RESEARCH ARTICLE OPEN ACCESS

A Mechanism to Detect the Provenance Forgery and Packet Drop Attack in Wireless Sensor Networks

Amandeep Kaur, Sandeep Singh Kang
Department of Computer Science and Engineering
Global Institute of Management & Emerging Technologies
Amritsar, Punjab
India

ABSTRACT

WSNs are quickly gaining attractiveness due to low cost solutions to a selection of real world challenges. The vital plan of sensor network is to separate minute sensing devices, which are proficient of sensing some changes of occurrences/ parameters and communicating with extra devices over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring, etc. Sensor can monitor humidity, temperature, pressure, vehicular movement, lightning conditions, mechanical stress levels on attached objects and other properties. This research is based on detecting provenance forgery and packet drop attack. WSN is opened and vulnerable network. So chances of attack are always there. This research deals in discovery of such activity by detecting the malicious node and removing it from the network. Key distribution method is followed to establish a new path. This path will be secured and helpful in reducing delay and packet loss. This research shows that the throughput and stability of network will increased after implementing key distribution technique.

Keywords:- Wireless Sensor Networks, Attacks, Security, AODV, Throughput, Packet loss, Delay

I. INTRODUCTION

Wireless sensor networks are network of thousand of sensor nodes. Sensor nodes are small in size, less memory space, cheaper in price with restricted energy source and limited processing capability. WSNs are rapidly gaining popularity due to low cost solutions to a variety of real world challenges. The basic idea of sensor network is to disperse tiny sensing devices, which are capable of sensing some changes of incidents/ parameters and communicating with other devices over a specific geographic area for some specific purposes like surveillance, environmental monitoring, target tracking etc. Sensor can monitor pressure, humidity, temperature, vehicular movement, lightning conditions, mechanical stress levels on attached objects and other properties. Due to the lack of data storage and power sensor networks introduce severe resource constraints. These are the obstacles to the implementation of traditional computer security techniques in a WSN. Security defenses harder in WSN due to the unreliable communication channel and unattended operation. As a result these networks require some unique security policies. Cryptography, steganography and other basics of network security and their applicability can be used to address the critical security issues in WSN. Many researchers have begun to address of maximizing the processing capabilities and energy saving of sensor nodes with securing them against attackers.

II. TYPES OF WIRELESS OPERATING MODES

A. Infrastructure Networks

In infrastructure predicated network, communication is takes place only between the wireless nodes and the access points. The communication is not established between the wireless nodes. Here the access point is utilized to command the medium access as well as it acts as the bridge to the wireless and wired networks. In this network, fine-tuned base stations are utilized when the node goes out of the range of base station another base station come into range. The example of infrastructure deployed network is cellular networks system. It is centralized dominance device like router or Master System [1]. The major problem which occurs in this system is that if controller fails all the systemlink to it will go down or crash.

B. Infrastructure less Networks (Wireless Ad-hoc Network)

The infrastructure less network does not require any infrastructure to for communication. In this network each host can transmit data to wireless node and it does not access point or controlling medium access. Infrastructures less networks do not have routers that are fine-tuned. In this network all the nodes need to act as routers and all nodes are capable of kineticism and can be connected dynamically in an arbitrary manner. All the contrivances in infrastructure less network are wirelessly communicated to each other. The specialty of this network is that it has fileserver encompass core station of Wi-Max which controls pool of access point with in 6 kms rage. Utilizing Wi-Max base station and access points communicating and utilizing Wi-Fi utilizer and access points communicating [5].

III. WIRELESS AD HOC NETWORKS

Wireless Ad-hoc Network comes under the category of infrastructure less networks. Ad-hoc wireless network is collection of many devices equipped with wireless communications and networking capabilities. Ad-hoc network is decentralized with no pre-subsisting infrastructure such as routers in wired networks or access points in wireless networks on which it is depended. In routing each node participates by forwarding data for other nodes in ad hoc network the resoluteness of which nodes forward data is made dynamically on the substratum of network connectivity.

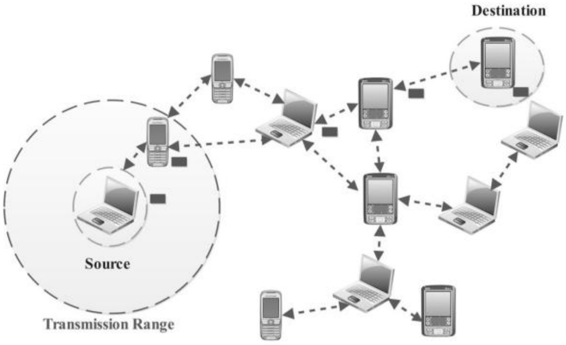


Figure 1- Wireless Ad-hoc Network [15]

Ad-hoc network is a wireless, self-organizing and rapidly deployable network in which neither a wired backbone nor a centralized control exists. The nodes are often energy constrained i.e. battery powered devices with great diversity in their capabilities.

IV. CHARACTERISTICS OF WIRELESS AD-HOC NETWORKS

There are some characteristics which define strength of Wireless Ad-hoc Network [7]:

Dynamic Topology

For this any node can be frequent change so any random or dynamic topology required establishing communication.

Multihop Routing

In Ad-Hoc multi-hop routing is very important factor, Becsause one node want to broadcast its packet information to destiantion nodebeyond its scope outside networkrange.packet should pass with number of intermediate or neighbour node.

Energy Constrained Operation

Some or all MANET nodes relay on batteries so important challenges is to design the system to consume law battery power.

Limited Bandwidth

Bandwidth is low compare to wire network is low due to stale routes, various noise, distortion and fadding effect.

Limited Physical Security

Bandwidth is low compare to wired network is law due to stale routes, various noise, distoration and fadding effect.

Autonomous (Region or Orgiation) Node (Terminal)

In this network each node is act as host and router depend on the situation of communication so it is called Autonomous System (AS).

V. THREAT ATTACKS IN WIRELESS SENSOR NETWORK

Why is security necessary in WSN? Due to the broadcast nature of the transmission medium wireless sensor networks are vulnerable. There are another reason of vulnerability of WSNs are nodes are often placed in a hostile or dangerous environment and they are not physically safe. Most of the threats and attacks against security in wireless sensor networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. WSNs are usually more vulnerable to various security threats because the unguided transmission medium is more susceptible to security attacks, but also through traffic analysis, privacy iolation, physical attacks and so on. Different possible attacks can be categorized as follows:

A. Denial of Service Attacks

In WSN, Denial of Service (DOS) is produced by the unintentional failure of nodes or malicious action. In DOS attack the adversary attempts to subvert, disrupt or destroy a network. DOS attack diminishes a network capability to provide a service for any event. The simplest DOS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled.

B. Flooding

Flooding is a DOS attack in transport layer. A protocol becomes vulnerable to memory exhaustion through flooding when it maintains at either end of a connection. An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored. Disrupt communication is one of purpose of this attack. It creates resource exhaustion and reduces availability.

C. Black hole Attack

A malicious node acts as a black hole in the range of the sink attracts the entire traffic to be routed through it by advertising itself as the shortest route. The adversary drops packets coming from specific sources in the network. Once the malicious device is in between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. This attack can also affect the nodes those are considerably far from the base stations. It creates high rate of packet loss, network partition. It decreases the throughput of a subset of nodes. The network architecture of this attack is traditional wireless sensor network.

D. Physical Attacks

Sensors networks typically operate in hostile outdoor environments. The sensor networks are highly susceptible to physical attacks, i.e. threats due to physical node destructions as sensors are small in size, deployed with the unattended environment. Physical attack destroys sensors permanently, so there are looses of cryptographic secrets, tamper with the associated circuitry, modify or replace sensors with malicious sensors under control of the attacker.

VI. PROBLEM FORMULATION

In Ad-hoc Network inside and outside attacks are probable, which mortify the performance of the network. In Inside attacks a node within the network become malicious node and it launched attacks on network. In outside attacks a malicious node which is outside the network, it become the member of the networks and then launched the attack on network. A passive outsider eavesdrops on all communication and aims to negotiation privacy. Among all the attacks discussed previous selective packet drop attack is the most common active type of attacks. Selective packet Drop attack is the partial denial of service attacks which is triggered by the malicious nodes in the network. In the previous times, many techniques have been proposed to isolate selective attacks from the network.

When Selective packet attack is triggered in the network, throughput of the network reduced and delay increase as steady rate. In this research work, detection and isolation of Selective Packet drop attack in AODV protocol is performed. In Figure 3 there are nodes in the network green one is acting as a source and blue one is acting as a destination. Presume source sends packet to the destination. It sends 10 packets. There is a malicious node (mentioned in the red color) at the mid of the path which drops the packet selectively and only forward few packets.

To avoid selective packet drop attack most powerful technique is to observe the behavior of traffic in route set the threshold, calculate the reverse path from any point in route and identify the malicious node use the key distribution technique (KD) to secure routing and it will provide the confidentiality that the lawful source send these packet.

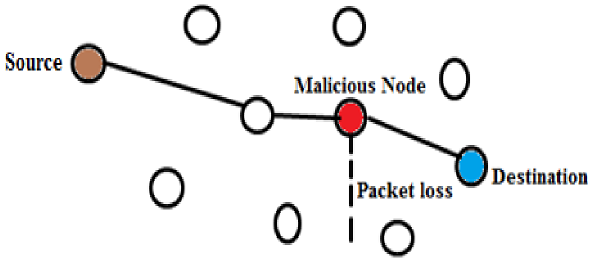


Figure 2- Shows Packet Loss Due to Malicious Node

VII. METHODOLOGY FOLLOWED

New technique is to be designed that can detect the forgery and packet drop in WSN. After detection of this packet drop, the effect of this packet drop will be analyzed. Working on enhancing the network efficiency is the core part of this research. This can be achieved by using the mechanism of key distribution and at last the proposed method is analyzed on some parameters like delay, throughput etc. Firstly wireless ad hoc network with finite number of nodes will be deployed. All the mobile nodes are randomly deployed into the fixed area. The source and destination are selected for route establishment. For the route establishment source node flood the route request packet in the network and route reply packets are send back to the source by the adjacent nodes. The route is established between source and destination on the basis of hop counts and sequence numbers. The malicious node exists in the route which is selected between source and destination. The malicious node will be responsible for triggering the selective packet drop attack. The methodology will detect the malicious node and isolate, it from the network. The methodology is based on the throughput of the network.

When the throughput of the network, will degrades to certain threshold value, nodes in the network will go to monitor mode and detect the malicious node. The technique is to detect packet drop attack in network and improve the performance of the network. The concept use in the technique is based on the monitoring mode and key distribution technique. Proposed technique is working will work in two parts:

- **A.** Key Distribution.
- **B.** Monitoring mode technique.

A. Key Distribution

Ad-Hoc network is created with finite number of nodes. Select the source and destination from the given node. Then check for the availability for the path between node. If path does not exist between the node, then called the AODV routing protocol and deploy the shortest path between the nodes. The node who participates in routing will become a active node. Now, start to flood the packet from the source to destination. The attacker on the path who selectively drop the packets and result will be the packet loss in the given network. To detect this malicious node first we have to make the channel secure so the result will be no interruption in the communication.

B. Monitor Mode Technique

When the source floods the ICMP packet, the entire nodes in the network apart from node who are participated in the routing becomes a passive node. These entire passive nodes start monitoring to one hop node, which issue for routing. Each monitoring node send request to node which is on path. If the replay didn't come in particular time stamp, node is considered as malicious node and all the information about malicious node is send to the Source node. Source node alert its as malicious and start to deploy the new path towards destination and secure it by diffie-hellman.

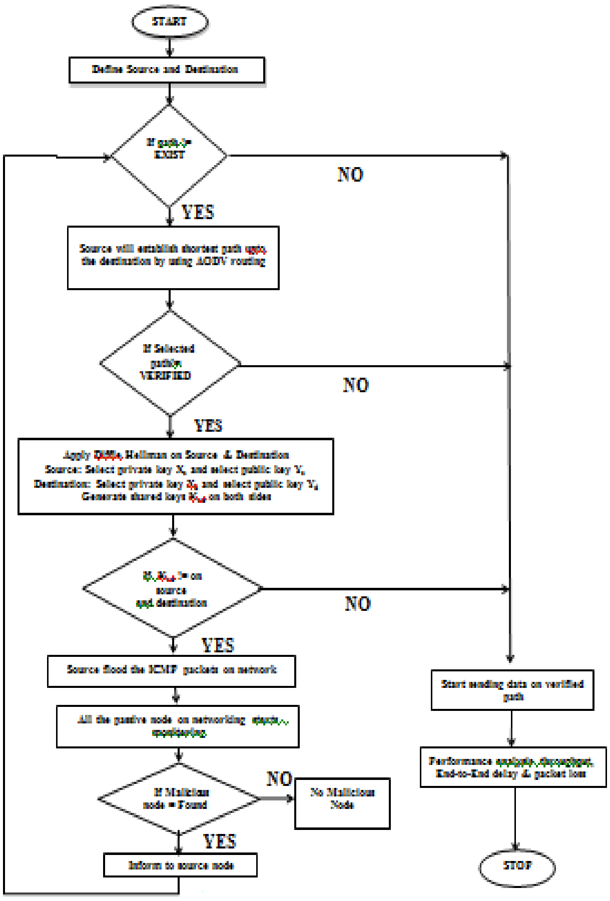

START
Define Source and Destination
If path is EXIST
NO
YES
Source will establish shortest path upto the destination by using AODV routing
If Selected path is VERIFIED
NO
YES
Apply Diffie Hellman on Source & Destination
Source: Select private key X, and select public key Y,
Destination: Select private key X and select public key Y
Generate shared keys K on both sides
If K == on source and destination
NO
YES
Source flood the ICMP packets on network
All the passive node on networking starts monitoring
If Malicious node = Found
NO
No Malicious Node
YES
Inform to source node
Start sending data on verified path
Performance analysis throughput, End-to-End delay & packet loss
STOP

Figure 3- Flowchart of Methodology

VIII. RESULTS OF SIMULATION

In the setup, nodes are labeled as node 0, 1, 2 upto 23. Some nodes among these will be a part of communication and responsible of sending and receiving information.

Figure 4 shows the initial screen shot of this setup in which all the nodes are shown in an idle state. The whole implementation is divided into two parts. In the first part, packet drop attack takes place in which a forgery happens and one node will behave unexpected. After detecting the malicious node, in the second part, it is removed from the group and it will no longer act as a communication node. Then the communication path is updated and used for further transmission. In between "key distribution" mechanism is followed. This mechanism helps to establish a secured path. For selection of malicious node, reverse transmission takes place. It is helpful and really strong method for detection of provenance attack.

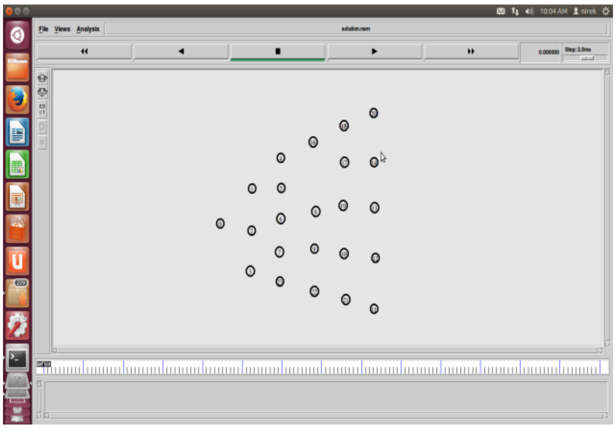
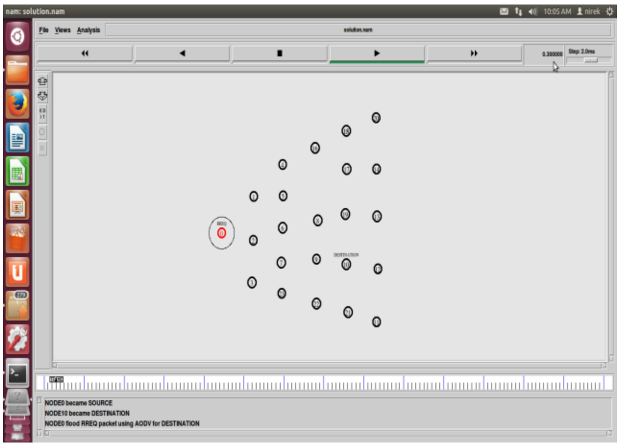


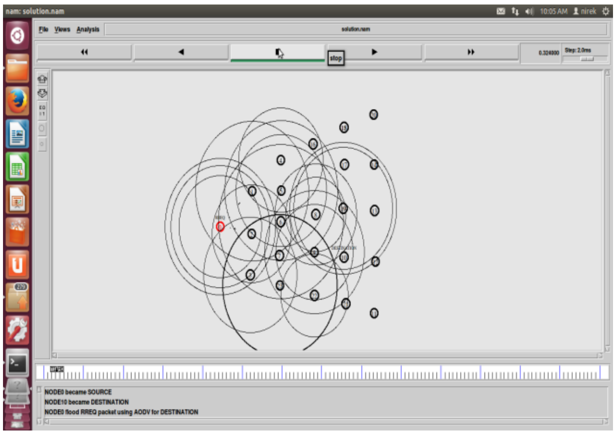
Figure 4- Basic Setup of nodes



```
NODE0 became SOURCE
NODE10 became DESTINATION
NODE0 flood RREQ packet using AODV for DESTINATION
```

Figure 5- Source and destination

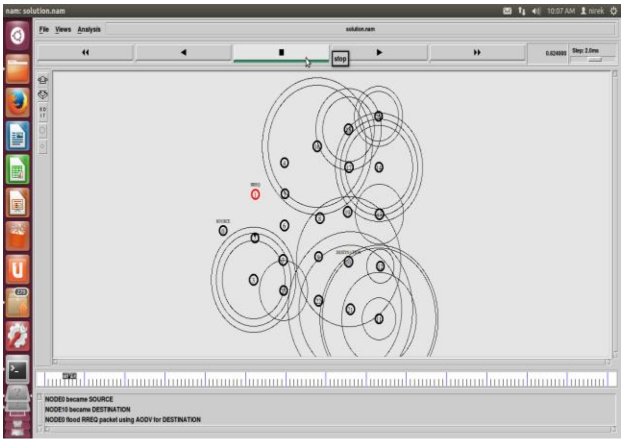
Figure 5 reflects source and destination. In the scenario, node 0 will act as a source and node 10 will act as a destination. Node 0 is labeled as a RREQ (route request packet). It means RREQ packet is being broadcasted from the source node to the other nodes within the network.



```
NODE0 became SOURCE
NODE10 became DESTINATION
NODE0 flood RREQ packet using AODV for DESTINATION
```

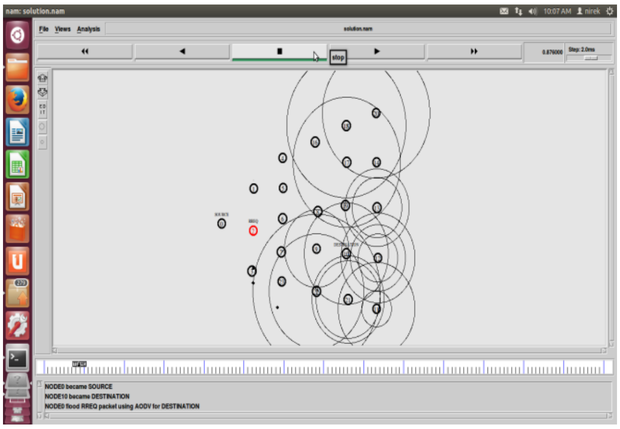
Figure 6- Flooding

In Figure 6, flooding took place in which every incoming packet is sent through every outgoing link except the one it arrived on. Node 0 is still labeled as RREQ this shows that node 0 is broadcasting packets to other nodes in the network. Figure 8 shows packet broadcasted from node 0 and reached to node 1. Now, node 1 is labeled as RREQ means whatever is performed by node 0 is now performed by node 1.



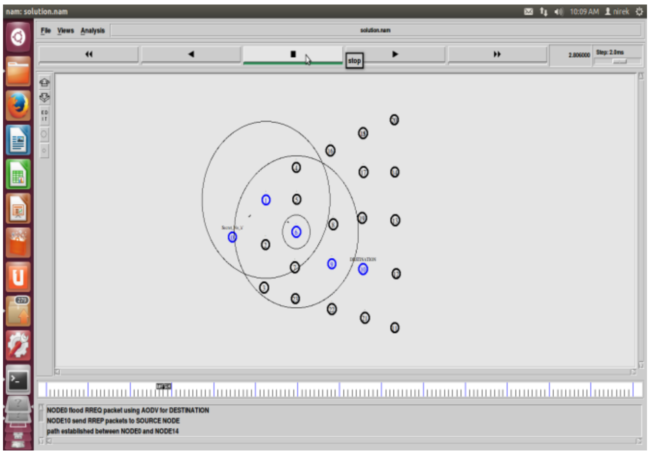
```
NODE0 became SOURCE
NODE10 became DESTINATION
NODE0 flood RREQ packet using AODV for DESTINATION
```

Figure 7- Establishing path



```
NODE0 became SOURCE
NODE10 became DESTINATION
NODE0 flood RREQ packet using AODV for DESTINATION
```

Figure 8- Node 2 is labeled as RREQ

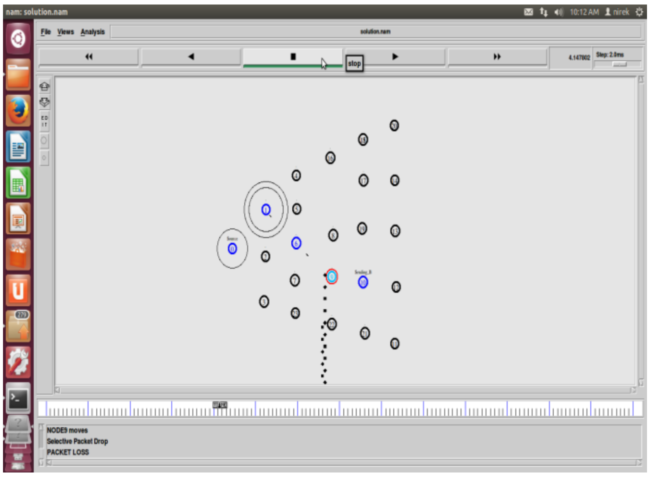


```
NODE0 flood RREQ packet using AODV for DESTINATION
NODE10 send RREP packets to SOURCE NODE
path established between NODE0 and NODE14
```

Figure 9- Established Path

Node 2 is labeled as RREQ in figure 8. This screenshot shows the process of packet delivery from one node to another. The actual path is established step after step. Figure 9 is showing fully established path. In this path node 0 is acting as a source node and node 10 is acting as destination node. In between nodes will collect packet and transfer to the next available node in the network. The established path consists of five nodes labeled as node 0, node 1, node 6, node 9 and node 10.

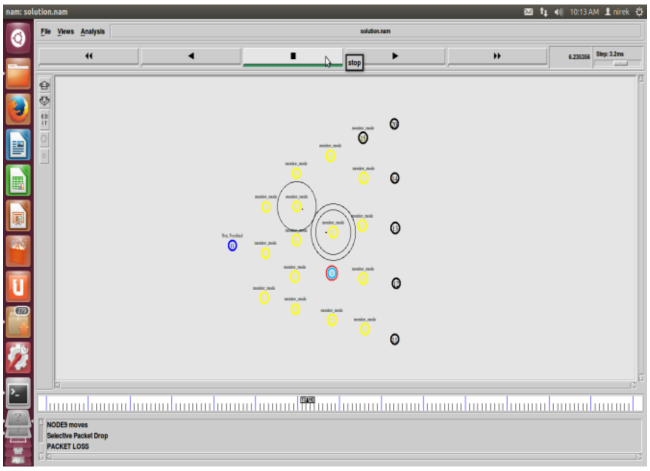
In figure 10, it is shown that node 9 behaving abnormal, it start dropping packets. This clearly means that provenance forgery/ packet drop takes place. All the data transfer further on the same path will be lost.



NODE9 moves
Selective Packet Drop
PACKET LOSS

Figure 10- Packet Drop

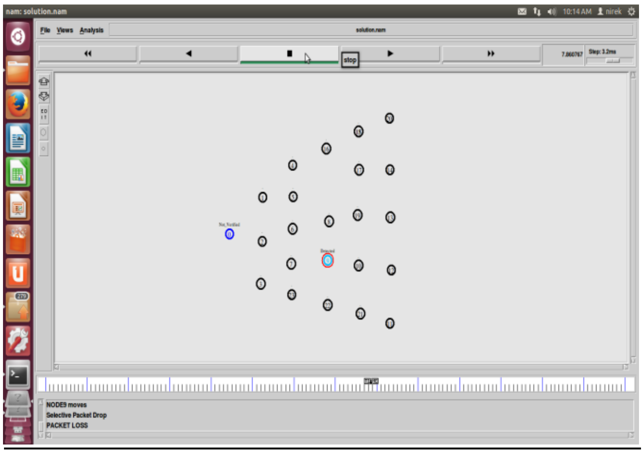
In figure 11 monitor nodes are shown. These nodes get activated after the packet drop. These nodes actually performing high alert in the network so that every other nodes comes to know about the performance of node 9. So, all the nodes around node 9 will act as a monitor node and monitor the activities of node 9.



NODE9 moves
Selective Packet Drop
PACKET LOSS

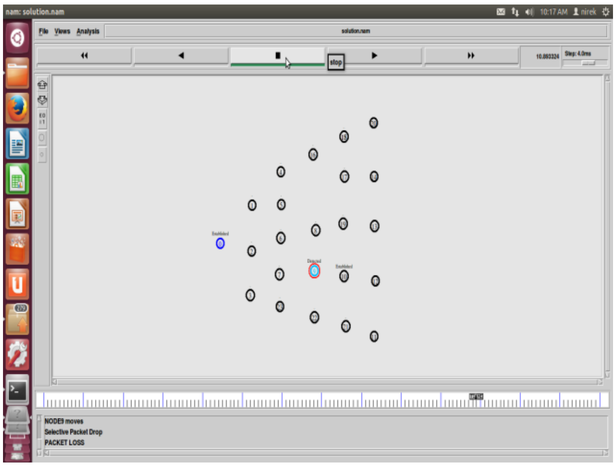
Figure 11- Monitor Nodes activated

Figure 12 shows the node 9 labeled as detected. This means node 9 is a malicious node and performing abnormal jobs. So, the primary mission now is to remove it from the network. Before removing it node 0 and node 10 will communicate to each other by sending some secret packet a and b. So, node 0 will send Secret No. a and node 10 will send Secret No. b.



NODE9 moves
Selective Packet Drop
PACKET LOSS

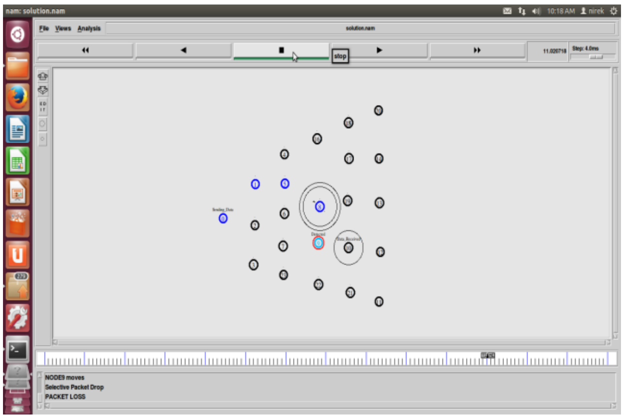
Figure 12- Malicious node detected



NODE9 moves
Selective Packet Drop
PACKET LOSS

Figure 13- Established nodes

In figure 13 both nodes 0 and 10 are showing established as their labels. This means that now secured path exist in between both. Figure 14 shows the final path that is secured and can support pure transmission. Now the new path is established in which node 9 is no longer participating. In the new path node 0 is acting as source node and node 10 is acting as a destination node. In between nodes are node 1, node 5 and node 8.



NODE9 moves
Selective Packet Drop
PACKET LOSS

Figure 14- Successful transmission

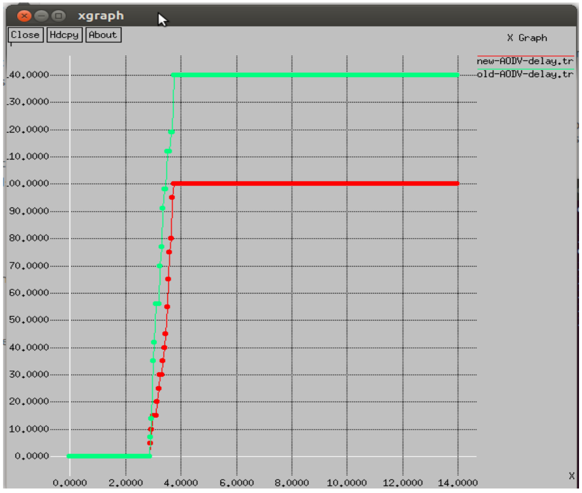


Figure 15- delay Graph

Figure 15 showing the delay graph, here in this screen shot, two graphs are shown. One graph is of green color and other is of red color. Red one is new and green one is old. Both are labeled as new AODV- delay and old AODV-delay. So, in old AODV-delay when malicious node was a part of communication path, the delay was more and it is reduced in new AODV-delay when malicious node was removed and new path is established.

Figure 16 shows the loss of packet in graphical form. Packet loss in new AODV-packet loss is very much reduced as compared to the old AODV- packet loss. So, this graph shows the effect of malicious node on the network and performance of network after removing malicious node from the network.

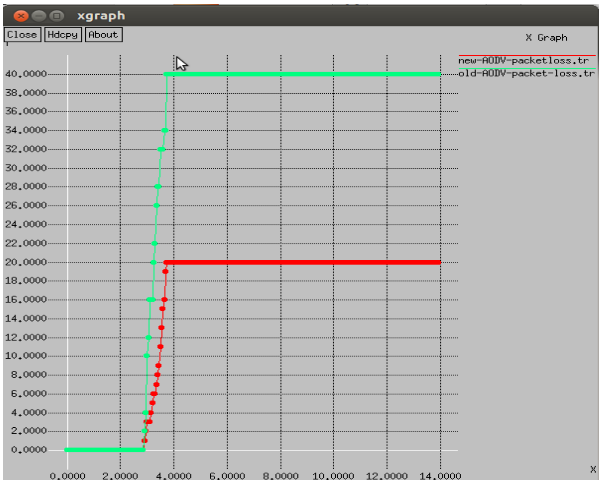


Figure 16- Packet Loss Graph

Throughput is reflected in figure 17. Again both scenarios are represented here. Throughput in case of old AODV-throughput is very less and it is showing dramatically change in case of new AODV- throughput.

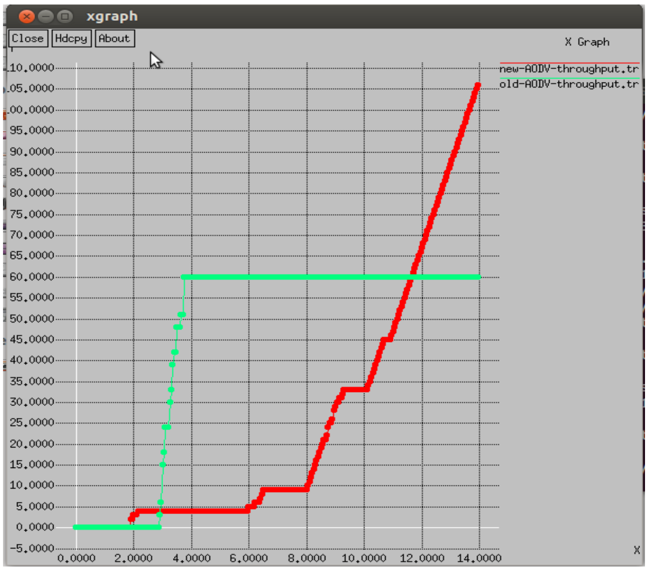


Figure 17- Throughput Graph

IX. CONCLUSION

Wireless ad-hoc network is widely used for business purposes and in battle field as well. So, it has become a vast area of research from past decade. Wireless Sensor Network (WSN) follows dynamic topologies and due to its openness it is vulnerable and insecure. Chances of attack are always higher. In this research, a network is established and data transmission takes place among nodes. The whole work is divided in two phases. In first phase, the attack took place and it put huge impact on the network and its performance. Then reverse communication takes place. After detection of malicious node, the source and destination both exchanges keys and another communication path is established. After establishing another path, again communication takes place and second time; the already detected node will not further act as a participant node. The graphs generated from the research concluded everything. In graphs, throughput, delay and packet loss is shown. All the three graphs perform the comparison of new technique with the older one. So, key distribution techniques works very effectively. Packet loss and delay is reduced and throughput is increased. Network efficiency and its stability after implementation of key distribution are also improved.

REFERENCES

[1] Salmin Sultana et al., "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacksin Wireless Sensor Networks", IEEE transactions on dependable and secure computing, 2015.

[2] K.Sangeetha et.al, "Secure Data Transmission in MANETS Using AODV", International journal of Computer and communication engineering research, 2014.

[3] N.Madhuri1 et al., "Secured Routing through Multi Stage Authentication in MANETs, International Journal of Computer Science and Network Security, 2014.

[4] A.Janani et.al, "Survey of packet dropping attack in manet", Indian Journal of Computer Science and Engineering, 2014.

[5] Sagar Patolia, Harmandeep Singh, "Review of Isolate and Prevent Selective Packet Drop Attack In MANET", International Journal of Innovative Research in Science, Engineering and Technology, 2014.

[6] Anubha Goyal, "Selective Packet Drop Attack in MANET- A Review", A Monthly Journal of Computer Science and Information Technology, 2014.

[7] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE, Volume 40, Number 10, 2002, pp 70-75.

[8] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, volume 5, Number 3, 2007, pp 338-346.

[9] LathaTamilselvan and V Sankarnarayana, "Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp. 13-20.

[10] N.Bhalaji and Dr.A.Shanmugam, "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", Journal of Software, Vol. 4, Number 6, August 2009, pp. 536-543.

[11] Sahabul Alam `and Debashis De, "analysis of Security threats in Wireless Sensor Network", International Journal of Wireless & Mobile Networks, 2014.

[12] Pradip M. Jawandhiya, Mangesh M. Ghonge "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), 2010, pp. 4063-4071.

[13] Muhammad Umar Aftab et al, "A Review Study of Wireless Sensor Networks and Its Security", http://www.scirp.org/journal/cn, http://dx.doi.org/10.4236/cn.2015.74016, Communications and Network, 2015.

[14] M.-Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Communications, vol. 34, 2011, pp. 107-117.

[15] Priyanka Goyal, Vintra Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011, pp. 32-37.

[16] Ahmed M.Abd EL-Haleem and Ihab A. Ali, "TRIDNT: The Trust-Based Routing Protocol with Controlled Degree of Node Selfishness for MANET", IJNSA, Volume-3, May 2011, pp.189-203.

[17] Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar," End to End Delay Analysis of Prominent On-demand Routing Protocols", International Journal of Computer Science and Technology IJCST,Vol. 2, Issue 1, March 2011,pp.42-46.

[18] H.-M. Sun, C.-H. Chen, and Y.-F. Ku, "A novel acknowledgment based approach against collude attacks in MANET," Expert Systems with Applications, vol. 39, July 2012,pp.7968-7975.

[19] S. Sharmila and G. Umamaheswari, "Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012.

[20] A.Baayer, N.Enneya and M.Elkoutbi, "Enhanced Timestamp Discrepancy to Limit Impact of Replay

Attacks in MANETS", Journal of Information Security (JIS), Vol.3, 2012, pp. 224-230.

[21] (2012, 17 May). The Network Simulator - ns-2. Available: http://www.isi.edu/nsnam/ns/