International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 8, August-2014, pp: (83-90), Impact Factor: 1.252, Available online at: www.erpublications.com

Detection and Performance Analysis of MANET under Wormhole Attack

Neha Rani[1], Vinay Rana[2]
[12]Department of Computer Science & Engineering, International Group of Institutions, Sonipat, Haryana

Abstract: Mobile ad-hoc networks are the wireless open media network where there is no physical link between the nodes and the nodes are mobile in nature. Consequently there is no fix topology. The conventional routing protocols can't meet the needs of such networks hence we have different set of protocols for such networks which can be further classified as per their way of collecting and maintaining routing information. However, these protocols make some assumptions about the nodes and network. They do not consider the security issues, treat all the nodes as non-malicious nodes etc.This paper detects and analyzes the performance of mobile ad-hoc network using AODV as the routing protocol, under the launch of wormhole attack in the wireless network. All the simulations are done in ns2.35 simulator.

Keywords: MANET, AODV, NS2.35, Malicious node.

I) INTRODUCTION (MANETs)

Mobile ad-hoc networks are the infrastructure less wireless network i.e. there is no central authority and the nodes are mobile in nature therefore the topology of network is dynamic in nature[2][3]. There are many application areas of MANETS like –military operations, rescue operations during any natural calamity, emergency services and cellular phones[5]. MANETs have many features associated with them like- adhoc in nature, easy and quick to implement, easy to maintain, economical(eliminates cabling cost). Wireless networks have different characteristics, applications and needs than conventional wired network [4]. Consequently traditional routing protocols can't be used to facilitate communication among mobile nodes [1]. Moreover MANETs are open media in nature (there is no network boundary). As a result we need to have different routing protocols for such networks. Routing protocols in MANET can be broadly classified as follows

1) **Proactive routing protocols**: - Every node in the network has one or more routes to any possible destination in its routing table at any given time. e.g. .DSDV

2) **Reactive routing protocols**:-Every node in the network obtains a route to a destination on a demand fashion. Reactive protocols do not maintain up-to-date routes to any destination in the network and do not generally exchange any periodic control messages.e.g. AODV

3) **Hybrid routing protocols**:-Every node acts reactively in the region close to its proximity and proactively outside of that region, or zone. e.g. LANMAR

II) Brief Description of Routing Protocol in MANET(AODV)

Ad hoc On-demand Distance Vector Routing protocol[4][5] is a protocol which is used in Mobile Ad-hoc Networks(MANETS). It is capable of both unicasting and multicasting. It is a reactive protocol. Reactive protocols are those protocol which build routing path when communication between nodes is needed i.e. on demand, path vector which contain route for communication is created at the time when there is need of communication channel between two nodes. - AODV is on demand routing protocol which is used when network mobility is high and all the nodes are trusty. This provide reliable route between the nodes in adhoc network.

In case of AODV, network remains silent until there is request of transmission from a node. As a node broadcast request for connection to some specific node, which called as destination node. All intermediate nodes recode the route and forward the message. As if the message is received by the destination node, it selects the route with minimal hop count and send back the route information to the source node and route information in being stored by intermediate nodes. In order to decrease routing search message overhead, node use sequence no. to identify the recent route and reject the new one if old one is present. Only least sequence no. request are forwarded. Moreover if route failed, total

route will not be repaired only the breaking point will be repaired. In case like is broken or transmission failure the process of route creation will be repeated again. Entries will be refreshed after transmission over.

MESSAGES IN AODV RREQ

A route request message is transmitted by a node requiring a route towards destination node.As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ [4] carries a time to live (TTL) value that defines for how many hops this message should be travelled. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received from any node. Data packets waiting to be transmitted (i.e. the packets that initiated the RREQ) should be buffered locally and transmitted by a FIFO principle when a route is set.

RREP

A route reply message is unicast back to the sender of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

RERR

Nodes supervise the link status of next hops in active routes. When a link break in an active route is detected, a RERR message is used to aware other nodes for the loss of the link. In order to enable this reporting system, each node keeps a precursor list", Which contains the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

III) SECURITY ISSUES IN MANET

Routing protocols associated to MANET lack two features viz. security (since there is no central authority) and cooperation (since nodes are mobile and may behave selfish at times). Conventional security solutions [7] used for wired networks fall ineffective and inefficient for wireless network [10]. Hence to create security solutions for these networks we need to take in mind their vulnerabilities such as:

Dynamic topology- in addition to the absence of any network boundary, the interconnected nodes are mobile in nature. Consequently the topology of network keeps changing which makes it even harder to differentiate the normal behavior of network from malicious.

Wireless links connecting the nodes- since radio waves or other wireless links are used to interconnect the nodes forming a network, it makes the network susceptible to attacks such as interference(active) and eavesdropping. Also attackers may consume network bandwidth.

Cooperation- Routing algorithms in MANET assume that all the nodes are non-malicious and cooperative in nature consequently the attacker can easily become an routing agent and affect the network topology and operations.

Absence of network boundary- there is no clear line of defense that separates the network from outside world.

Limited resources- MANET may consist of variety of communicating devices like mobile phones, PDAs, laptops etc. these devices may have different storage and computing ability. Battery of communicating devices is the main resource in case of MANET that must be taken care.

Attacks in MANET
Attacks that may be launched in MANET can be classified in many ways.

Internal vs. external attack

- Internal attack-These attacks are caused by compromised nodes, which are the part of our network.
- External attacks-carried out by the nodes that don't belong to the domain of our network.

Active vs. passive attack

- Active attack-Attacker tries to alter the data being exchanged over network and may disrupt normal functioning of network. He may also inject,drop or alter the packets.

• Passive attack-Attacker just snoopes the data exchange over network without altering it.This attack targets confidentiality. However it is hard to detect,easy to launch and may lead to active attacks.

Wormhole attack

It [7][8] is an active , network layer attack to the network.A malicious node receives the packet at one end in the network and tunnels them to another location where they are resent to the network. This tunnel between two attackers is called as wormhole. This tunnel could be established through wired link or wireless link. When this attack is used against an on-demand routing protocol it can prevent the discovery of any routes other than through the wormhole[12].

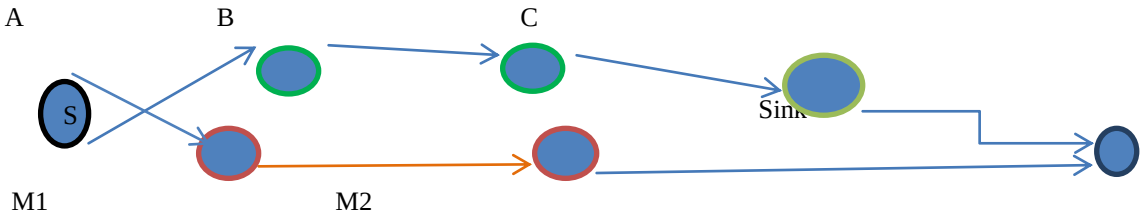

Fig 1. Wormhole attack

S is the sender of data packet, initiates the route discovery process. M1 and M2 are the malicious nodes and the path between them in orange acts as a tunnel. Both A and M1 get the RREQ packet and the route discovery process gets started. Node M1 forwards the packet to M2 and sends it to the sink node. Similarly, sink gets a packet from B tracing the path S-A-B-C .now at the sink node, it appears as if the S-M1-M2 is the shortest route. Consequently the sink chooses this route for route reply and sends the RREP packet to M2. Hence the path S-A-B-C- sink was not even discovered due to the wormhole nodes and their tunnel.

Wormhole attack can be classified into two types-
Based on the fact that whether the wormhole nodes put their identity information into packet header when tunneling and replaying, the wormhole attack [11]can be classified as hidden and exposed attack as follows-

Hidden attack-
In this attack the wormhole node doesn't update the packet header with its own identity(MAC address), before forwarding it. Consequently other nodes are unaware of their existence.

Exposed attack-
In this attack, the wormhole nodes don't alter the contents of packet but add their identity to the packet header. Hence other nodes are aware of such nodes but are unaware of the fact that the former is a malicious node.

IV) PROPOSED WORK

Our objective is to find out the malicious node that performs the wormhole attack in network. We have assumed that the MANET consists of clusters of nodes. The assumptions related to the organization of the MANET are listed below Assumption.

Assumptions

The following assumptions are taken in order to design the proposed algorithm.
1. A node interacts with its 1-hop neighbors directly and with other nodes via intermediate nodes using multi-hop packet forwarding.
2. Every node has a unique id in the network, which is assigned to a new node by existing nodes.
3. The entire network is geographically divided into a few disjoint or overlappingclusters
4. Each cluster is monitored by only one cluster head (monitoring node).

Detection of Malicious Behavior

In AODV routing protocol a malicious nodes can easily disrupt the communication. A malicious node that is not part of any route may launch Denial of Service (DOS) Attack. Also once a route is formed, any node in the route may turn malicious and may cease forwarding packets, alter them before forwarding or may even forward to an incorrect intermediate node. Such malicious performance by a misbehaving node cannot be detected for in pure AODV protocol . During the judgment process the neighbors send their conclusion about a node. When the node collects all conclusion of neighbors, it decides about honesty behavior of reply's sender node. The decision is based on the following cases which are used to judge about honesty of a node.

Steps to judge an honesty node

Case1: If a node delivers many data packets to destinations, it is supposed as an honest node.

Case2: If a node receives many packets but do not sent same data packets, it is probable that the current node is a misbehavior node.

Case3: When the case2 is correct about a node, if the current node has sent any Route REPLY packets; therefore surely the current node is misbehavior node.

Case4: When the case2 is correct about a node, if the current node has not sent any Route REPLY packets; therefore the current node is a failed node.

In this paper, a proactive scheme is proposed to detect the above-mentioned malicious activities. A malicious node flooding the network with fake control packets, such as RREQs (Route Requests) causes congestion in the network. The processing of RREQ by the nodes in the network leads to further degradation in performance of the network. This abnormal behavior is handled in our scheme by ensuring a fair distribution of resources among all contending neighbors. Incoming RREQs are processed only if number of RREQs from the said neighbor is below RREQ ACCEPT LIMIT. This parameter specifies a value that ensures uniform usage of a node's resources by its neighbors. Another threshold RREQ BLACKLIST LIMIT determines whether a node is acting malicious or not. If the number of RREQs goes away from RREQ BLACKLIST LIMIT then the node is blacklisted and all requests from it are blocked temporarily. Thus isolating the malicious node. Tamper of packets by a malicious node in the route can be detected by promiscuous listening by the other nodes that are part of the route. This type of moral policing, done by the nodes, ensures detection of any malicious activity taking place. To facilitate detection, extra information regarding route is exchanged while route formation. To provide security to it, promiscuous listening is proposed during the route formation also. Malicious nodes can easily disable RREQ_RATELIMIT and send out as many RREQ packets as possible. Not much can be done to stop the malicious node from doing this. However, the neighbors of this malicious node can work to control the number of fake RREQ packets that are sent, thus preventing the flood from crossing further hops.

Algorithm to Isolate Malicious Node:

Let L is the maximum limit each node having.
i.e L= RREQ_RATELIMIT
LT= RREQ_ACCEPT_LIMIT
M= RREQ_BLACKLIST_LIMIT
On receiving the RREQ by a neighbor
Increment rreq_count for that neighbor
If rreq_count < LT
Process the RREQ
Else
If rreq_count > M
Black list the specific node and declares it is malicious node
If the node behaves as malicious
Drop the data packets received by the malicious node.
Else
If the rreq_count > L
Ignore all route requests

Explanation of algorithm:

Step 1: Source node sends the RREQ to the next neighbor node. If the route is found sends a RREP to the source node.
Step 2: if the route is established then source node sends data packet to the next node.
Step 3: if the intermediate node is a malicious node it will drop the packets which it receives from the neighbor node.
Step 4: The malicious node may send the fake RREQ to other nodes. So stop fake route request by ignoring the RREQ from the malicious node

V) SIMULATION

NETWORK PARAMETERS CONSIDERED DURING SIMMULATION AND ANALYSIS

Throughput (bits/sec)- It is the measure of number of packets successfully transmitted to the destination per unit of time.

Packet delivery ratio- It is the ratio of number of packets received by the destination to the total no. of packets originated at the application layer of the sender (CBR source).

Total packets received- It specifies the total number of packets received by the destination.

Table 1. Parameter Table

Channel type	**Wireless channel**
Radio propagation model	**Two way propagation**
Interface queue type	**Queue**
Max. packet in ifq	**50**
Routing protocol	**AODV**
Mac type	**802.11**
No. of nodes	**50**
No. of cluster	**5**
Network interface type	**wirelessPHY**
Antenna type	**Omnidirectional**

NEED OF SIMULATON

Since the real systems are not available to us or it may be expensive or infeasible to work with them e.g. space simulations, flight simulations, we simulate the network environment[9] and then analyze it. Simulation quickly evaluates design alternatives (eg: different system configurations) and complex functions.

ABOUT NS2 SIMULATOR

A Network Simulator is a package of tools that simulates the behavior of networks we simulate the MANET behavior using ns2 simulator. Network Animator is a visual aid that enables us to see how packets flow in network from one node to another.
We can make it work using many of the available routing protocols like AODV, DSR, DSDV etc. I used AODV as the routing protocol. We can see the snapshots of nodes, base stations in the simulated network environment.

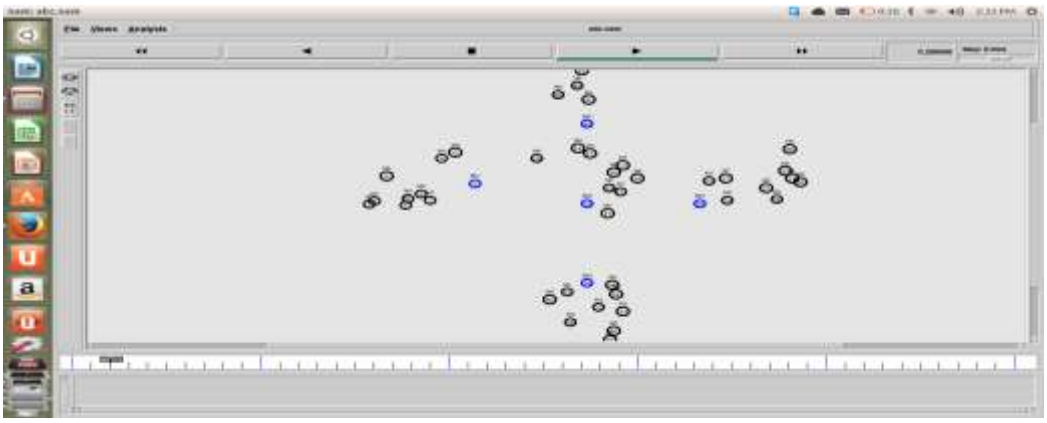

Fig 2.nodes and base stations in simulated network

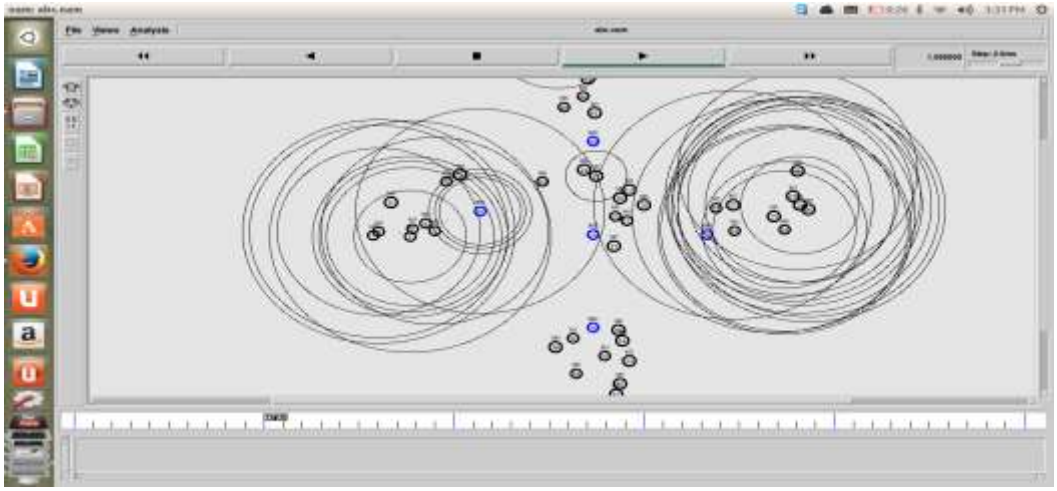

Fig 3. routing in MANET

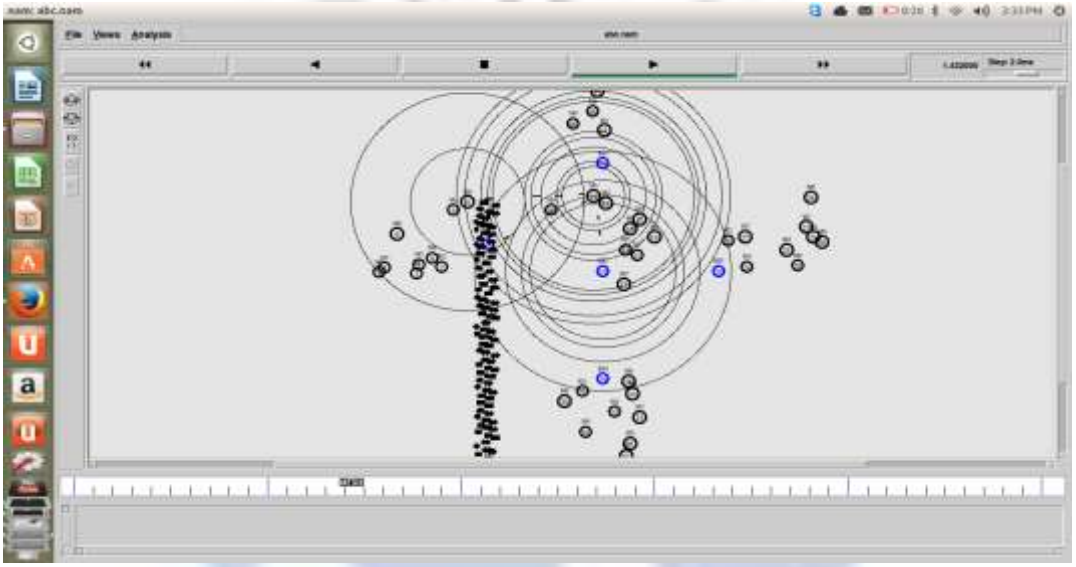

Fig 4. Packet drop in MANET

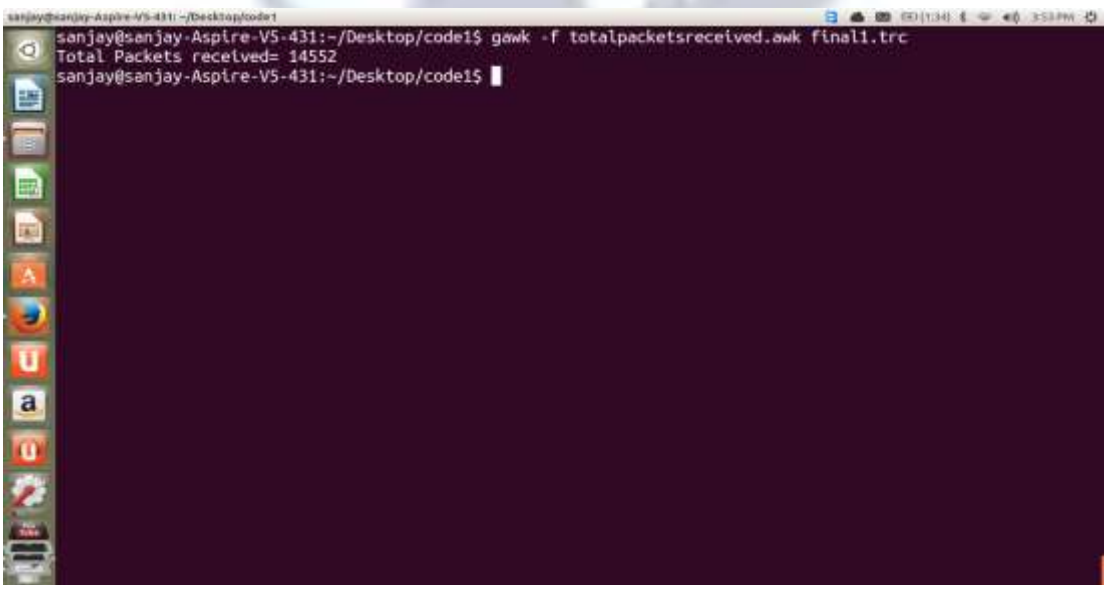

Fig 5. Total packets received

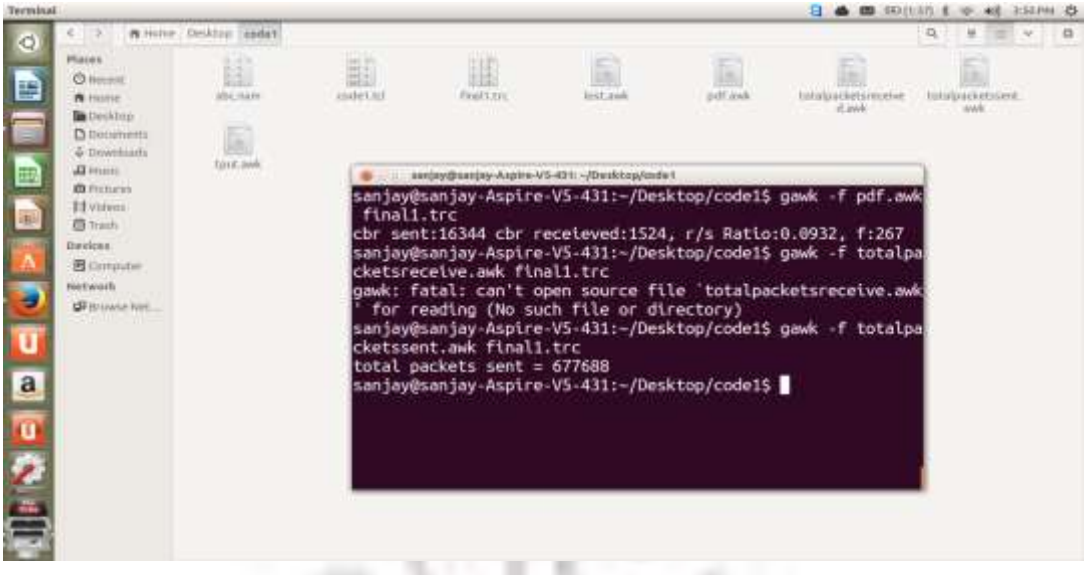

Fig 6. Total packets sent

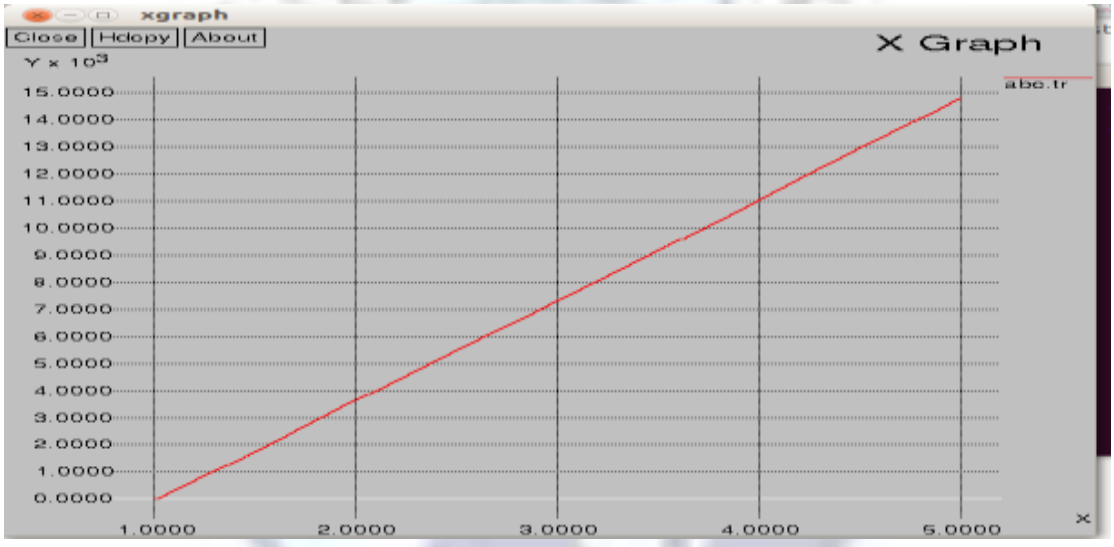

Fig. 7 Packet loss graph

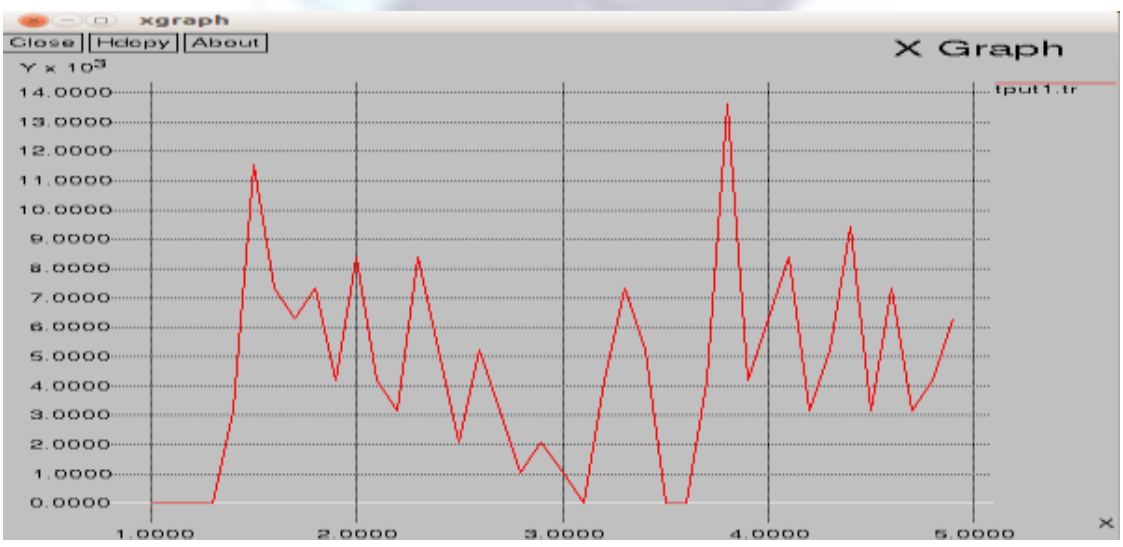

Fig 8 Throughput graph

CONCLUSION AND FUTURE SCOPE

In this paper, we studied about various types of warmhole detection algorithms in MANET and particularly we have proposed a new algorithm for detecting a malicious node and I studied about various types of attacks which MANET is prone to and considered the wormhole attack in particular to see its effect on MANET using AODV as routing protocol. I used ns2.35 network simulator and we can draw following conclusion: Due to the mobility and open media nature of MANET these networks are more prone to security threats as compared to the wired network. I saw that the wormhole attack affects the network performance which can be analysed using various network parameters like total packets sent, total packets received, throughput, packet delivery fraction by the help of simulation and graphs etc. If proper mechanisms are not employed to protect the MANET, most of the ad hoc routing protocols will fail to find the valid routes. In future, this work can be extended by simulating the proposed protocol and comparing the effect of wormhole attack on various routing protocols in MANET. More network parameters can be considered for comparison of performance of various routing protocols under this attack. Further we can consider other possible attacks in MANET and their effect on network.

REFERENCES

[1]. data communications and networking by Behrouz A. Forouzan.
[2]. C. Siva Ram Murthy and B.S. Manoj, "Ad-Hoc wireless networks", Architecture and protocols, Pearson Education, Fourth Impression,2009.
[3]. Piet demeester, Jeroenhoebeke An overview of Mobile Ad hoc Networks : Applications and Challenges http://cwi.unik.no/images/Manet_Overview.pdf.
[4]. http://moment.cs.ucsb.edu/AODV/aodv.html.
[5]. http://en.wikipedia.org/wiki/Ad_hoc_On-Demand_Distance_Vector_Routing.
[6]. C. Perkins, Adhoc on-demand distance vector routing http://www.ietf.org/rfc/rfc3561.txt.
[7]. Wenjia Li and Anupam Joshi Security issues in Mobile Ad-hoc Networks http://www.csee.umbc. edu/~wenjia 1/699_report.pdf.
[8]. Shalinijain, Dr. Satbir Jain Detection and Prevention of wormhole attack in MANET http://www.ijcte.org/papers/120-G224.pdf.
[9]. http://en.wikipedia.org/wiki/Ns_(simulator).
[10]. F. Anjum and P. Mouchtaris, Security for Wireless Ad hoc Networks 1st ed. WileyInterscience,2007.
[11]. http://www.ijarcsse.com/docs/papers/Volume_3/6_June2013/V3I6-0488.pdf.
[12]. http://warse.org/pdfs/ijccn03122012.pdf .