An Approach to Detect Wormhole Attack in AODV based MANET

Neha Dubey
Maharana Pratap College Of Technology
Gwalior (M.P) India

Krishna Kumar Joshi
Maharana Pratap College Of Technology
Gwalior (M.P) India

ABSTRACT
Wireless networks are playing very important role in the present world. Mobile Ad hoc Networks (MANET) are the extension of the wireless networks. These networks are playing crucial role in the each and every field of the human life. They are used in those places where a simple wireless network cannot use. They play a significant role in real tile applications such as military applications, home applications wireless sensor applications etc. Due to their adaptive nature they are threatened by number of attacks such as Modification, Black Hole attack, Wormhole attack etc.

Wormhole attack is one of the dangerous active attacks in the mobile Ad hoc Networks (MANET). In this paper a secure and efficient approach for the detection of the wormhole attack in the Mobile Ad Hoc Networks (MANET) is described. The proposed algorithm is implemented on a very popular on Adhoc On Demand Distance Vector known as AODV routing protocol. The beauty of this proposed algorithm is that it not only identifies the wormhole attacker node but also confirm it as well. To simulate the effect of the proposed work the popular NS 2(Network Simulator 2) is used.

General Terms
Mobile Adhoc Networks, Routing protocols, Active attacks, Passive attacks, Reactive Routing protocol, Algorithm.

Keywords
MANET; AODV; RREP; RREQ; Wormhole

1. INTRODUCTION
Wireless Networks can be classified into two categories:

Infrastructure Wireless networks and Infrastructure less Wireless Networks.

In Infrastructure Wireless networks, communication takes place between the Wireless nodes through the Access Point (AP) and the wireless nodes cannot communicates directly. The access point just not works as a control medium access, but acts as a bridge as well.

Infrastructure less Wireless Networks do not need any fix infrastructure for the communication. These networks are also called Ad Hoc Networks. In these types of networks, each node can communicate directly with other node and thus there is no requirement of the access point. An important thing about these networks is that these networks do not have routers, the wireless nodes work as routers. These networks don't have any fixed or static topology.

Mobile Ad hoc networks are collection of mobile nodes that use wireless transmission for communication. These networks have no fixed infrastructure, no fixed configuration and other controlling device such as router etc. The setup or deployment of these networks is very easy because these networks don't have a fixed infrastructure or a fixed topology also they have a very less setup time. The routers are free to move randomly.

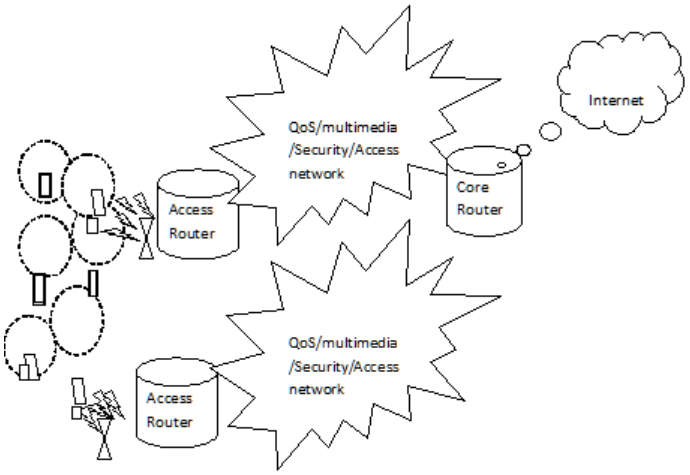


Fig 1: Mobile Ad hoc Networks

2. ROUTING PROTOCOLS
Many protocols have been suggested for Mobile Adhoc Networks keeping applications and type of network in view. Routing protocols can be classified mainly into three categories, as defined below:

2.1 Proactive Routing Protocols
In Proactive routing protocols each node maintains one or more tables containing routing information about all other node in the network. All nodes keep on updating these tables to maintain latest view of the network. Some popular proactive protocols are: DSDV, WRP and ZRP

2.2 Reactive Routing Protocols
In these protocols, the nodes don't maintain a routing table. Instead, they maintain a route cache. Routes are created only when a node want to communicate with another node. For this purpose source invokes the route discovery procedure. Some reactive routing protocols are: DSR, AODV and TORA

2.3 Hybrid Routing Protocols
This type of protocols contains the best features of proactive and reactive routing protocols. In case of the intra-domain routing, these protocols uses the proactive approach, while in case of inter-domain routing these protocols uses the reactive approach For example, Zone Routing Protocol (ZRP) etc.

3. WORMHOLE ATTACK
Wormhole attack is one of the most dangerous attacks in the mobile Ad Hoc Networks. In wormhole attack, two or more malicious nodes together makes a tunnel in the network, in which the traffic is enter from one end and passes through the tunnel and leaves from the other end [10]. Wormhole link or tunnel can be created by means of a high quality wireless link or a logical link. After building a wormhole link, one attacker is able to receive all the messages which travel from this

route. This attacker node then copies packets from its neighbors, and forwards them to the other malicious attacker through the wormhole link. Then another malicious node which receives these packets, replays them into the network in its vicinity. Figure 2 showing the wormhole tunnel

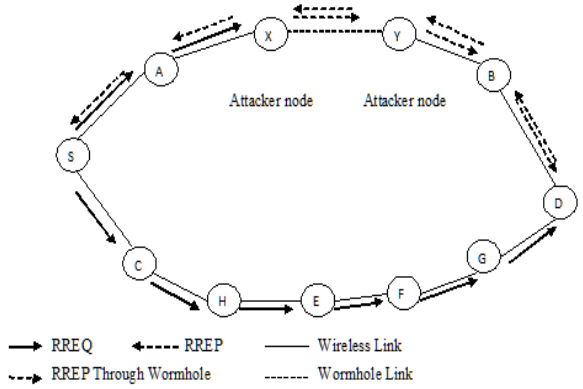


Fig 2: Wormhole Attack.

3.1 Active Attacks

Active attacks are the kind of attack in which the attacker can see the information of a user and can modify it too. These attacks contain some modification on the actual data or a false data. In these attacks, the attacker injects arbitrary packets into the network. The goal may be to attract packets destined to other nodes to the attacker for analysis or just to disable the network. Active attacks sometimes are detected. This makes active attacks a less inviting option for most attackers. These attacks can be subdivided into four categories: replay, modification of message, masquerade and denial of service. An active attack may be internal or external.

Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network. Modification, Impersonation and Fabrication are some of the most common attacks that cause a big security concern for DSR.

3.2 Passive Attacks

In a passive attack the attacker can learn or use the information of a user but does not modify nor change it. In a passive attack, the attacker does not change or alter the operation of a routing protocol but only attempts to discover valuable information. Defending against such attacks is very difficult. Two important passive attacks are the traffic analysis and the release of the message contents.

These attacks are very difficult to detect because they do not involve in any modification of the data. Routing information contains the relationships among nodes and also information about the nodes such as their IP addresses, hardware addresses etc. so if attacker is able to find the routing information, he can easily extract the information about the nodes and about the relationship among the nodes.

4. AODV PROTOCOL

As a routing protocol for mobile ad hoc networks, AODV is intended to accommodate networks that are as large as several thousand nodes. It is one of several *demand-driven* (or *on-demand*) protocols that are in existence today. Hence, the protocol is invoked only when a node (host) has data to transmit. It is a *reactive* protocol. The AODV RFC indicates that the transport layer protocol is UDP, which of course only offers best effort delivery of packets, and does not support either error recovery or flow control. Addressing is handled using IP addressing. Since each node acts as both a host and routing node, each must maintain a routing table that contains information about known destination nodes. Entries are keyed to destinations. Each entry in the routing table contains nine fields. In addition to the destination node IP address, the fields contain routing information and information that relates to the qualitative state of the route for maintenance purposes. AODV only maintains information on the next destination (hop) in the route, not the entire routing list. This saves memory and lowers computational overhead for route maintenance. It also contains information enabling the host to share information with other nodes when link states change. The sequence number, unique to each destination route, is the key to maintaining up to date routing information. Protocol messages that contain routing information also include a sequence number. By observing the value of the sequence number, an intermediate node can determine the "freshness" of the routing information.

The basic message set consists of RREQ (Route Request), RREP (Route reply), RERR (Route error) and HELLO message.

4.1 RREQ Messages

- When communication routes between nodes are valid, AODV does not play any role.
- When a node wants to discover a route to a destination, a RREQ message is broadcasted.
- Intermediate nodes use RREQ to update their routing tables (in the direction of the source node), as it propagates through the network.
- The RREQ also consists of the most recent sequence number for the destination.
- A sequence number is must to the valid destination route at least as great as that contained in the RREQ.

Route Request (RREQ) Message Format

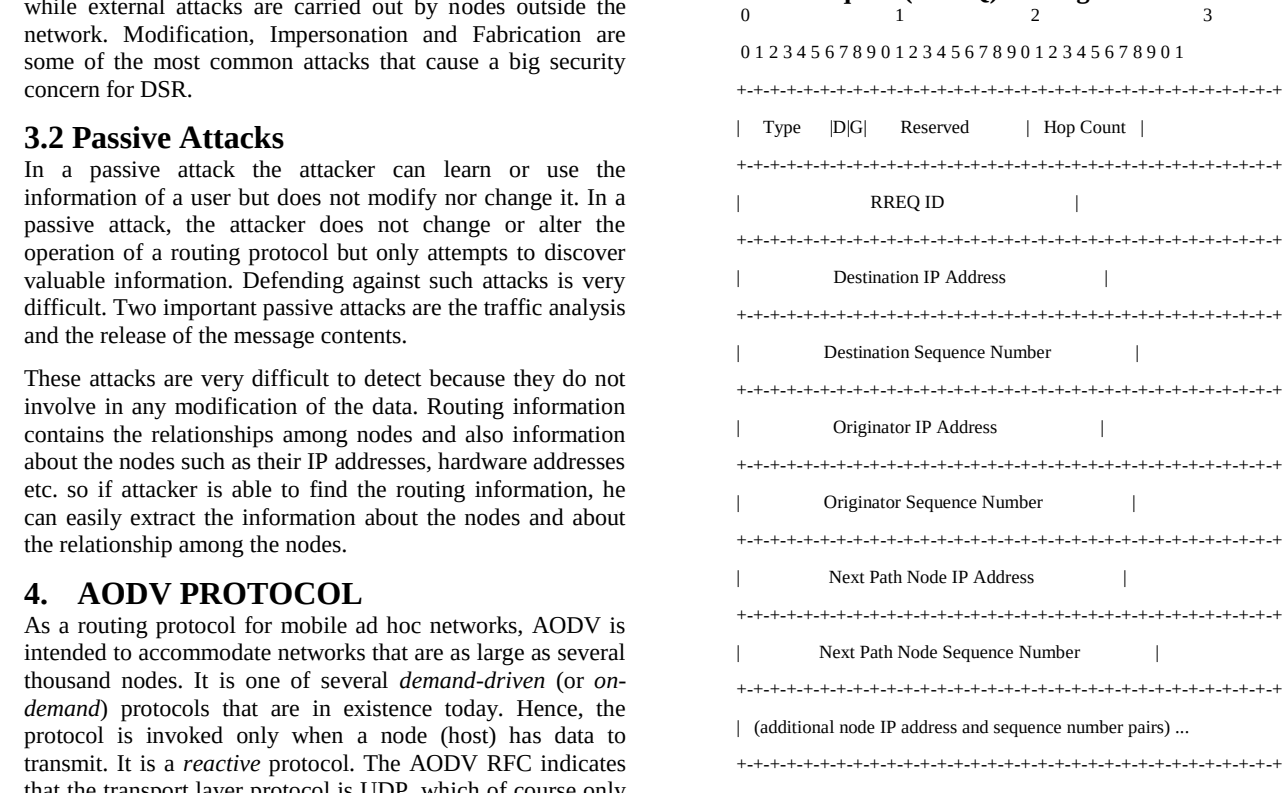


Fig 2: RREQ Packet

4.2 RREP MESSAGES

 When a destination node has a RREQ message, the destination route is made available by unicasting a RREP back to the source route.

 Intermediate nodes update RREP routing tables (in the direction of the destination node), as the RREP propagates back to the source node

Route Reply (RREP) Message Format

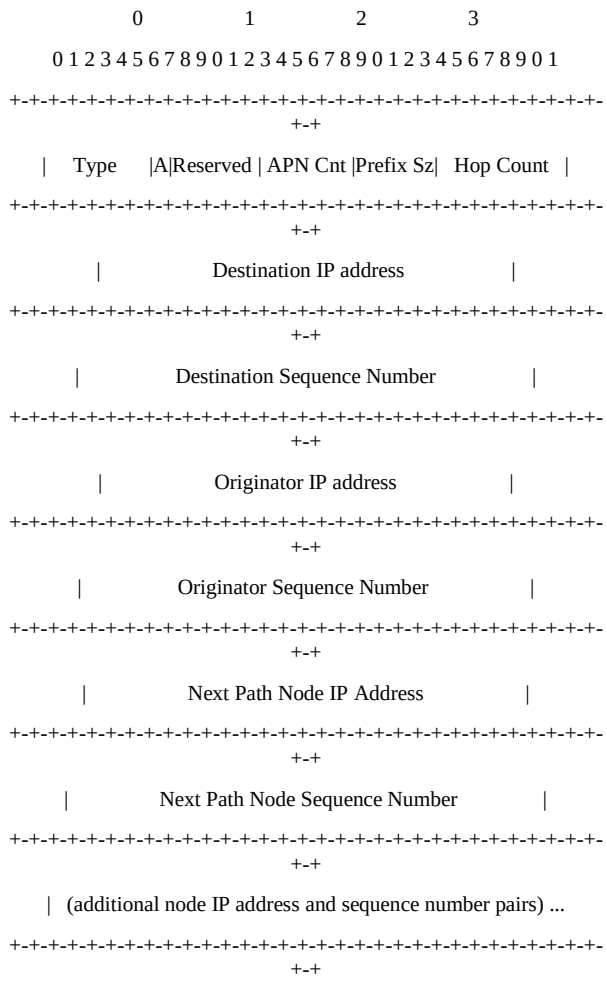


Fig 3: RREP Packet

4.3 Route Error (RERR) Message

 For broken links, RERR message is broadcasted.

 Directly generated by a node or passed on when received from another node

Route Error (RERR) Message Format

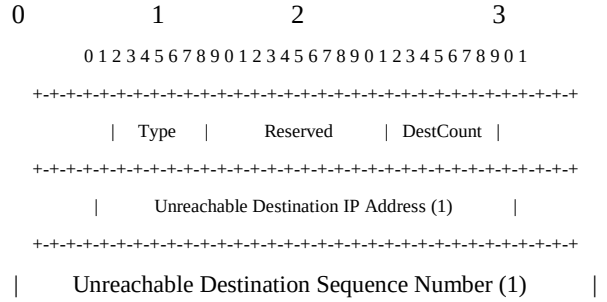


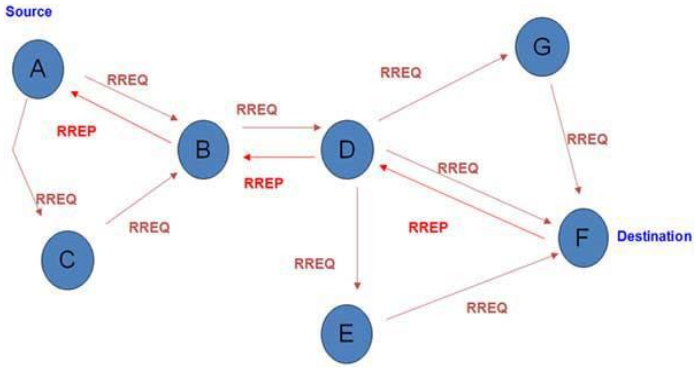
Fig 4: RERR Packet

4.4 Hello Messages

 Hello Message = RREP with TTL = 1

 For broadcasting connectivity information, this message is used.

 Anode should use Hello messages only if it is part of an active route.



5. LITERATURE REVIEW

Wormhole attack is one of the most dangerous attacks. Many researchers did their work on this attack and try to provide the solution for this attack. The researchers provide a lot of solution based on different technologies, concepts and terms. Some important approaches are described below

Marianne et al [1] proposed an algorithm based on the theory of diffusion of innovations. The algorithm is divided into five phases: Normal network routing, wormhole parameters measurement, actor's network formation, route selection using penalties and intrusion detection. In the normal network routing phase AODV protocol find the route on the basis of minimum hop count. Also a counter is added to check how many times a particular node participated in routing. In wormhole parameter phase some parameters such as arrival speed are measured for malicious node identification. In the actor's network formation phase, when a node receives the RREQ/RREP packet, compares how many hops offered by the incoming packet and by the routing table entries. Then it selects a node which has minimum hop count and has a recent route to the destination. Then it checks how many times this selected nodes participated in routing for a particular destination and if it has greater value than the threshold then this node is treated as a malicious node.

Kuldeep Sharma et al [2] proposed an approach which is based on the MHA (Multiple hop count analysis) .in this approach they use a general concept that the route contains the hop count 5 or 6, but the route under a wormhole has a hop count value 2. So, if the users avoid the route with the small hop count can easily avoid most of the wormhole attacks. In this approach, they calculate the hop count value for all the routes and then select a safe set of routes for the transmission of the data. And then send the packet in a random order by

these safe routes. They implemented their approach in the AODV routing protocol. Then they assign a unique ID to each and every node so that we can easily differentiate between the simple node and the attacker malicious node.

Yih chun hu et al [3] propose an approach, called packet leashes. The lease contains timing and global positioning system information about each packet on the basis of hop by hop. So a node can easily detect that that whether the packet which he received has travelled a distance larger than the physically possible by using the information stored in a packet leash. There are two types of the leashes: geographical and temporal. Geographic leash requires loose clock synchronization. Temporal leases works on tighter clock synchronization and also they are not dependent on GPS.

Khalil et al [4] propose a protocol, called LiteWorp for wormhole attack discovery, basically for the static networks. In this LiteWorp approach, all the nodes of the mobile ad hoc networks obtain the complete routing information about their neighbour nodes. In comparison to the normal routing protocols where the nodes finds the information about their neighbouring nodes by using the route discovery process, in LiteWorp approach the nodes actually knows who is their neighbour and who is the neighbour of the neighbour because LiteWorp approach uses two hop routing approach to find the information about the neighbouring nodes rather than the one hop approach This information is very useful to detects the Wormhole attack because nodes can easily analyze the behaviour of their nodes and detect that which node is the malicious node and by this they can easily avoid the wormhole attack.

Pirzada et al [5] proposed an algorithm which does not need any special hardware. This approach is mainly works on the round trip time mechanism. Basically, the round trip time is the total time to send the message to the destination plus the time to receive the acknowledgement receiving time. Generally, the round trip time is twice of the propagation time. In this approach the round trip time is calculated as the total time to send the route request message from the source to the destination node plus the time to receive the route reply message from the destination. The round trip time between the two real neighbour nodes is always less than the round trip time between the two malicious (fake) nodes. By this theory, a node can easily differentiate between a real node and a malicious fake node. In this approach, every node do this work, means every node calculates the round trip time between itself and all of its neighbour node and thus easily detects the malicious node.

Hubaux et al [6] proposed anther solution for detection of the wormhole attack by using the directional antennas. In this approach node uses the specific sectors of their antennas to communicate each other. So every node has the information about the location of its neighbor when it receives a message from its neighbor. So this extra information about the location of the nodes is very useful in case of detection of the wormhole attack.

S. Capkun et.al [7] Proposed a secure scheme for the detection of the wormhole attack in wireless sensor networks. This scheme is based on an authenticated distance bounding technique, called MAD. This approach is similar to the packet leashes approach at a particular, but has some significance differences. This approach does not require the information about the location and clock synchronization, which are needed in the packet leashes. In this scheme to find the distance for secure location verification ultrasound is used. This helps to relax the timing requirements. Also for the verification of the true neighbor, means it is not a fake neighbor, this scheme is used. The main problem with this scheme is that it needs an additional hardware and also it still remains unclear that how the realistic timing analysis will be done at the lower cost for the wireless sensor networks.

Saurabh gupta et al [8] proposed an approach, called WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on the AODV protocol. In this approach a Hound packet is sent after the route discovery process, means after the route has been discovered. This hound packet is processed by all the nodes, except that nodes which are involve in the path setup process. Basically the path discovery is done by the help of the two types of packet, called RREQ and RREP. When the sender get the message, it creates a hound packet and computes its message digest and signed this message digest with its own private key and attached all this information with the hound packet.

Xia Wang et al (9) In this article we presented an end-to-end detection of wormhole attack in wireless ad hoc networks. A simple comparison method based on the estimated shortest path and the actual shortest path is used to determine whether there is a wormhole attack for each received route. Once a wormhole attack is detected, the source node launches wormhole TRACING procedure to identify the two end points of the wormhole and the result is broadcast into the network to warn other nodes. Finally, based on the wormhole detection and identification the source could select a shortest route from a set of legitimate routes. Our EDWA wormhole detection method is novel in that it is the first approach using end-to-end method in wormhole attack detection and wormhole identification. Both analysis and simulation results show that EDWA is effective when the source and destination are not too far away.

Pushpendra Niranjan et al (10) Our method provides good performance for detecting tunneling attacks it detects 75 percent of attackers within five minutes, In addition, since we only select part of the searched routes for multi-path transmission, the probability that attacks can occupy the route are further reduced. In another scenario, attackers may maliciously modify other nodes instead of itself in the graylist. Thus the nodes that have been modified would be reported as modifiers and be blocked by the source node. To counter this, some ID-based cryptographic methods such as digital signatures can be adopted to prevent this.

Subrat kar et al (11) This paper proposes routing protocol WHOP which we have seen in simulation is quite well in detecting wormhole of large tunnel length without support of any hardware and clock synchronisation. WHOP does not require significant changes in the working of existing AODV protocol, it uses an additional Hound packet for wormhole detection, so if adhoc network is formed between trusted parties or private use then security related issues will not be needed hence we would not send Hound packet but if network is public and nodes experiences high packet dropping then Hound packet will be send after the path discovery phase. Hence WHOP can easily be included in the wide range of ad hoc routing protocol with only significant change in the existing protocol to defend against wormhole attack As future work, we intend to optimize the hound packet to overcome from processing delay of the packet. We also plan to improve the table entries at destination node to get the detection of wormhole nodes faster.

Harbir Kaur et al (12) This paper proposes a solution for wormhole attack in VANET. Wormhole attack is the most dangerous attack as it can also become a cause of other attacks like sink hole attack as it creates a sinkhole in the network by falsifying the route information, DOS attack as by discarding the packet in the wormhole results in permanent denial of service. By introducing the decision packets the occurrence of the wormhole reduces to a great extent. Moreover, it does not require any additional hardware to be installed on the nodes.

Dr. A. Francis Saviour Devaraj et al (13) In this paper, a novel approach, WAD-HLA to detect wormhole attack in MANET is proposed.The main advantage of WAD-HLA includes the early detection of wormhole attack during AODV route discovery phase, no requirement of specialized hardware or strict clock synchronization, effective mechanism with good performance is achieved. As a part of the future work, we would propose prevention mechanisms for wormhole attack in MANET.

L. Sudha Rani et al (14) The Geographic multicasting routing mechanism has been presented in this paper. Among the existing multicasting routing protocols the reason for selecting.

Robust and Scalable Multicast Geographic Multicast Protocol (RSGM) protocol is it handles empty zone problem very efficiently when compared to the other zone based protocols and it has an efficient source tracking mechanism which avoids the periodic flooding of source information. RSGM has the minimum control overhead and joining delay protocol can also scale to a large group size and a large network size, and can more efficiently support multiple multicast groups in the network. One possible attack on the RSGM protocol has been discussed in this paper. The detection of such attack is difficult and is of course very much important. Multicast Authentication Node Scheme is the solution that is proposed to defend against the wormhole attack in RSGM protocol .This solution clearly shows that the protocol achieves higher Packet Delivery Ratio under all circumstances with different moving speeds, node densities, group sizes, and network sizes.

Jyoti Thalor et al (15) Wormhole attacks in MANET significantly degrade network performance and threat to network security. Here we have basically surveyed the existing approaches which will help us in future to design a new approach for detecting the wormhole attack in Mobile Ad Hoc network Overall a significant amount of work has been done on solving wormhole attack problem. We can‟t say one solution is applicable to all situations. So there is choice of solution available based on cost, need of security may lead better result, but can be costly, which may affect other networks need. Similarly some network require more security like military area network. A standard solution is still lacking, although several very useful solutions applicable to some networks have been described.

6. PROPOSED WORK

In the previous section we described a lot of approaches for the detection of wormhole attack in Mobile ad hoc Networks. Even though these approaches are very good but some of them have limitations also. In this paper a secure and very efficient approach for the detection of the Wormhole nodes is described. We implement this work in a popular reactive routing protocol, called AODV protocol. This approach will help to reduce the processing delay. So this will improve the speed of the searching .

6.1 Algorithm

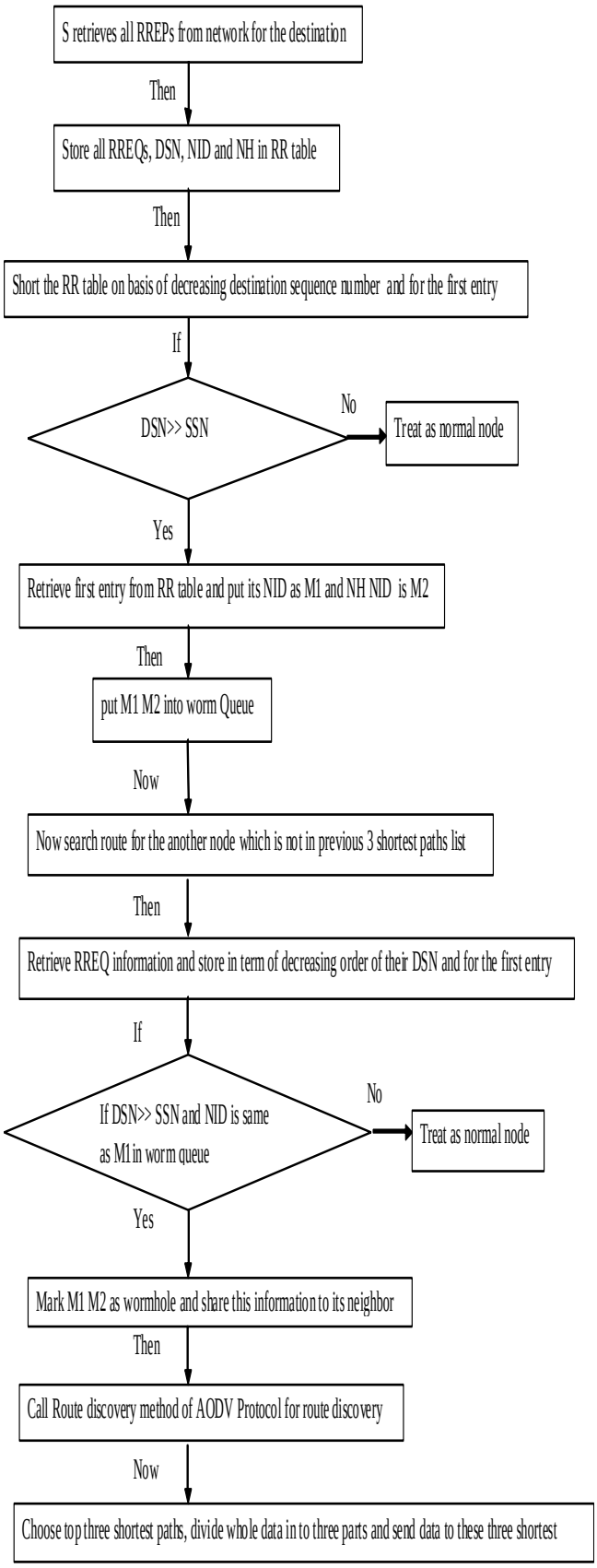
Initial notation---------

Source node =S, Destination node = D, Malicious Nodes = M1, M2(Wormholes),

Destination sequence number DSN, NODEID= NID, Next Hop = NH

- **Step 1** (network initialize process)
- Get the current time (CT)
- Wait for the constant time and retrieve RREP information of network
- **Step 2** (Storing the information get in step1)
- Store all the RREPs ,DSN,NID and NH in RR table .
- **Step 3**(identify the malicious behavior and make its suspicious behavior)
- Short the RR table on the basis of destination sequence number
- Retrieve the first entry from the RR table if DSN>> SSN and its shows the shortest path to destination.
- NID in first entry is M1 and NH NID is M2
- **Step 4** put M1 M2 into gray Queue
- **Step 5** now search route for the another node
- **Step 6** Get the current time (CT)
- Wait for the constant time and retrieve RREQ information of network
- **Step 7** Store all the RREQs ,DSN,NID and NH in RR table .
- **Step 8** (identify the malicious behavior and make its malicious)
- Short the RR table on the basis of destination sequence number
- Retrieve the first entry from the RR table if DSN >> SSN and its shows the shortest path to destination.
- NID in first entry is M1 and NH NID is M2
- **Step 9** marks M1 M2 as wormhole
- **Step 10** share this information to its neighbor
- **Step 11** (continue default process)
- Call Route discovery method of AODV Protocol for route discovery
- **Step 12** sorts all the path of RR table on the basis of hop count
- **Steps 13** choose top three shortest paths.
- **Step 14** divide whole data in to three parts and send data to these three shortest paths.

6.2 Flow Chart



7. IMPLEMENTATION AND RESULTS

The proposed work is implemented in NS-2 (ns 2.34) simulator and executed on a AMD Turion II Dual-Core Mobile M500 processor with 3 GB of RAM, running at 2.40 GHz under Fedora workstation 10.0

8. PARAMETERS

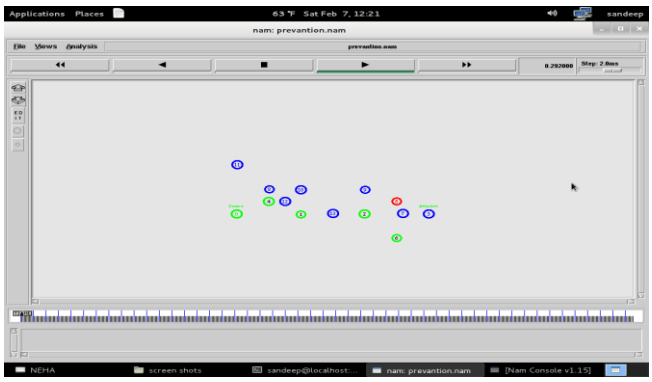
The effectiveness of work to detect the Wormhole attack is evaluated in this subsection using the simulations performed in a very popular simulator, called Network Simulator (NS)-2 with the 10 mobile nodes. The graphical representation of this simulation is shown in the popular animator, called Network Animator (NAM).The traffic type is Continuous Bit Rate (CBR), the channel used is a wireless channel, the Ad hoc routing protocol used is AODV and the network interface is wireless physical.

Table 1. Table captions should be placed above the table

Parameter	Value
Number of Nodes	Variable (10,20, and 50)
Topography Dimension	750 m x 750 m
Traffic Type	CBR
Signal Propagation Model	Two Ray Ground model
MAC Type	802.11 MAC Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Antenna Type	Omni directional
Mobile Ad Hoc Routing Protocol	AODV
Interface Queue	Drop Tail/Priority Queue
Maximum packets in Interface Queue	100
Channel	Wireless Channel
Link Layer Type	LL
Network Interface Type	Wireless Phy
Number of Wormhole attackers	1

9. SIMULATION RESULTS

Below figure(1) is showing the simulation scenario of the 10 mobile wireless nodes. This figure is used to show the initial position of these nodes.



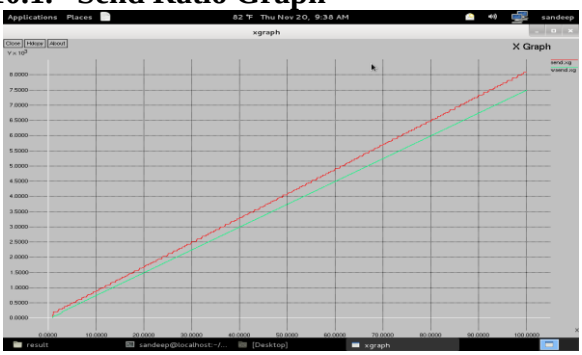
Simulation of 10 Mobile Nodes Implementing AODV Protocol

Figure (2) is showing the movement of the scenario file contains the location of the mobile nodes

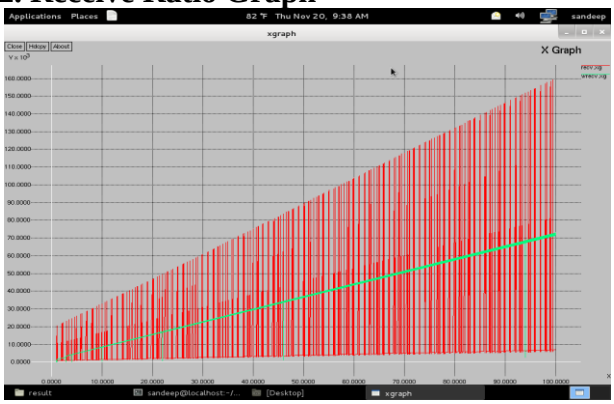
10. SIMULATION GRAPHS

Three graphs end to end delay, throughput and packet delivery ratio are described here to show the simulation results. Every graph contains three sub graphs. The first graph is for the simple AODV protocol, when there is no attacker node presented. This graph is shown by the Dark blue color. Second graph is for the case where there are the attacker nodes and no prevention algorithm is presented. This graph is shown by the red color. And the last graph is for the case when we implemented our algorithm to identify the attacker nodes. This graph is shown by the green color. Basically the graph is drawn between the time and the number of mobile nodes presented in the network (in our case, there is 10 nodes).The next subsections are used to describe these graphs.

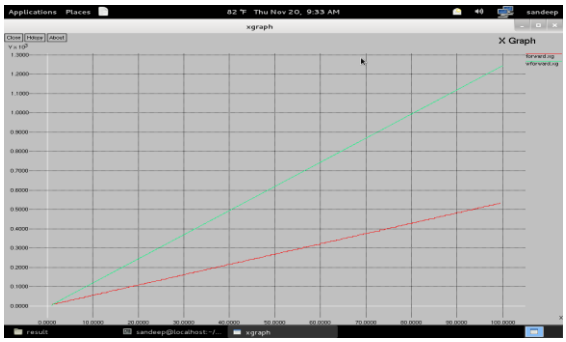
10.1. Send Ratio Graph



10.2. Receive Ratio Graph

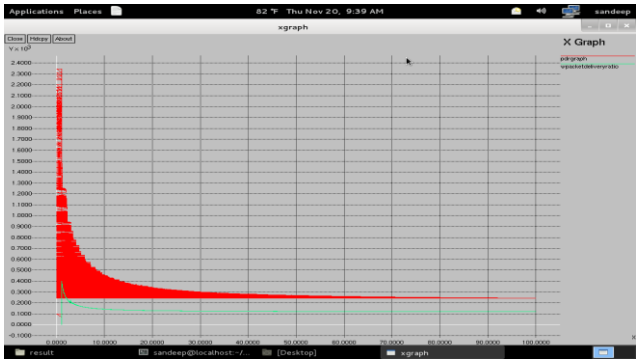


10.3. Forward Ratio Graph



10.4. Packet delivery Ratio Graph

Basically this graph is used to describe the Packet delivery ratio which is the ratio of the total incoming packets and the actual received packets by the destination



11. CONCLUSION AND FUTURE SCOPE

In this paper a secure efficient approach for the detection of the wormhole attack in the Mobile Ad Hoc Networks is described. The algorithm is implemented in AODV protocol. In the proposed approach a solution is provided which is based on the--------

For the future work, it may be worthwhile to merge other solution improvement methods to improve the performance of the proposed approach, so that we can get good results when the number of mobile nodes is large and also the number of attacker nodes is much more.

12. ACKNOWLEDGMENTS

It is with deep sense of gratitude and reverence to **Prof K. K. JOSHI, for providing all the facilities and working environment in the institute.** We want to express our deep sense of obligation to our family and God for their blessings and encouragement.

13. REFERENCES

[1] Marianne A. Azer, , IEEE, Sherif M. El-Kassas, and Magdy S. El-Soudani, " An Innovative Approach for the Wormhole Attack Detection and Prevention In Wireless Ad Hoc Networks", in IEEE Conference, 2010

[2] Kuldeep Sharma**,** Dr.G.Mahadevan, "Advance Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Int. J. on Recent Trends in Engineering & Technology, Vol. 05, No. 01, Mar 2010

[3] Vih-chun-hu, Adrian Perrig, David B.Johnson, "Packet Leashes: A defense against Wormhole Attack in Wireless Mobile AD-HOC network", Rice University Department of computer science.Technical Report TRO1-384 December 17, 2010

[4] Khalil "WAP:Wormhole Attack Prevention Algorithm in Mobile AD-HOC network", Sensor network, Ubiquitous and Trustworthy Computing 2010

[5] A. Pirzada and C. McDonald, "Detecting and evading wormholes in mobile ad-hoc wireless networks", International Journal of Network Security, 3(2):191C202,

[6] P. Hubaux, and L. Buttyan, "Mobility helps security in ad hoc networks", Proceedings of MobiHoc, 2011

[7] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations", Proceedings of the 25th IEEE International Conference on Computer Communications Societies (INFOCOM '06), Barcelona, Spain, April 2011

[8] Saurabh Gupta, Subrat Kar, S Dharmaraja, WHOP: Wormhole Attack Detection Protocol using Hound Packet, 2011 International conference on innovations in information technology.

[9] Xia Wang **,**Ritesh Maheshwari, Jie Gao, Samir R Das, "Detecting Wormhole Attacks in Wireless Networks using Connectivity Information", in IEEE INFOCOM 2011 Alaska..

[10] JohnnyWong "An End-to-end Detection ofWormhole Attack in Wireless Ad-hoc Networks" Department of Computer Science Iowa State University Ames, Iowa 2011.

[11] Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni, Ram Pratap "Detection of Wormhole Attack UsingHop-Count And Time Delay Analysis" information Technology, LNCT (RGPV) Bhopal, India International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 1 ISSN 2250-3153

[12] Subrat Kar, S Dharmaraja, " WHOP: Wormhole Attack Detection Protocol using Hound Packet" Dept CSE Indian Institute of Technology Delhi Hauz Khas, New Delhi , 2011 International Conference on Innovations in Information Technology.

[13] Harbir Kaur, Sanjay Batish & Arvind Kakaria, "An Approach To Detect The Wormhole Attack In Vehicular Adhoc Networks" International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248-9738 Volume-1, Issue-4, 2012

[14] L. Sudha Rani , R.Raja Sekhar (Ph.D) , "DETECTION AND PREVENTION OF WORMHOLE ATTACK IN STATELESS MULTICASTING",International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518

[15] Jyoti Thalor, Ms. Monika, "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks" Department of Computer Science &Applications Kurukshetra University, Kurukshetra Haryana, India, International Journal of Advanced Research in Computer Science and Software Engineering 3(2), February - 2013, pp. 137-142

[16] Dr. A. Francis Saviour Devaraj, Vandana C.P "MLDW-A MultiLayered Detection mechanism for Wormhole attack in AODV based MANET" Scholar, Department of Information Science Engineering Oxford College of Engineering, Bangalore, India International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 3, June 2013

[17] Mahesh Gour, Amrit Sumanyand Ankur Kulhar, " Detection and Prevention of Wormhole Attack in ALARM Protocol (MANETs)" HCTL Open Int. J. of Technology Innovations and Research HCTL Open IJTIR, Volume 4, July 2013 e-ISSN: 2321-1814 ISBN (Print): 978-1-62776-132-1

[18] Sivakumar , Dr. G. Selvaraj**,**"Analysis of Worm Hole Attack In MANET And Avoidance Using Robust Secure Routing Method" International Journal of Advanced Research in Computer Science and Software Engineering 3(1), January - 2013, pp. 235-242 ©

[19] N. Satheesh, Dr. K. Prasadh, " Analysis and Parameterized Evaluation of Impact of Wormhole Attack Using AODV Protocol in MANET", International Journal of Advanced Research in Computer Science and Software Engineering 3(9), September - 2013, pp. 708-713

[20] A.VANI, D.Sreenivasa 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 June 2013