The Enhancement of Routing Security in Mobile Ad-hoc Networks

Turkan Ahmed Khaleel
Department of Computer Engineering
Engineering College
Mosul University, Iraq

Manar Younis Ahmed
Department of Computer Science
Sciences & Mathematical College
Mosul University, Iraq

ABSTRACT
In this paper we study the routing security issues of MANETs, we propose an algorithm to detect malicious nodes based on intelligent water drops algorithm and examine "routing modification attack" problem that can easily be exploited against the MANETs. We also propose a solution for this problem and examine security issues related to proactive routing protocols for MANETs. This could be achieved by adding some extensions to secure routing. These extensions include integrity which means that the message will not change along the route and authentication which means that the sender is the one who introduces himself. This protection is provided by a hash chain and authentication by digital signature which both added to all control massages. We obtained acceptable results depending on the performance of metrics(end-to-end delay and network load). The difference in average of end-to-end delay when using secure protocol is very small and the average of network load is also very small.

Key Words
Ad-hoc network; Routing security; Routing attacks; Intelligent water drops.

1. INTRODUCTION
A mobile Ad-hoc network(MANET) consists of a group of wireless mobile nodes that are able of communicating with each other without the use of a network infrastructure or any centralized administration. A MANET are gaining popularity because of availability of mobile devices at low cost and their ability to provide instant functionality of wireless network implementation in which wired network is not possible or valuable[1]. MANET is an emerging research area with applicable applications. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation and security requirement. Routing plays an important role in the security of the entire network. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve.

Currently, two complementary classes of routing protocols MANET exist in the world. Capture demand reactive protocols routes through the floods a "route request" (which usually also records the path to the followed) and receiving a "route reply" (which is commonly indicate the path followed by the request path to reach the destination node); that is, the required parts of the topology graph is built in a node only when necessary for the communication of data traffic. Reactive MANET routing protocols include AODV and DSR. The other class of MANET routing protocols is proactive, i.e. the routing protocol ensures that all nodes at all times have sufficient information to construct topology paths for all destinations in the network. This is achieved through periodic exchange of messages. Proactive MANET routing protocols include OLSR and TBRPF[2].

Today wired computer systems could be made safe at a high level, but when it comes to wireless networks weak security is often used if safety measures are taken at all. This relates to the services running on wireless networks, including MANET routing protocols. While a wireless network is more varied than a wired one, it is also more vulnerable to attack. This is due to the very nature of radio transmissions, which are made on the air. In a wired network, an intruder would need to get in a car or physically intercept a network cable. In a wireless network, an adversary can intercept all messages within the emitting region, operating in promiscuous mode and using a packet sniffer[3].

The main objective of this paper is to discuss Ad-hoc routing security. We limit our study to IP based networks and put a new algorithm for enhancing and protection routing. The rest of this paper is organized as follows. Next section reviews briefly the related works. Attacks against the routing layer in MANET are in section 3, and Intelligent water drops(IWD) Algorithm based on Malicious node detection are in Section 4. Implementing secure protocols in OPNET Modeler are in section 5., and implementing the attack models in the OPNET Modeler are in section 6. Metrics for evaluation are in section 7. Experimental results are in section 8., Section 9 concludes the paper.

2. RELATED WORKS
All Wireless mobile Ad-hoc networks have become a very active field of academic research and industrial applications for their expected size. These networks have no fixed infrastructure. The nodes in Ad-hoc networks are usually limited devices compared to their sources of energy, computer and communication range. They are susceptible to a wide variety of attacks due to the open medium, dynamic changing topology, possible node compromise, difficulty in physical protection, absence of infrastructure, and lack of confidence between the nodes[4].

Routing in Ad-hoc networks has been an active research in recent years, and includes many routing protocols for MANETS. Many different approaches with Ad-hoc routing protocols are proposed to ensure security routing. There are many proposed security protocols, e.g. SAODV[5], SEAD[6], Secure OLSR[7], and Ariadne(Hu et.al., 2005) due to the unpredictable behavior of remote hosts and the lack of protection of the hardware, these protocols are still vulnerable to many attacks. The main drawback of all the above approaches is that all of them require clock synchronization.

3. ROUTING ATTACKS IN MANET

All of the routing protocols in MANET depend on active cooperation of nodes to provide routing between the nodes and to establish and operate the network. The basic acquisition in such a setup is that all nodes are well behaving and authentic. Due to dynamic, distributed infrastructure, less nature of MANET and need of centralized authority, the Ad-hoc networks are vulnerable to various kinds of attacks. The challenges to be faced by MANET are over and above to those to be faced by the traditional wireless networks. The accessibility of the wireless channel to both the genuine user and attacker make the MANET susceptible to both passive eavesdroppers as well as active malicious attackers[9].

The attacks on MANET can be classified as active or passive. In passive attacks the attacker does not send any message, but just listens to the channel. Passive attacks are non disruptive but are information seeking, which may be critical in the operation of a protocol. Active attacks may either be directed to break the normal operation of a specific node or target the operation of the whole network.

These attacks may have the aim of modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. An attack may also aim at impeding the formation of the network, making legitimate nodes store incorrect routes, and more generally at perturbing the network topology. Attacks at the routing level can be classified into two primary categories: incorrect traffic generation and incorrect traffic relaying[3].

3.1 Incorrect Traffic Generation

This includes attacks that consist of false communication messages sent with the identity of another node (identity spoofing). The consequences are a possible action of information in different parts of the network, communications degradation and unreachable nodes.

An adversary can either action a Denial of Service by saturating the support with a large amount of broadcast messages, reducing the rate of knots and, at worst, preventing them from communicating[10]. One way in which a node can misbehave is by generating control messages in a way that is not according to the protocol. As Shown in Fig.1, a misbehaving node X may send HELLO messages with a spoofed originator address set to that of node C. Subsequently, nodes A and B may announce reachability to C through their HELLO and TC messages. Furthermore, node X chooses MPRs from among its neighbors, signaling this selection while pretending to have the identity of node C . Therefore, the chosen Multi Point Relays will advertise in their Topology Control messages that they provide a last hop to C . Conflicting routes to node C , with possible connectivity loss, may result from this act.

3.2 Incorrect Traffic Relaying

Communications from authorized nodes can be infected by malicious nodes. A node opponent can avoid relaying the messages it receives in the end and reduce the amount of information available to other nodes. This was called black hole attack. And this is a simple way to perform a DOS. This attack can be performed on all or a portion of the received packets, making it unavailable or difficult to arrive the destination node[10].

Fig.2 shows how black hole problem arises, here node “A” want to send data packets to node “D” and initiate the route discovery process. So if node “C” is a malicious node then it will demand that it has active route to the specified destination as soon as it receives route request packets. It will then send the response to node “A” before any other node. In this way node “A” will think that this is the active route and thus active route discovery is complete. Node “A” will ignore all other replies and will start sending data packets to node “C”. In this way all the data packet will be exhausted or lost. In this paper we propose a solution for the routing modification attack problem for Ad-hoc networks.

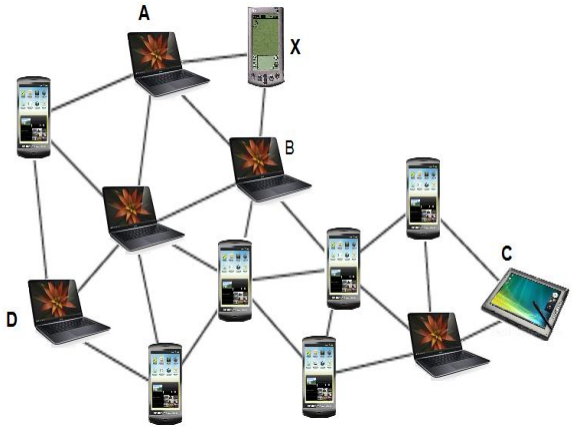

Fig.1: Node X sends HELLO messages pretending to be C.

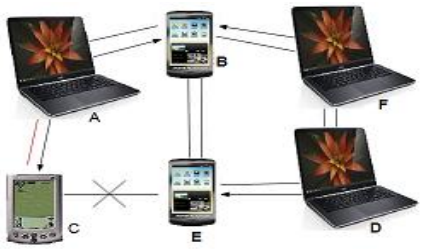

Fig.2: Black Hole Problem

4. IWD ALGORITHM BASED ON MALICIOUS NODE DETECTION

In an Ad-hoc network, from the point of view of a routing protocol, there are two kinds of messages: the routing messages and the data messages. Both have a different nature and different security needs. Data messages are point-to-point and can be protected with any point-to-point security system (such like IPSec). On the other hand, routing messages are sent to immediate neighbors, processed, possibly modified, and resent. Moreover, as a result of the processing of the routing message, a node might modify its routing table. This creates the need for the intermediate nodes to be able to authenticate the information contained in the routing messages (a need that does not exist in point-to-point communications) to be able to apply their imported authorization policy.

When discussing network security in general, three important aspects need to be considered: security requirements, security attacks and security mechanisms. Security requirements

include the functionality necessary to provide a secure networking environment, while security attacks cover the methods that could be employed to break these requirements. Security mechanisms are the fundamental structure blocks used to provide and apply the security requirements[11].

At first we need techniques to intrusion detection techniques and there are many of them mimic what nature. In this research we used intelligent water drops to detect the malicious nodes in MANET. Intelligent water drops algorithm (IWD) was introduced in 2007 by Shah Hosseini is based on optimization approach. The algorithm is natural inspired and mimics the behaviour of an action of water drops and soils of the riverbed [12].

This algorithm has been used because it is based on acceptable performance even in the worst environmental conditions, it is based on relative comparison of errors. The distance-error values of neighbour beacons are compared to find the probability of trustworthiness or goodness of a node. IWD algorithm incorporates the method of natural water drops to the select the next location. Velocity of an IWD increases inversely to soil between its current and next location so the drop will gain velocity on the path with low soil. IWD prefers the path with low soil, so the probability of selecting a path with low soil is higher. Probability of selecting a next node by IWD is calculated by the following equation:

$$p_i^{IWD_{(j)}} = \frac{f(soil(i,j))}{\sum_{k \notin vc(IWD)}^{n} f(soil(i,k))} \quad (1)$$

This formula has been applied by[13] to detect malicious beacon nodes for secure localization in wireless sensor.The following is the steps of IWD algorithm[14] that is used in this research detect malicious node in MANET:

Algorithm1. *IWD based on Malicious node detection*

BEGIN

Step1. static and dynamic Parameters initialization.

Step2. Put all IWDs on the first node.

Step3. Update the velocity of the IWD.

Step4. Select an edge to reach to the next node.

Step5. Compute the amount of soil (Δsoil) which is gathered by the IWD.

Step 6. Update the edge soil and the IWD soil.

Step7. IF Have all IWDs completed their solutions

THEN GOTO step 8 ELSE GOTO Step 4.

Step 8. Find the elitist IWDs.

Step 9. Perform the local search on elitist IWDs.

Step 10. Update the global best solution.

Step 11. IF all Elitist IWDs produce the same results THEN GOTO Step 2.
ELSE Return the global best.

END

5. IMPLEMENTING SECURE PROTOCOLS IN OPNET MODELER

In general, the wanted security for the routing mechanism regards integrity (fewer often non-repudiation) and availability of service. Hence, when talking about protecting routing control messages, we mostly analyze how to generate and verify digests or digital signatures. Encryption is often left aside, because it is more time- and power-consuming, and because confidentiality is not commonly required, as routing information is not secret. (However, this is not always accurate. In the case of military applications, routing information may be tactical information of basic importance; for example, could help enemies identify and locate their targets on a battlefield.)

In this research, we have implemented secure routing, in the OPNET Modeler simulation environment, using the Application Programming Interface functions of the OPNET development kit and the embedded C language. The malicious feature of a wireless node is integrated into the routing protocol model, so that each wireless node can be easily switched back and forth between the normal mode and the malicious mode.

We can use the C/C++ language to implement/modify the behavior of a module. For easy development, OPNET provides quite a large library. Fig.3 shows steps to add new secure features into proactive routing protocols into the OPNET Modeler.

Add security features into new routing is further represented in Fig.4. At the origin nodes that generate the routing packets, the security fields are added into the routing packets at the packet creation phase of the routing process as shown in Fig.5. These security fields will be verified against the secure conditions at the intermediate nodes and at the destination node. If the security conditions are not met, the nodes will discard the routing packets; otherwise they accept the packets and proceed to next appropriate processing phase. These conditions are defined by each specific protocol and added at the processing phase of the routing process.

6. IMPLEMENTING THE ATTACK MODELS IN THE OPNET MODELER

In the simulation, the attack models are implemented as part of the routing process. Fig.5 illustrates how attack models are integrated into the routing processes. Each wireless node, during the routing process, will check if itself is a malicious node. If it is, it will turn on the appropriate attacking process; otherwise, it will process the routing packets as a normal node[15]. The following is the steps of algorithms that are used in this research to secure routing:

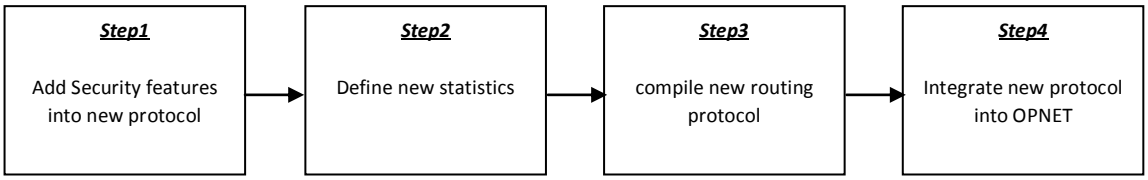

Fig.3: Steps to add new secure routing protocols into OPNET

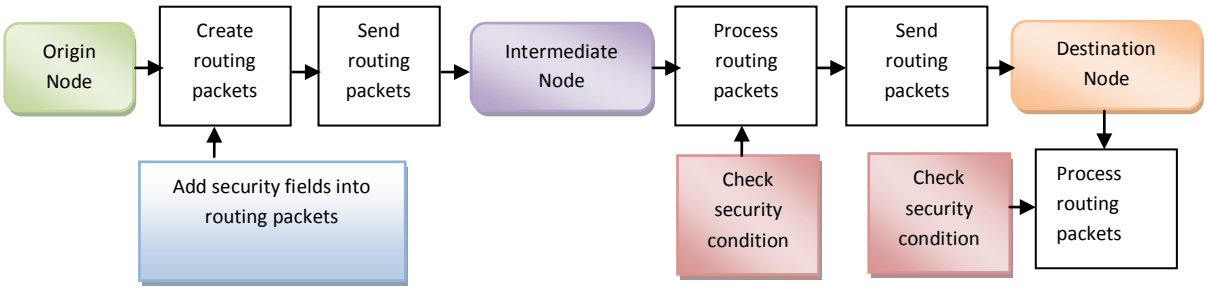

Fig.4: Procedure to add security features into existing protocols in OPNET

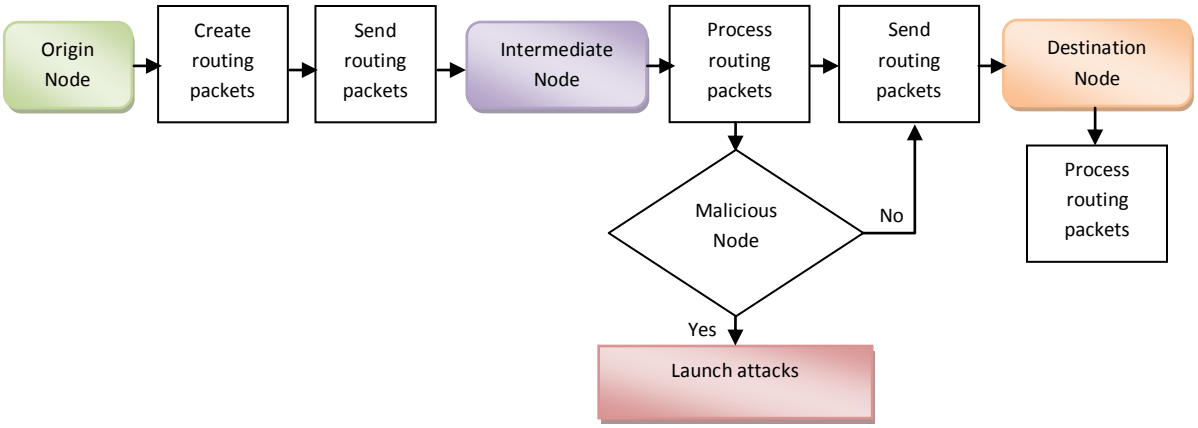

Fig.5: Procedure to integrate attack models in the routing process

Algorithm2. *Calculate Security Value for each message*

Begin

Step1. Initialize hash chain.

Step2. Generate hash chain.

Step3. Max hop count.

Step4. Define hash function type.

Step5. Generate hash based on Source address.

Step6. Extract public key.

Step7. Generate signature.

End

Algorithm3. *Check signature integrity and verify the hop count*

Begin

Step1. IF the signature is invalid
THEN simply drop the packet.
ELSE signature verified.

Step2. IF verify hop count is invalid
THEN destroy the packet
ELSE recalculate hash field

End

7. METRICS FOR EVALUATION

The following metrics were used for performance evaluation:

7.1 Average End-to-end Delay (AED)

This is defined as the average delay in transmission of a packet between two nodes and is calculated as follows:

$$AED = \frac{\sum_{i=0}^{n} (time\ Packet\ \mathrm{Re}ceived_i - time\ Packet\ Sent_i)}{totalNumber\ of\ Packet\ \mathrm{Re}ceived} \quad (2)$$

A higher value of end-to-end delay means that the network is congested and thus the routing protocol doesn't perform well. The upper bound on the values of end-to-end delay is determined by the application. For example multimedia traffic such as audio and video cannot tolerate very high values of end-to-end delay when compared to FTP traffic[15].

7.2 Network Load

Network load represents the total load in bit/sec submitted to wireless LAN layers by all higher layers in all WLAN nodes of the network. When there is many traffic coming on the network, and it is difficult for the network to hold all this traffic so it is called the network load. The efficient network can easily act with large traffic coming in, and to make a best network, many techniques have been introduced. High network load affects the MANET routing packets and slow consume the delivery of packets for reaching to the channel, and it results in increasing the collisions of these control packets. Thus, routing packets may be slow to be stabe.

8. EXPERIMENTAL RESULTS

In this paper, we set up a network with 36 wireless nodes moving at random, each with various speed between 1 and 10 meters per second, which is the average speed of a walking person or a running vehicle. This is a medium group that represents some of the typical scenarios, such as a rescue team working in a disastrous area, a group of moving vehicles in the city, a squad of soldiers or armored vehicles in an army operation, or a place of an event. The *pause time* values represent the movement of the objects. Each of the objects can move at a random direction, stop for some time (per the *pause time*), and then change its direction at random and move again. The *traffic pattern* models the voice data transferred from one node to the other. The simulation scenario is summarized by table(1) as shown below.

To create the malicious environments, an *Intermediate_node12* and *Intermediate_node33* are selected to launch the *Route Modification attacks*. The main characteristics of the malicious environments include the route modification attack. Our simulated results are provided in Fig.6 which displays malicious environment; the source node wants to send traffic data(voice) to destination node. The intermediate nodes transmit traffic data(voice) until reached destination node. If we assume that two of intermediate node are attacks (intermediate node12 and intermediate node33) have been receiving the traffic data and either incorrect traffic generation or incorrect traffic replaying. This is one of the security challenges faced by the MANET protocols like; OLSR. There are many researches in the field of security and security issues in MANET routing protocols, but all suffer from the overhead. In this research we enhance security by added security fields(signature, public key, hash) to all routing messages and messages authentication and integrity checking function are included. Fig.7 gives the variation in network nodes while under *Route Modification attack* after adding security mechanism. Note that attacks were detected and isolated from the network.

Table 1: Simulation Parameters

Examined protocols	OLSR and IWD
Simulation time	1 hour
Simulation area (meters)	4000m x 4000m
Number of Nodes	36 Wireless Mobile nodes(1Source node, 1 Destination node, 2 Hacker node and 32 Intermediate nodes)
Application traffic	Voice
Performance Parameter	Delay, Network Load
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint
Node speed	1-10 m/second

To evaluate the behavior of simulated intrusion based *Route Modification attack*, we consider the performance metrics of packet end-to-end delay and network load. For packet end-to-end delay we carry out two different simulations(one for OLSR routing protocols without adding security mechanism and IWD proactive routing protocols with adding security mechanism). The behavior of attack (*Route Modification*) also depends on protocols as shown in table(2). Fig.8 shows the Voice Packet End-to-End Delay (sec) for OLSR and IWD in case of 36 nodes. This result is carried out when *Route Modification* attacks are introduced and the graph is compared with the normal working protocol so as to observe the effect of attack on the whole network. The graph show higher delay when there is no malicious node present in the network.

Table 2: Global Statistics (Average)

Scenario 1: MANET_Voice	
Voice Packet End-to-End Delay (sec)	
IWD	OLSR
0.12426	0.1396
Wireless LAN Network Load (bits/sec)	
IWD	OLSR
266,665	279,604

Table 2 and Fig.8 show that the difference in the average end-to-end delay is very small and this is due to the security mechanism that used to achieve the authentication and integrity computation times. When measuring the network load as shown in Table 2 and Fig.9 we get small network load especially when using the IWD protocol. This means that the network is stable and not affected with routing modification attack.

9. CONCLUSION

In this paper, an overview of the security problems in wireless networks has been presented, focusing on the routing protocols in mobile Ad-hoc networks and contributing with proposing an enhancement of routing security to both reactive and proactive routing protocols. We added a digital signature to the control traffic which is mainly used to prevent the injection of incorrect information in the network. For each control message generated, corresponding signature is used by a receiving node to authenticate the corresponding routing control message and every message without a matching, corresponding signature is dropped.

In this research, we have implemented secure routing, in the OPNET Modeler simulation and created the malicious environments to launch the *Route Modification attacks*. We concluded that by adding a digital signature to all control messages we could guarantee message authentication or integrity and protection to this type of attack. We also obtained good results depending on the performance metrics(end-to-end delay and network load). The difference in average of end-to-end delay when using secure protocol is very small and the average of network load is also very small.

10. REFERENCES

[1] Shandilya S. K. and Sahu S.,2010. A Trust Based Security Scheme for RREQ Flooding Attack in MANET, *International Journal of Computer Applications (0975 – 8887),Vol. 5, No.12, pp. 4-8.*

[2] Adjih C., Clausen T., Laouiti A., Muhlethaler P., and Raffo D., 2005. Securing The OLSR Routing Protocol With Or Without Compromised Nodes In The Network, National Institute For Research In Computer Science And Control, No. 5494, pp.1-55.

[3] Raffo D., 2005. Security Schemes for the OLSR Protocol for Ad Hoc Networks, PhD. thesis, Université Paris 6, INRIA Thesis Director,version 1– 18.pp40-51.

[4] Imani M., Taheri M. and Naderi M., 2010. Security enhanced routing protocol for Ad-hoc networks, Journal of Convergence, Future Technology Research Association International, Vol. 1, No. 1, pp.43-48.

[5] Zapata M. G., 2001. Secure Ad hoc On-Demand Distance Vector Routing, Mobile Computing and Communications Review, Vol. 6, No. 3,pp. 106-107.

[6] Hu Y. C., Johnson D. B., and Perrig A. , 2002. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad-hoc Networks, Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp 3-13.

[7] Hafslund A., Tønnesen A., Rotvik R. B., Andersson J., and Kure Ø., 2004. Secure Extension to the OLSR protocol", OLSR Interop and Workshop, pp.1-4.

[8] Hu Y.C., Perrig A., and Johnson D.B., 2005. Ariadne: a secure on-demand routing protocol for Ad-hoc networks, Wireless Networks, Vol. 11, No.1–2, pp. 21-38.

[9] Agrawal S., Jain S., and Sharma S., 2011. A Survey Of Routing Attacks And Security

[10] Erritali M. and Reda O. M. and Ouahidi B. E., 2011. A Contribution To Secure The Routing Protocol "Greedy Perimeter Stateless Routing" Using A Symmetric Signature based, International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.5, pp. 95-103.

[11] Sadasivam K., 2005. Performance And Security In Mobile Ad Hoc Networks, M.Sc. thesis,University of Houston-Clear Lake, pp. 45-64.

[12] Hosseini H. S.,2009. "The Intelligent Water Drops Algorithm: A Nature-Inspired Swarm-Based Optimization Algorithm", *INT. J. Bio-Inspired Computation, Vol. 1, Nos. 1/2, pp.* 71-79.

[13] Qureshi S., Asar A., Rehman A., and Baseer A.,2011. Swarm Intelligence based Detection of Malicious Beacon Node for Secure Localization in Wireless Sensor Networks, Journal of Emerging Trends in Engineering and Applied Sciences (JETEAS) ,vol. 2, No. 4,pp. 664-672.

[14] Noferesti S. and Shah-Hosseini H. ,2012. A Hybrid Algorithm for Solving Steiner Tree Problem, International Journal of Computer Applications, Vol.41, No.5,pp. 14-20.

[15] Nguyen T. A., 2006. Evaluations Of Secure MANET Routing Protocols In Malicious Environments, M.Sc. thesis, University of Houston Clear Lake, pp.12-17.

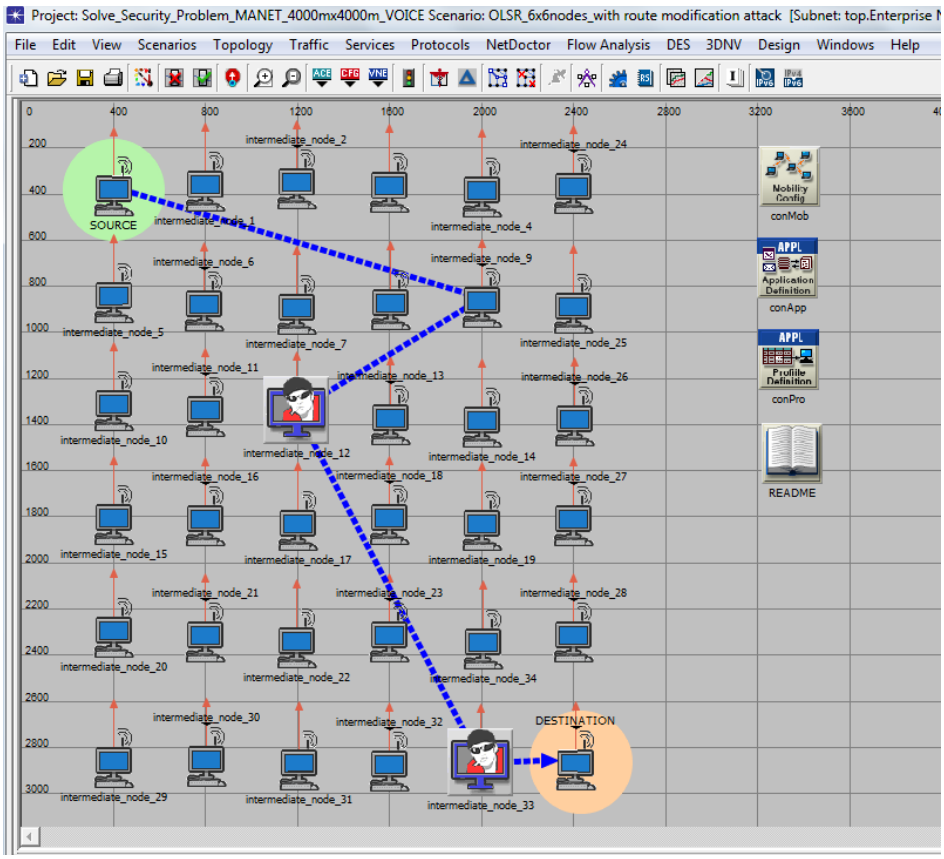

Fig.6: Network setup for the experiments before added security

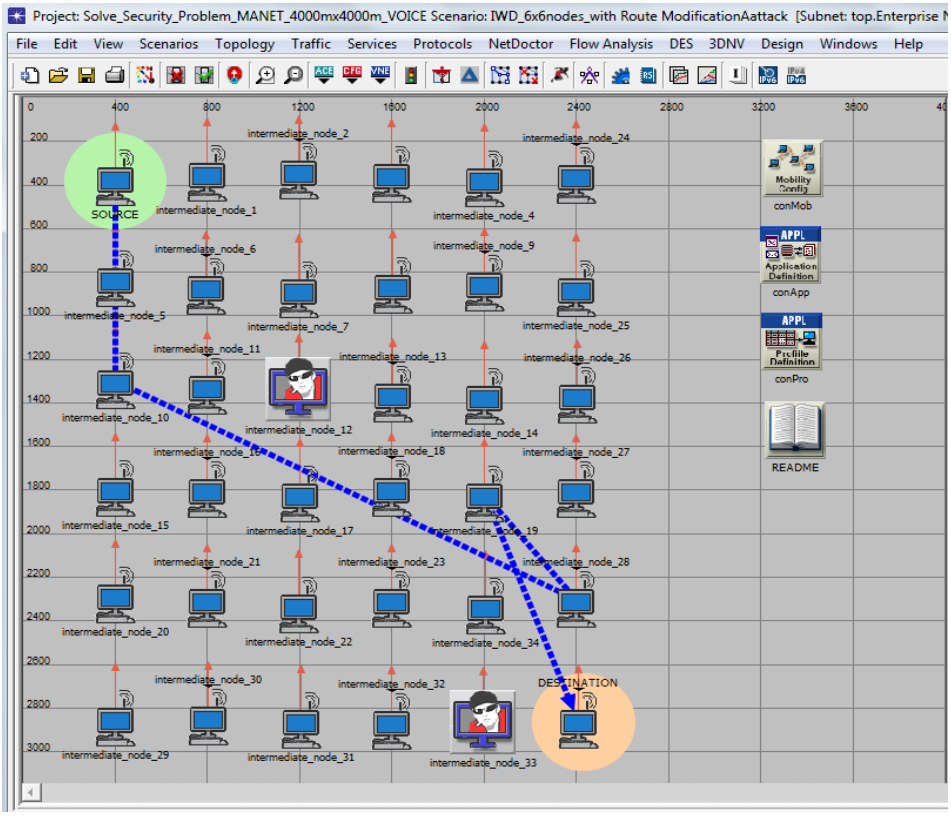

Fig.7: Network setup for the experiments after added security

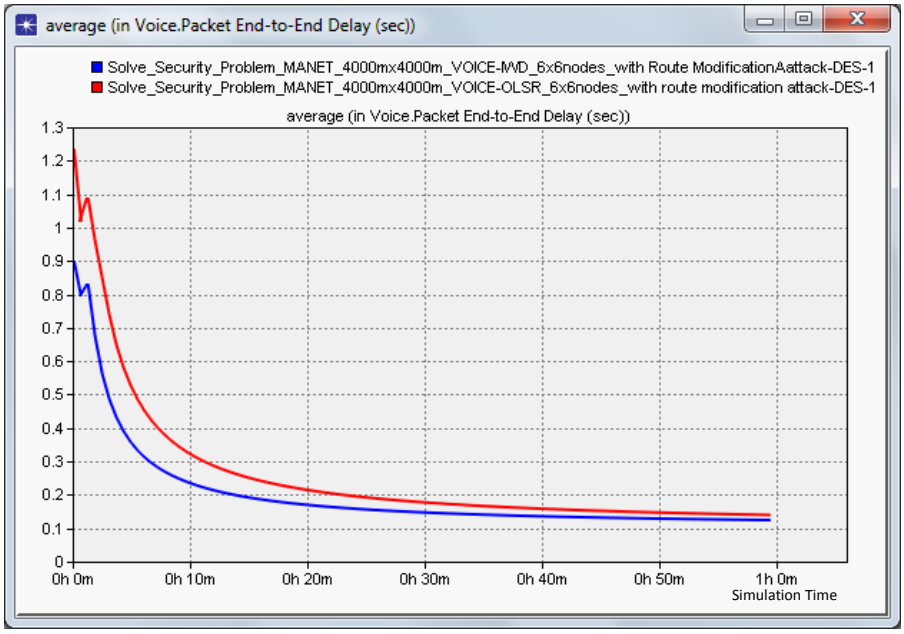

Fig.8 : Voice Packet End-to-End Delay(sec)

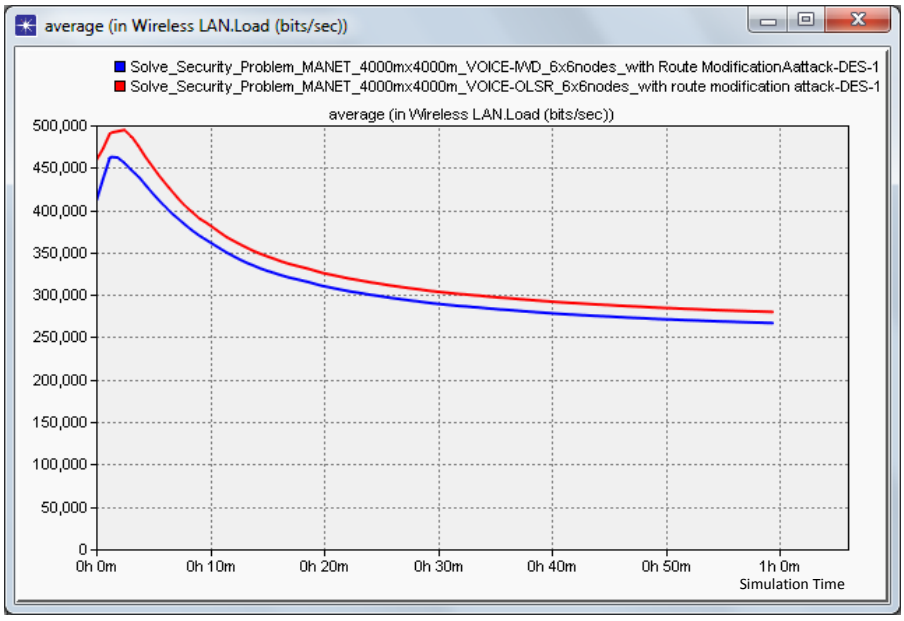

Fig.9: Wireless LAN Network Load (bits/sec)