An Implementation of Secure Wireless Network for Avoiding Black hole Attack

Neelima Gupta
Research Scholar,
Department of Computer Science and Engineering
Jagadguru Dattaray College of Technology
Indore, Madhya Pradesh, India

Krishnakant Kishore
Head of Department,
Computer Science and Engineering
JDCT College,
Indore, Madhya Pradesh, India

ABSTRACT

Mobile ad-hoc network (MANET) is a temporary infrastructure less network, Due to absence of infrastructure, MANET is vulnerable to attacks such as Black hole attack, Gray hole attack, wormhole attack, Sybil attack, and Route table modification attack. This research is concerned with "includes a way to produce and implement a simulation based solution, which is based on cluster organization of network approach". The proposed scheme is device specific technique, where individual devices are creating a trust over network and based on these trust values the network cluster heads and monitoring servers deciding malicious activities in network.

Keywords

MANET; MAODV; Cluster Head; security; wireless networks;

1. INTRODUCTION

Mobile ad hoc network is a new generation communication network. That support mobility and wireless connectivity between nodes. Due to mobility the routing protocols are responsible for searching a route between source and destination. In addition of that the routing protocols are also responsible for develop and maintain the topology of network. Due to dynamic nature of network topology any intermediate node between the routing paths can leave or join the network. Therefore most of the attacks are deployed using the routing protocols. In this presented work different routing based attacks are analysed and most frequently deployable attack namely black hole attack is investigated.

Black hole attack is a serious kind of security flaw, where a malicious node advertises self for having the shortest path between source and destination. Therefore, the network traffic is attracted by the malicious attacker and most of the data is lost when the malicious node found a data packet. This results low packet delivery ratio, and high end to end delay. Therefore in this presented work a new node configuration is suggested for developing secure and efficient environment. In this new configuration the network nodes are organized using a hierarchical manner the server node which monitors the traffic of network a cluster head responsible for find the destination nodes in network and the client nodes which making communication between source and destination.

2. OBJECTIVE

The main goal of the paper to find an optimum solution for detecting and preventing the black-hole attack thus the following work is involved in this work.

1. **Study of different routing protocol for MANET:** In this phase different routing protocols are studied by which the working of the routing and their issues are learned.
2. **Study of different security techniques for MANET:** In this phase different routing based security techniques are discussed. These techniques are helps to find the optimum technique for preventing the malicious activity in network.
3. **Implementing a new security scheme:** After studying the literatures about the MANET security and the enhanced routing technique. A new security configuration and network topology development is prepared for MANET. The proposed technique of security is simulated using NS2 network simulator.
4. **Performance study of proposed routing technique:** In this phase the performance of the proposed routing technique and network is investigated during the attack deployment conditions. The performance of the technique is prepared in terms of end to end delay, packet delivery ratio, and throughput.

3. BACKGROUND

In Black hole attack, using routing protocol to an attacker advertises itself as the shortest path to the target device. An attacker watches the routes request in a flooding based routing protocol. When the attacker receives an appeal for a route to the target node, it forms a respond involving of really short route. If the mischievous respond reaches the initiating node before the reply from the genuine node, a fake route gets created. Once the malicious device joins the network itself among the communicating nodes, it is bright to do anything with the packets passing through them. It can crash the packets between them to perform a denial-of-service attack, or on the other hand use its position over the route is the first step of man-in-the-middle attack.

The black hole attack is a well-known security issue in MANET. The intruders develop the loophole to deploy their malicious activities because the route detection process is necessary and predictable. Many researchers have conducted different detection techniques to propose different types of detection schemes.

For example, in Figure 1, source node S wants to send data packets to destination node D and initiates the route detection process. Suppose that device 2 is a malicious device and it claims that it has a route to the destination whenever it receives route request packets, and straight away sends the reaction to node S. If the reply from the malicious node 2 influences firstly to node S, then node S considers that route detection is finished, than S ignores all other replies and starts to send data packets to node 2. As an outcome, all packets through the malicious node is consumed or lost.

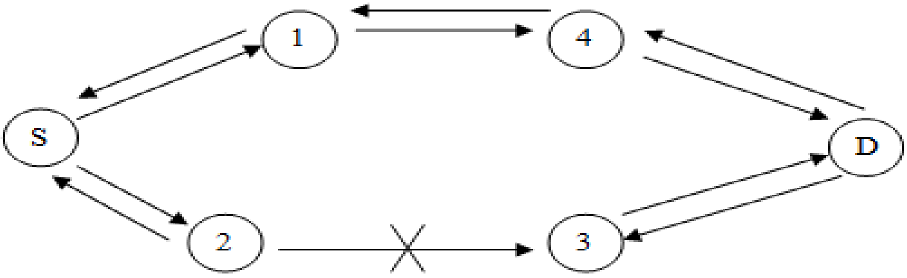


Figure 1- Black Hole Attack

4. PREPOSE SOLUTION

The main goal of the paper to find an optimum solution for detecting and preventing the black-hole attack thus the following work is involved in this work.

1. **Study of different routing protocol for MANET:** In this phase different routing protocols are studied by which the working of the routing and their issues are learned.
2. **Study of different security techniques for MANET:** In this phase different routing based security techniques are discussed. These techniques are helps to find the optimum technique for preventing the malicious activity in network.
3. **Implementing a new security scheme:** After studying the literatures about the MANET security and the enhanced routing technique. A new security configuration and network topology development is prepared for MANET. The proposed technique of security is simulated using NS2 network simulator.
4. **Performance study of proposed routing technique:** In this phase the performance of the proposed routing technique and network is investigated during the attack deployment conditions. The performance of the technique is prepared in terms of end to end delay, packet delivery ratio, and throughput.

4.1 Methodology

The proposed methodology for configuring the network and preventing the black hole attack can be easily understand by the below given figure

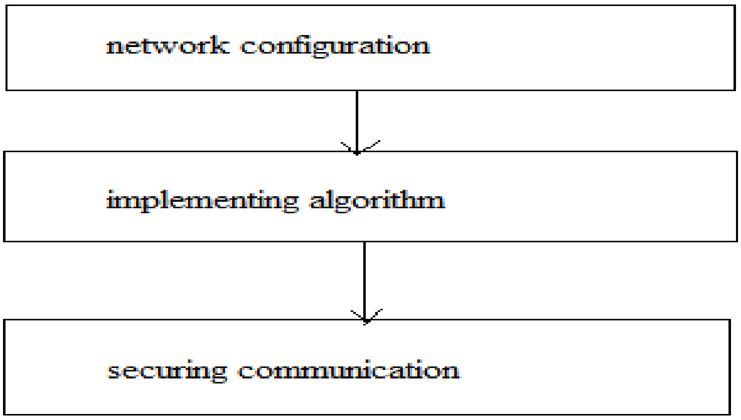


Figure 2- Layered Security

The proposed methodology is based on the three layered architecture of security the detailed description of each layer is given as:

4.1.1 Node Configuration

In first phase the network nodes are categorized in three main classes and their responsibilities are given as:

4.1.1.1 Client Node:

The end client nodes are those who are creating request for transmitting data to a specified node. Therefore in this node configuration the only those nodes are send data which are acting as client node.

4.1.1.2 Cluster Head:

Cluster head is a different kind of device which is used to distribute the service to the end client. According to the clustered organization of network the flow of traffic is always go through the network cluster head. Additionally the cluster head is responsible for searching the target destination for delivering the data. In the given network configuration the cluster head is also responsible for generating a hash key which is used for identifying the client nodes which are under any cluster head. Additionally that is also responsible for preventing the malicious activity in network.

4.1.1.3 Server Node:

Server node keeps the entire networks information, such as the nodes PDR (packet delivery ratio) in addition of that the new network node is only joins when the server node authenticates the newly joined node.

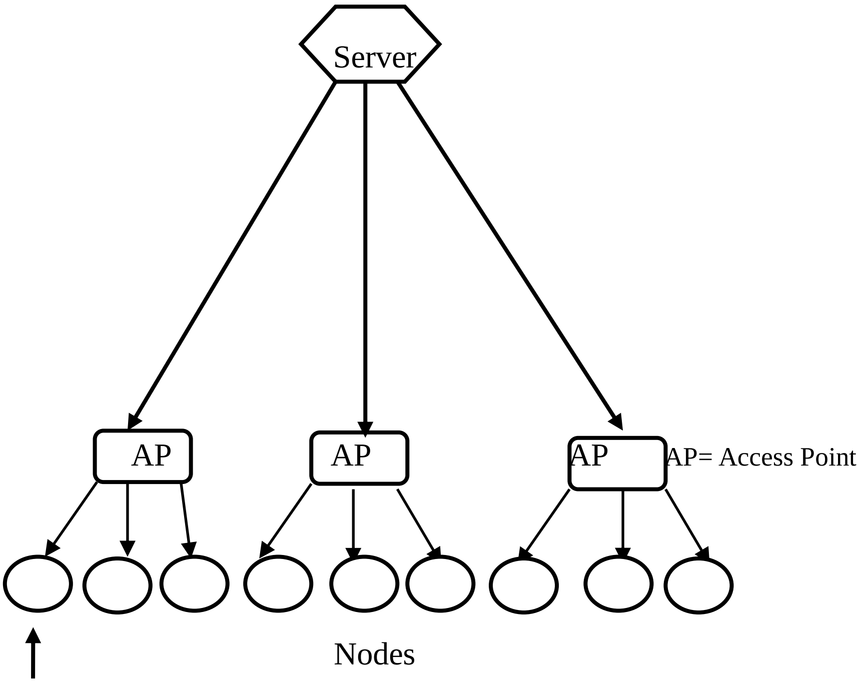


Figure 3- proposed network configuration

4.2 Implementing Algorithm

In this phase the network nodes are active and able to perform the given functionality. Therefore for distributing services the following algorithm works. Suppose the N nodes in network, and there C cluster heads in network for distributing the services. Here a network scenario is presented where a node S wants to send data to the target destination node. the presented algorithm works in the following manner.

```
1. All cluster head generate a Key
2. Broadcast the key to all the nodes under the cluster head
3. if S and D in similar cluster
        a. source S send data to CH (cluster head)
        b. if S.PDR < threshold and S.Key != assigned key
        c. node labelled as malicious
        d. drop the packets
        e. else
        f. CH send data to Destination node D
        g. End if
4. End if
5. If S and D in different cluster
        a. Source S send data to CH (cluster head)
        b. if S.PDR < threshold and S.Key != assigned key
        c. node labelled as malicious
        d. drop the packets
        e. else
        f. CH send data to concerning cluster head CH
        g. CH send data to Destination node D
        h. End if
6. End if
```

5. IMPLEMENTATION AND RESULT ANALYSIS

This section provides the desired network configuration for simulation of security scheme implementation using AODV routing protocol.

Table-1 network setup

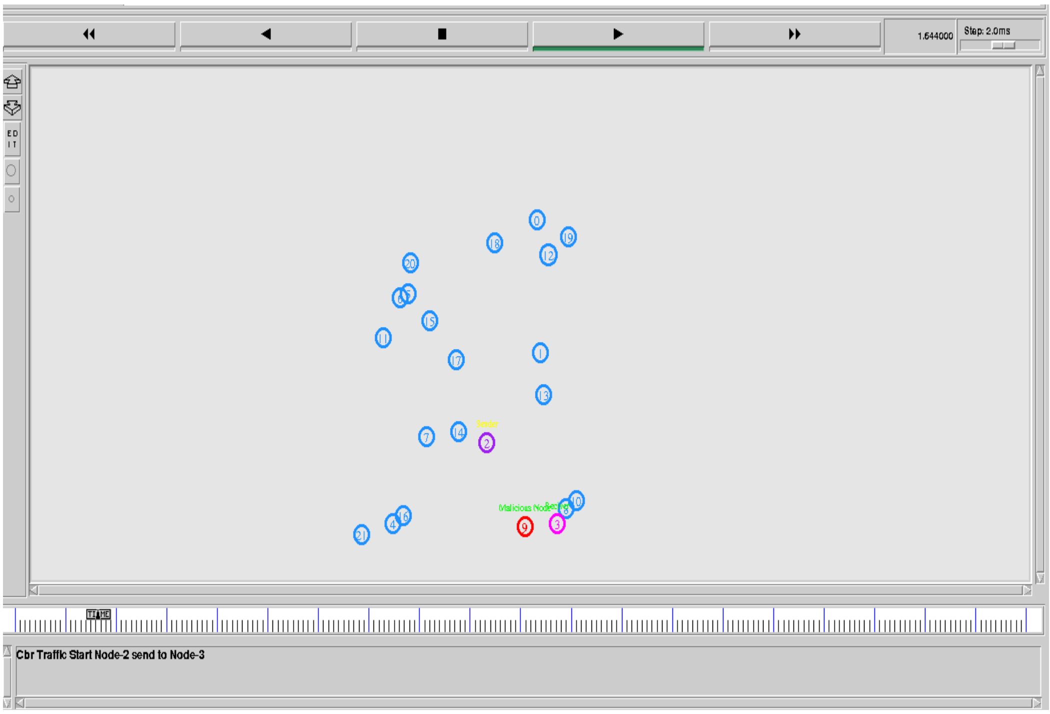
Simulation properties	Values
Antenna model	Omni Antenna
Dimension	750 X 550
Radio-propagation	Two Ray Ground
Channel Type	Wireless Channel
No of Mobile Nodes	15
Routing protocol	AODV
Time of simulation	10.0 Sec.

5.1 Simulation Scenarios

The simulation of the proposed network configuration for preventing the black hole attack is performed in two major scenarios.

5.1.1 Simulation using the traditional ad hoc network:

The traditional network configuration is given using figure 4.1, in this network scenario not any fixed network points are given all the nodes having similar functionality and all the nodes can send and receive the data. using the given network configuration a malicious node is also deployed in the network and performance of network is measured.

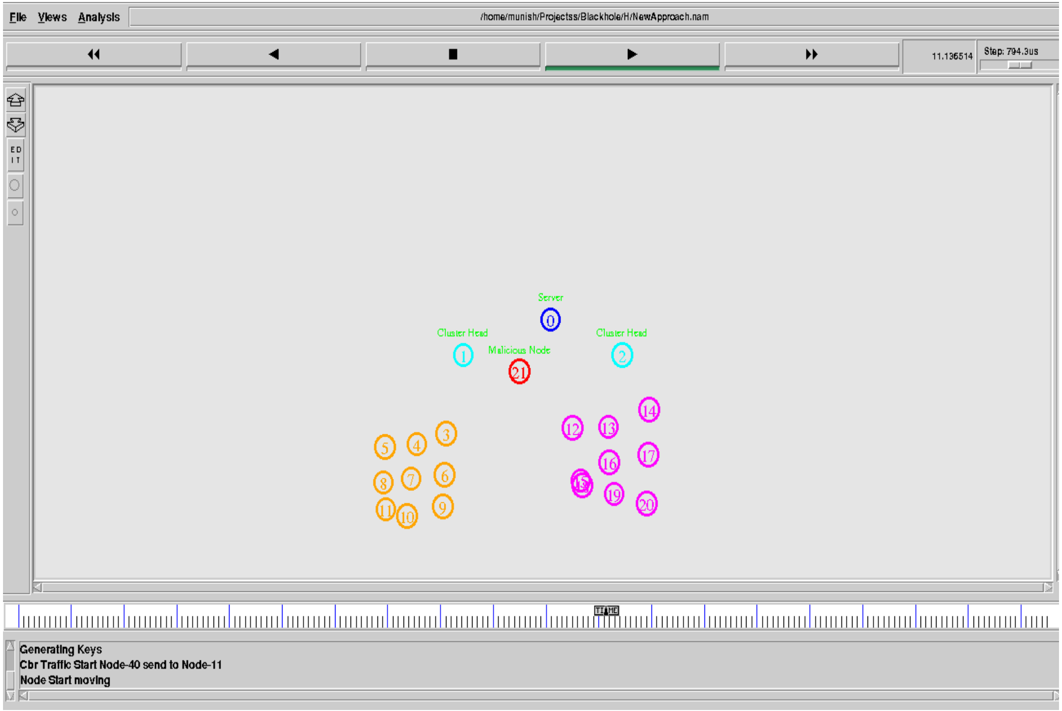


Cbr Traffic Start Node-2 send to Node-3

Figure 4.1 - normal network topology

5.1.2 Simulation using the proposed network topology:

The proposed secure network configuration for preventing the black hole attack is given using figure 4.2.



Generating Keys
Cbr Traffic Start Node-40 send to Node-11
Node Start moving

Figure 4.2 - proposed network topology

In this network topology a server node (using blue node) is presented, in addition of that there are two cluster heads are deployed (using green nodes). The client nodes are represented using orange and pink nodes after configuring the network a malicious node is deployed and presented using red colour node. After deploying the attack on network performance of the network is calculated and compared.

5.2 Experimental Observations

After implementing the desired network configuration the following facts are found.

1. The traditional network initially performs the normal functioning, as the malicious attacker is deployed on network. The performance of network is degraded considerably and the packet delivery becomes too few.
2. The proposed network configuration is acting as the normal and after the attack deployment that also not affected. Additionally the network performance is not affected due to effect of malicious attacker.

The given details demonstrate the obtained results and their analysis for reporting the performance and comparativeness of the techniques.

5.2.1 End to end delay

End to end day on network refers to the time taken for a packet to be transmitted across a network from source to destination device.

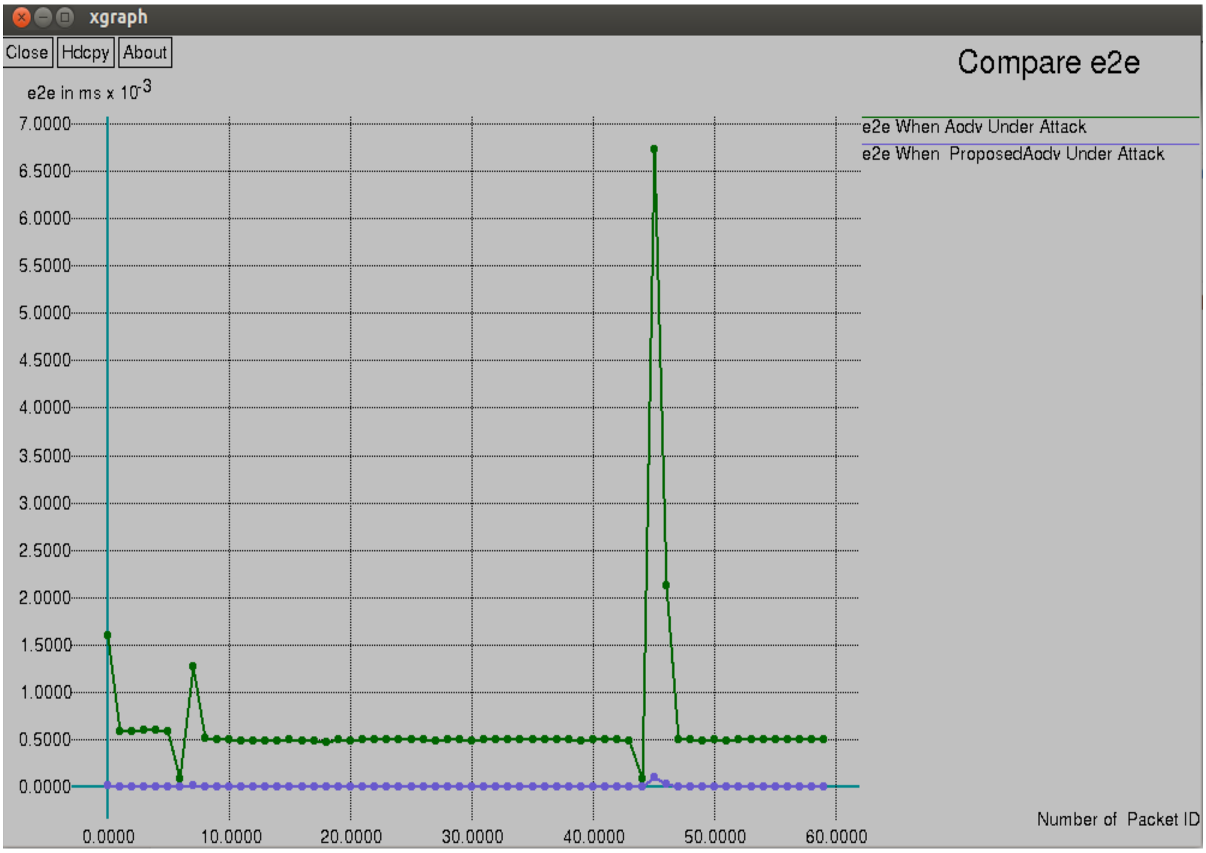


Figure 4.3 - End to end delay

Figure 4.3 shows the obtained performance of the proposed and traditional network performance in terms of end to end delay. In this given diagram the green line shows the end to end delay of AODV routing protocol under attack conditions and the blue line shows the end to end delay of the proposed network configuration. In addition of that the X axis shows the number of packets transmitted during the communication scenarios. And the Y axis represents end to end delay in terms of milliseconds. According to the obtained results the traditional routing protocol having higher end to end delay during attack deployment as compared to the proposed network configuration. Therefore the traditional network is majorly affected by the malicious attacker and the proposed network is not affected by the black hole attack.

5.2.2 Packet delivery ratio

Packet delivery ratio provides information about the performance of any routing protocols, where PDR is estimated using the formula given

$$packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

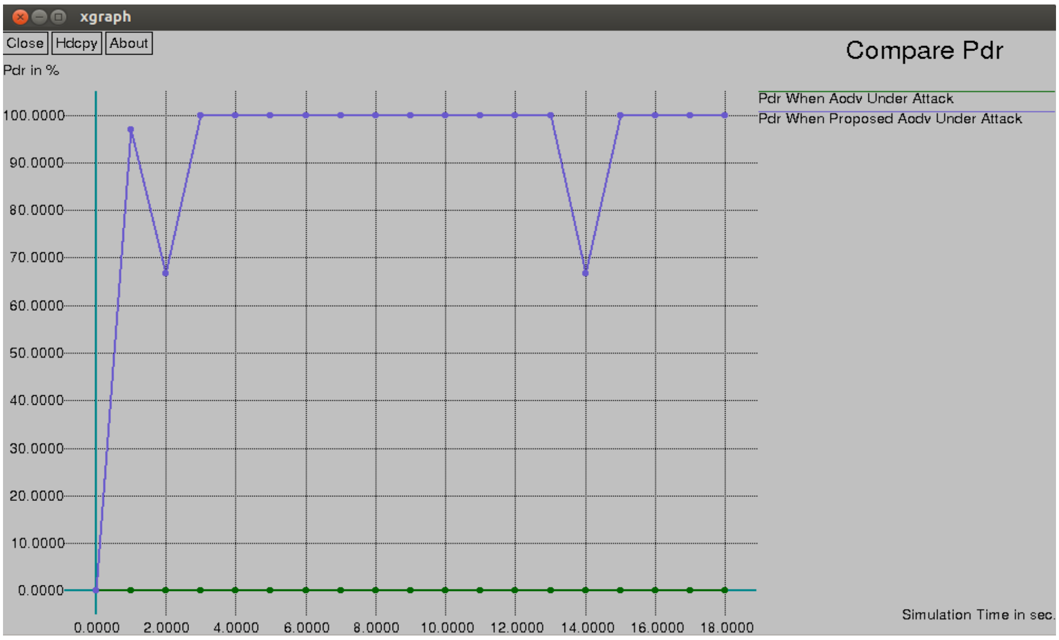


Figure 4.4 - packet delivery ratio

Figure 4.4 shows the packet delivery ratio of the network, in this diagram the green line shows the AODV routing protocol during the attack conditions and the blue line shows the proposed routing protocols performance. Additionally the X axis shows the simulation time and Y axis shows the packet delivery ratio in terms of percentage. According to the obtained results from the simulation the proposed routing protocol shows higher packet delivery ratio as compared to the traditional routing protocol. The blue line shows the higher packet delivery ratio because the network is not affected by the attacker in proposed routing protocol and the traditional routing protocol is not delivery any packet during the attack conditions.

5.2.3 Throughput

Network throughput is the usual rate of successful delivery of a message over a communication medium. This data may be transmit over a physical or logical link, or pass by a certain network node. The throughput is calculated in terms of bit/s or bps, and occasionally in terms of data packets per time slot or data packets per second.

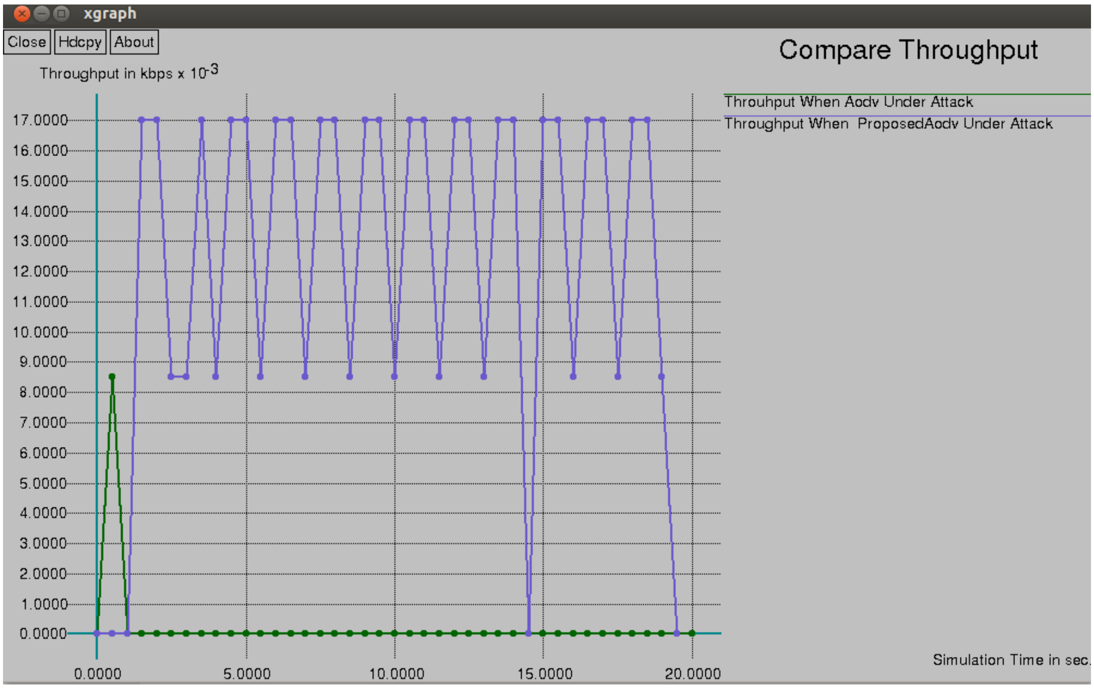


Figure 4.5 - Throughput

The figure 4.5- shows throughput of the traditional and proposed network routing technique. The blue line shows the throughput of the proposed network and the green line shows the AODV routing protocols throughput. According to the given results the X axis shows the simulation time and Y axis shows the obtained throughput during the attack conditions. The obtained results show that the performance of the network in terms of the throughput is much higher than the traditional routing protocol.

6. FINAL CONCLUSION AND FUTURE WORK

This section draws the conclusion of the entire work; finally the future extension of the work is also reported in this section.

6.1 Conclusions

Mobile ad hoc network is mobility based wireless network nodes collection, where not any centralized control is available for regulating the network and their topology. Therefore the network suffers from the uneven connectivity and performance issues. In this network routing algorithms are providing ease in data transmission and topology development and management. But most of the malicious activities are also deployed using the routing techniques. Thus in this paper a new configuration of network and network nodes for preventing the effects of the malicious attacker.

In order to optimize the network performance and routing security a new network topology is prepared. Where a server node performs the monitoring on the devices and the cluster heads are responsible for making the decision of data delivery and the malicious acting node detection. The cluster head nodes are measured the PDR (packet delivery ratio) and a random key for performing the secure communication between two nodes. The implementation of the proposed network routing technique is achieved by modifying the traditional AODV routing protocol. The simulation of the desired network configuration is performed using NS2 (network simulator version 2). After implementation of secure networking scheme the performance of the system is evaluated in terms of packet delivery ratio, throughput and end to end delay.

6.2 Future Work

The proposed secure routing technique is able to provide the efficient results and also able to overcome the routing based attack detection and prevention. Therefore the proposed technique is helpful for improving the network performance in different applications such as securing communication in organizational networks. The proposed scheme is in near future extended through the real world scenarios additionally by considering the additional detection parameters.

7. REFERENCES

[1] Muhammad Raza1 and Syed Irfan Hyder2 in January 2012 (A Forced Routing Information Modification Model for Preventing Black Hole Attacks in Wireless Ad Hoc Network)

[2] E.A.Mary Anita, V.Vasudevan, A.Ashwini in 2010.(A Certificate-Based Scheme to Defend Against Worm Hole Attacks in Multicast Routing Protocols for MANETs)

[3] Sudharson Kumar and Parthipan.V in June 2011.(SOPE: Self-Organized Protocol for Evaluating Trust in MANET using Eigen Trust Algorithm)

[4] U. Venkanna and R Leela Velusami in 2011. (Black Hole Attack and Their Counter Measure Based On Trust Management in Manet.)

[5] Fidel Thachil 1, K C Shet 2 in 2012, A trust based approach for AODV protocol to mitigate black hole attack in MANET.

[6] E.A.Mary Anita\ V.Vasudevan2, A.Ashwini3 in 2010, A Certificate-Based Scheme to Defend Against Worm Hole Attacks in Multicast Routing Protocols for MANETs.

[7] Muhammad Raza1 and Syed Irfan Hyder2 in 9th - 12th January, 2012, A Forced Routing Information Modification Model for Preventing Black Hole Attacks in Wireless Ad Hoc Network

[8] Mehdi Sookhak 1, Mahbubeh Haghparast 2, Abdullah Gani 3 in 2012, Anomaly detection in Geographic Routing Protocols.