryptographic for Mobile Adhoc Networks” *Proc. IEEE IACC 2009* [Online : IEEE Xplore Digital Library, Digital Object Identifier: 10.1109/IADCC.2009.4809177], pp. 1152-1157 Available: http://ieeexplore.ieee.org/ (2009).

[5] Yogesh Chaba, **Yudhvir Singh**, Prabha Rani, “Comparison of Various Passive Distributed Denial of Service Attack in Mobile Adhoc Networks” *Proc. WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communication(EHAC 10),Cambridge,* UK (ISBN: 978-960-474-155-7), pp 49-53 (2010).

[6] Jen Shang-Ming , Laih Chi-Sung and Kuo Wen-Chung, “A Hop-Count Analysis Scheme for Avoiding wormhole Attacks in MANET”, Fourth International Conference on Systems and Networks Communications, pp-5022-5039, 2009.

[7] Yogesh Chaba, **Yudhvir Singh**, KP Singh, Prabha Rani, “Performance Analysis of Impact of Multiple Mode Wormhole Attacks on various Routing Protocols in Mobile Ad Hoc Networks“ *Communications in Computer and Information Sciences, Springer* [Online : Springer Digital Library] (2010) Volume 101, Part 3, pp 518-527, (2010).

[8] L. Qian , N. Song and X. Li , “Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path”, Wireless Communications and Networking Conference, vol.4, pp-2106-2111, 2005.

[9] **Yudhvir Singh**, Yogesh Chaba, Prabha Rani, “Integrating – VPN and IDS – An approach to Networks Security”, *International Journal of Computer Science & Security*(ISSN: 1985-1533), Vol. 1, Issue 3, pp. 1-13(2007).

[10] M. Azer, S. El-Kassas, M. El-Soudani, “A Full Image Of Wormhole Attacks Towards Introducing Complex Wormhole Attacks In Wireless Ad Hoc Network” , International journal of computer science and information security, vol.01 , pp-41-52, 2009.

[11] M. Natu , A. Sethi , “Intrusion Detection System To Detect Wormhole Using Fault Localization Techniques”. Proceedings of international conference on security and management, 2007

[12] S. Choi, D. Kim, D. Lee, J. Jung, “Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks”, International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pp-343-348, 2008 IEEE.

[13] V. Mahajan , M. Natu , A.S. Sethi , “Analysis of Wormhole Intrusion Attack In MANETs”, In proceedings of IEEE military communication conference, 2008 IEEE.

[14] Prabha Rani, Yogesh Chaba, Yudhvir Singh, “Hybrid Approach for Detection and Prevention of Blackhole Attack in Mobile Adhoc Network”, *International Journal of Wireless Communication,* ISSN 0974-9640, August, 2011.

[15] KP Singh, Yogesh Chaba, Gaurav Lodha, **Yudhvir Singh**, “Intrusion Detection System for Protection against Packet Dropping Attack on Distributed Information Syatem in any Organization” *International Journal of Networking and Communication Engineering,* ISSN 0974-9616, (2011).

[16] W. Wang, B. Bhargava, Y. Lu, X. Wu, “Defending Against Wormhole Attack In MANETs”, under review at Wiley Journal Wireless Communication and Mobile Computing (WCMC), vol.6, pp-483-503, 2006

[17] Y. Chun- Hu , A. Perrig, B. Johnson David, “Wormhole Detection in Wireless Ad Hoc Networks”, In Ninth International Conference on Network protocol (ICNP), vol.1, 2002.

[18] Renu Dalal, Manju Khari, **Yudhvir Singh**, “Survey of Trust Schemes on Ad-hoc Network”, *Springer - Lecture Notes of the Institute for Computer Sciences, Social Informatics & Telecommunications Engineering (LNICST) Series,* ***Springer****, NETCOM-3, (2012).*

[19] Avni Khatkar, **Yudhvir Singh**, “Performance Evaluation of Hybrid Routing Protocols in Mobile Adhoc Networks”, *Second International Conference on Advanced Computing & Communication Technologies*, 2012

[20] S. Jain , “ Detection and prevention of wormhole attack in mobile adhoc Networks”, International Journal of Computer Theory and Engineering, vol.2, pp-78-85, 2010

[21] NS2 Manual and ns2.29 installation pdf .