International Journal of Innovative Research in Electronics and Communications (IJIREC)
Volume 1, Issue 9, December 2014, PP 15-22
ISSN 2349-4042 (Print) & ISSN 2349-4050 (Online)
www.arcjournals.org

SAR Protocol Based Secure Data Aggregation in Wireless Sensor Network

S. Archana
PG Scholar, Department of ECE
National Engineering College
Kovilpatti, Tamil Nadu, India
msarchana2008@gmail.com

A. Saravana Selvan
Asst Professor (SG), Department of ECE
National Engineering College
Kovilpatti, Tamil Nadu, India
asselvan1981@gmail.com

Abstract: *Wireless sensor networks are emerging as broadband communication networks, because of their bandwidth, low cost and easy installation. In large sensor networks, data aggregation significantly reduces the amount of communication and energy consumption in the network. In this paper two different routing protocols namely Ad hoc On-demand Distance Vector (AODV) routing protocol and Secure-aware Ad hoc Routing Protocol (SAR) are proposed. By using these protocols the network performances are evaluated in the presence of three types of attacks namely black hole attack, warm hole attack and grey hole attack respectively. The performance of the network is analyzed using the Network Simulator.*

Keywords: *Wireless sensor network, data aggregation, AODV, SAR, attacks.*

1. Introduction

1.1. Network

A computer network or data network is a telecommunication network that allows computer to exchange data. In computer networks, networked computing devices (network nodes) pass data to each other along data connections. Networks can interconnect with other networks and contain sub networks.

There are two kinds of network technologies:

- Wired – communicates through data cables
- Wireless – communicates through radio waves

1.2. Wired Networks

It refers to the transmission of data over a wire – based communication technology. Examples of wired networks are telephone networks, cable television or internet access and fiber optic communication. Waveguides used for high power applications are also considered as wired line.

1.3. Wireless Networks

Wireless networks are computer networks that are not connected by cables. The use of wireless network enables enterprises to avoid the costly process of introducing cable for connecting different equipments. The basis of wireless system is radio waves, an implementation that takes place at the physical level of network structure.

Devices commonly used for wireless networking include portable computer, hand - held computer, personal digital assistants (PDAs), cellular phones, pen based computers etc., Wireless technologies serve many practical purposes. Travelers with portable computers can connect to the Internet through base stations installed in air ports, railway stations and other public locations. At home users can connect devices on their desktop to synchronize data and transfer files.

1.4. Wireless Sensor Network

Wireless sensor network (WSN) is the collection of homogenous, self-organized nodes called sensor nodes. These nodes have the capabilities of sensing, processing and communication of data with each other wirelessly using radio frequency channel. The basic task of sensor networks is to sense the events, collect data and send it to their requested destination. Many features of these networks make them different from the traditional wired and wireless distributed systems. Traditional wired or wireless networks have enough resources like unlimited power, memory, fixed network topologies, enough communication range and computational capabilities. These features make the traditional networks able to meet the communication demands.

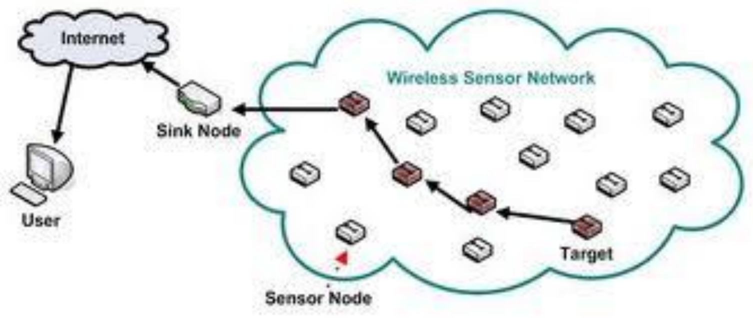

Fig1. *Wireless Sensor Networks*

On the other hand, WSNs are resource constrained distributed systems with low energy, low bandwidth and short communication range. The basic features which make WSNs different from the traditional networks are; self-organizing capabilities, short range communication, multi-hop routing, dense deployment, limitation in energy and memory. The constrained resource nature an unpredictable network structure (sensor nodes are scattered densely in an environment) poses numerous design and communication challenges for WSNs.

2. Data Aggregation, Security Issues and Attacks in WSN

2.1. Data Aggregation

Data aggregation reduces the amount of network traffic which helps to reduce energy consumption on sensor nodes. Two main security challenges in secure data aggregation are,

- Confidentiality
- Integrity of data

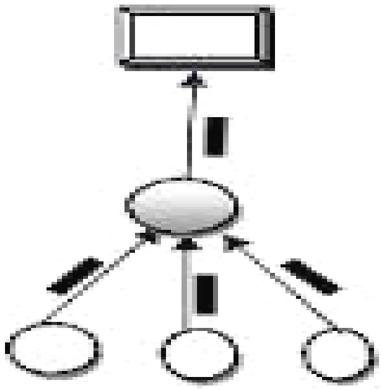

Fig2. *Data aggregation*

The aim of data aggregation is eliminates the redundant data transmission and enhance the lifetime of the energy in the WSN. Data aggregation is the process of one or more sensor nodes that collect the detected result all other nodes. The collected data must be processed by sensor to reduce the transmission burden before they are transmitted to the BS (Base Station). Data aggregation enhance the robustness and accuracy of information. It reduces the traffic load and conserve energy of the sensor nodes respectively.

2.2. Security Issues in WSN

As the sensor networks can also operate in an Ad Hoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of Ad Hoc sensor networks. The security goals are classified as primary and secondary. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA).

The secondary goals are Data Freshness, Self Organization, Time Synchronization and Secure Localization.

2.3. Attacks in WSN

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks.

2.3.1. Black Hole Attack

Malicious node acts as a black hole attack to attract all the traffic in the sensor node. The black hole attack has two properties. The node exploits the mobile Ad Hoc routing protocol, such as, AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Then the attacker consumes the intercepted packet without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other unaffected, which limits the suspicion of its wrongdoing.

2.3.2. Worm Hole Attack

An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a worm hole. Worm hole attack is used against an on-demand routing protocol such as DSR or AODV, the could prevent the discovery of any routes other than through the worm hole.

2.3.3. Gray Hole Attack

Attracting traffic to a specific node in called grey hole attack. In this attack, the adversary’s goal is to attract nearly all the traffic from a particular area through a compromised node. Grey hole attacks typically work by making a compromised node look especially attractive to surrounding nodes.

3. ROUTING PROTOCOLS

A routing protocol specifies how routers communicate with each other, disseminating information enables them to select routes between any two nodes on the computer network. Routing algorithms determine the specific choice of route. Routing protocol shares the information first with the immediate neighbors, and then throughout the network. In this way, routers gain knowledge about the topology of the network.

Routing protocols are in-charge of discovering and maintaining the routes in the network. Routing protocol is a standard that controls how nodes decide to route the incoming packets between devices in the wireless domain. Sensor network routing protocols must ensure the stability of the network infrastructure under varying network dynamics. The protocols must satisfy the system objectives, yet it should not require existing resources.

3.1. AODV Routing Protocol

The Ad Hoc on-demand distance vector (AODV) routing protocol is an on-demand routing protocol. All the routes are discovered only when needed, and are maintained only as long as they are being used. Routes are discovered through a route discovery cycle, whereby the networks odes are queried in search of a route to the destination node. When a node with route to the destination is discovered, that route is reported back to the source node that requested the route to the destination. The following sections describe the features of AODV that allow it to discover and maintain loop free route.

3.1.1. Route Discovery

When a source node has data packets to send to some destination, it checks its routing table to determine whether it already has a route to that destination, if so, it can then utilize that route to transmit the data packets. Otherwise, the node must perform a route discovery procedure to determine a route to the destination. To initiate route discovery, the source node creates a Route Request (RREQ) packet. In that packet the node places the IP address of the destination, the last known sequence number for the destination, its own IP address, its current sequence number and a hop count that is initialized to zero. If there is no last known sequence number for the destination, it set this value to zero. The source then broadcast the RREQ to its neighbors. When a neighboring node or any other more distant node receives the RREQ, it first increments the hop count value in the RREQ and creates a reverse route entry in its routing table for both the source node and the node form which it receives the request. In this way, if the node later receives a RREP to forward to the source, it will know a path to the source along which it can forward the RREP. After creating this entry, the node then determines its response to the request.

A current route is an unexpired route entry for the destination whose sequence number is at least as great as that contained in the RREQ. If this condition holds, the node creates a Route Reply (RREP) for the destination node. Otherwise, if the node does not have a current route to the destination, it simply rebroadcast the RREQ to its neighbors. The following illustrates the flooding of a RREQ, originating at the source node S, through the network.

For example when a source node wants to send a message to a destination and does not have a valid route to the latter, the source initiates route discovery process. Source sends a RREQ packet to all its neighbors, the latter forward the request to the their neighbors and so on, until either the destination or an intermediate node with fresh enough route to the destination is reached. Fig 3 illustrates the propagation of the broadcast RREQs across the network. As in DSDV, destination sequence numbers are used, to ensure that all routes are loop-free and contain the most recent route information. Each node has a unique sequence number and a broadcast ID which is incremented each time the node initiates a RREQ. The broadcast ID, together with the node's IP address, uniquely identifies every RREQ.

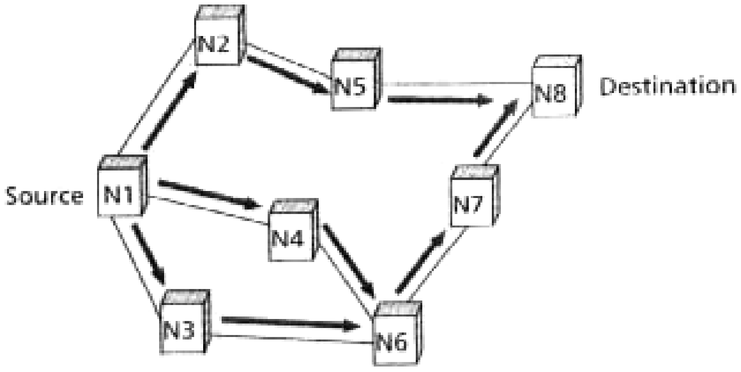

Fig3. *Propagation of route request (RREQ) packet*

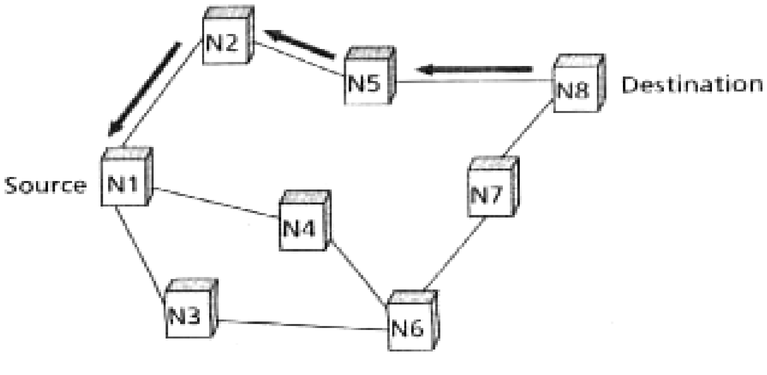

Fig4. *Path taken by the route reply (RREP) packet*

Intermediate nodes reply only if they have a route to the destination with a sequence number greater than or at least equal to that contained in the RREQ. To optimize the router performance, intermediate nodes record the address of the neighbor from which they receive the first copy of the broadcast packet. This establishes the best reverse path. All subsequently received copies of the RREQ are discarded. Once the RREQ reached the destination or an intermediate node with a fresh enough route to the destination, the intermediate or destination node sends a unicast route reply (RREP) message back to the neighbor form which it received the first copy of the RREQ as in the fig 4.

As the RREQ travels back on the reverse path, the node on this path set up their forward route entries to point to the node from which the RREP has been just received. These forward route entries indicate the active forward route. The RREP continues traveling back along the reverse path till it reaches the initiator or source of the route discovery. Thus, AODV can only support the use of symmetric links.

3.1.2. Route Maintenance

A route timer is associated with each route entry. This timer triggers the deletion of the route entry if it is not used within the specified lifetime. When a source node moves, it can reinitiate the route discovery procedure to find the new routes to the destination. If the nodes along the route move, their upstream neighbors (nodes just before them in route from source to destination) notice the movement and propagate a link failure notification to their own active upstream neighbors, and so on until the source node is reached. A link failure is essentially a RREP with infinite metric. The source node can now choose to reinitiate the route discovery procedure if a route to that destination is still needed. In this the route between the source and destination is maintained.

3.2. SAR Protocol

Secure-aware Ad Hoc routing protocol's operation is same as that of the AODV routing protocol. This SAR protocol can be used to defend against the black hole, grey hole and wormhole attacks. SAR protocol is based on the on on-demand protocols such as AODV or DSR. In addition to the AODV protocol this SAR protocol has a security metric which is added into the RREQ packet, and a different route discovery procedure is used.

RREQ packet consist of two security metrics,

- Security requirement.
- Security guarantee.

Then the RREP packet consist of

- Security guarantee.

Route discovered by SAR may not be the shortest route in terms of hop count. SAR finds a route with a 'quantifiable guarantee of security'. If one or more routes satisfying the required security attributes exists, SAR finds the shortest such route.

3.2.1. SAR – Protocol Overview

Basic protocol: On-demand protocol AODV

- Embed security metric into the RREQ packet itself and change the forwarding behavior of the protocol with respect to RREQs
- Source node
  - ➢ Specify desired level of security in the RREQ
  - ➢ Broadcast the packet
- Intermediate node
  - ➢ Process/forward the packet only if it can provide the required security or has the required authorization or trust level. Otherwise drop the RREQ
- If an end-to-end path with the required security found, the intermediate node or eventual destination sends a suitably modified RREP.

3.2.2. SAR (Details of Security Metrics)

In SAR protocol, on-demand route discovery using flooding, reverse path maintenance in intermediate nodes, and forward path setup via RREP messages

RREQ (Route REQuest) packet:

- RQ_SEC_REQUIREMENT: the security requirement set by the sender; does not change during route discovery phase.
- RQ_SEC_GUARANTEE : the security guarantee
  - ➢ Indicates the maximum level of security afforded by all nodes on the discovered path.
  - ➢ Updated at every hop during the route discovery phase.
- If the application requested integrity support, a new field to store the computed digital signatures added to the RREQ.

RREP (Route REPly) packet:

- RQ_SEC_GUARANTEE : the security guarantee
  - ➢ Copied from RREQ and sent back to sender to indicate security level over whole path.

In this way secure as well as valid route between the source and destination is established. Finally the data is securely send to destination through the secure as well as valid route even in the presence of attackers in the network.

4. Results and Discussions

The network performance is analyzed with respect to packet delivery ratio, throughput and delay in the presence as well as in the absence of attacks in the network respectively. The following results are obtained by using the tool network simulator (NS2) and the inference about the results are given by.

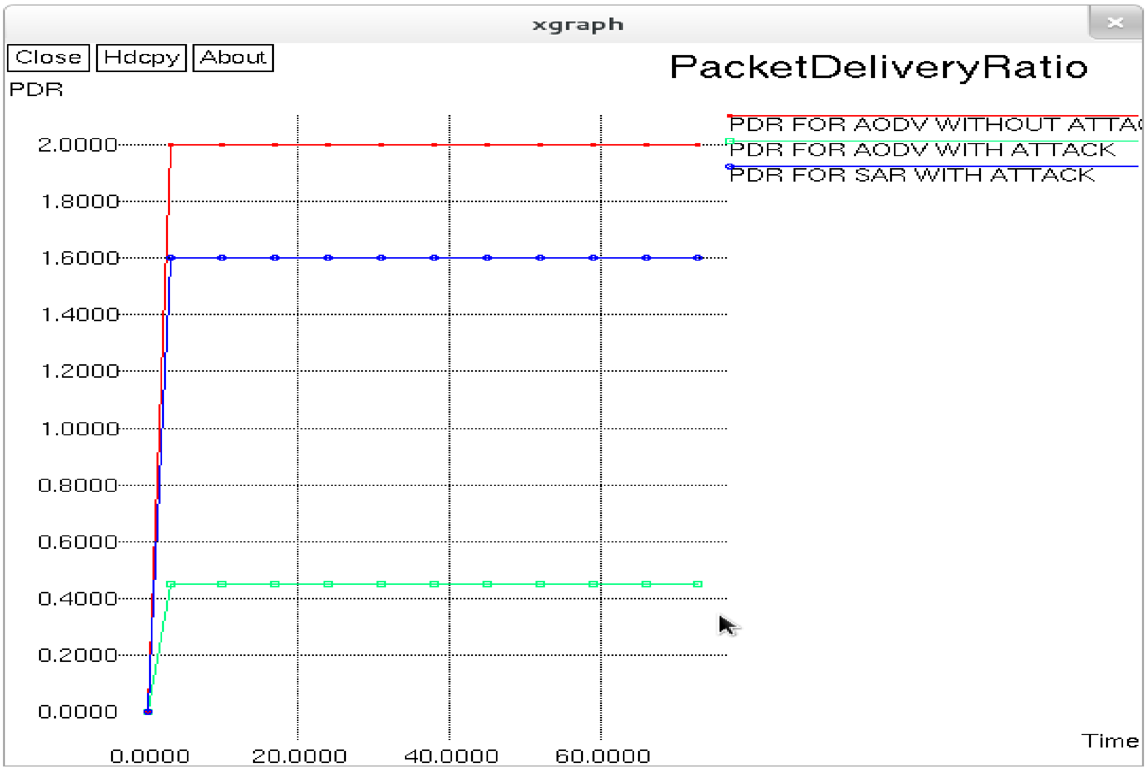

Fig5. *Packet Delivery Ratio*

The above figure shows the x graph for Packet Delivery Ratio. Red color shows the PDR for AODV routing protocol in the absence of attacks in the network. Green color shows the PDR for AODV routing protocol in the presence of attacks in the network. Blue color shows the PDR for SAR protocol in the presence of attacks in the network.

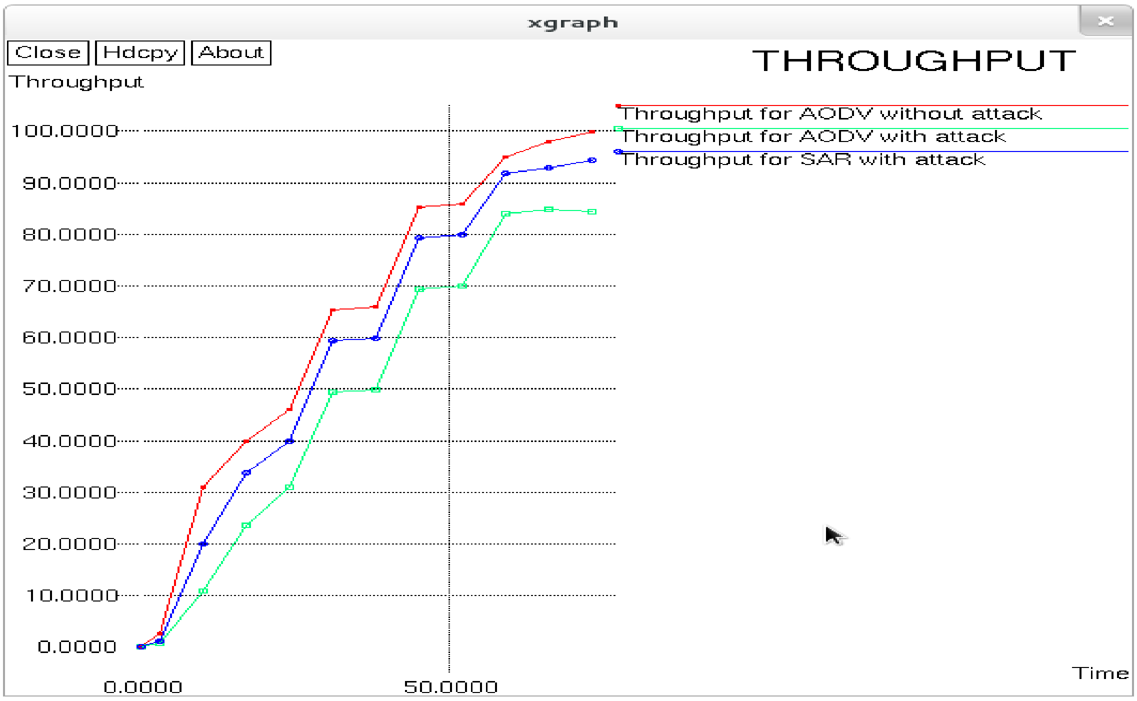

Fig6. *Throughput analysis*

From the above graph the PDR is efficient for AODV routing protocol in the absence of attacks when compared to AODV routing protocol in the presence of attacks in the network. But in the presence of attacks the PDR is efficient for SAR protocol when compared with AODV protocol.

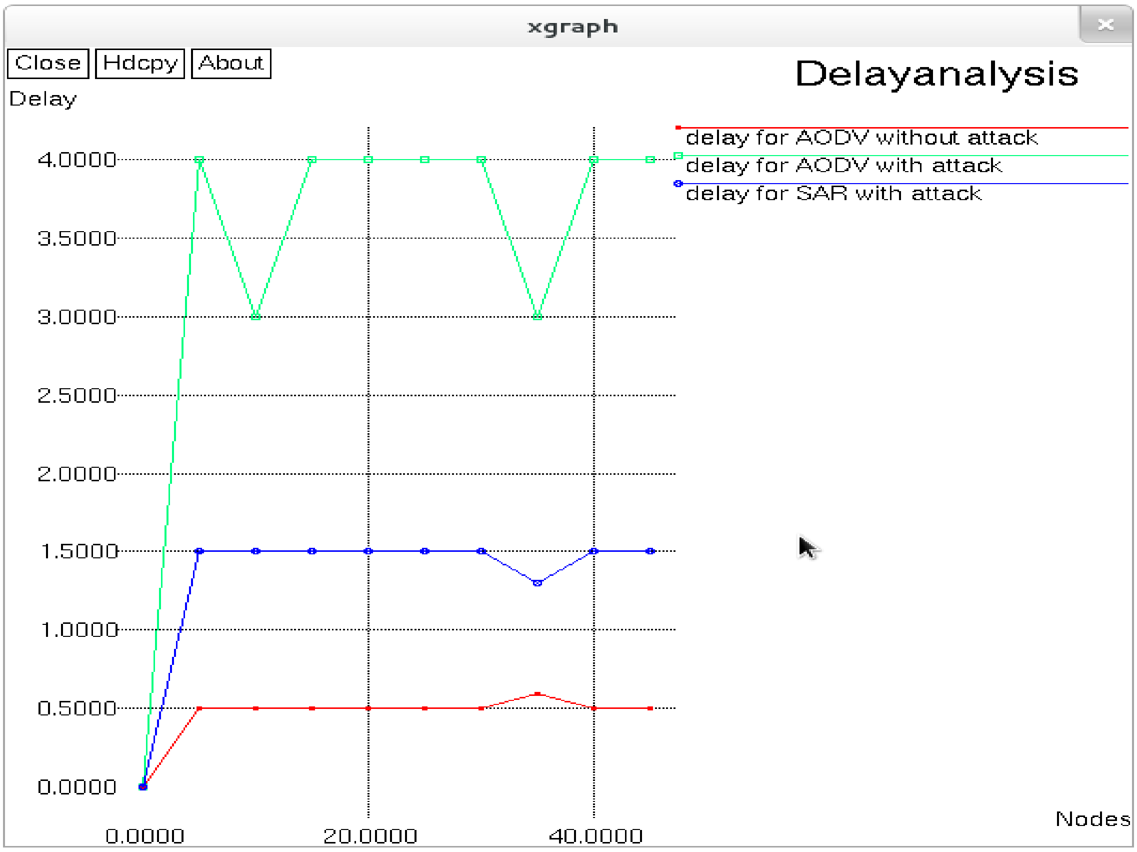

Fig7. *Delay analysis*

The above figure shows the x graph for Throughput analysis. Red color shows the throughput for AODV routing protocol in the absence of attacks in the network. Green color shows the throughput for AODV routing protocol in the presence of attacks in the network. Blue color shows the throughput for SAR protocol in the presence of attacks in the network. From the above graph the throughput is efficient for AODV routing protocol in the absence of attacks when compared to AODV routing protocol in the presence of attacks in the network. But in the presence of attacks the throughput is efficient for SAR protocol when compared with AODV protocol.

The above figure shows the x graph for Delay analysis. Red color shows the delay for AODV routing protocol in the absence of attacks in the network. Green color shows the delay for AODV routing protocol in the presence of attacks in the network. Blue color shows the delay for SAR protocol in the presence of attacks in the network. From the above graph the delay is minimum for AODV routing protocol in the absence of attacks when compared to AODV routing protocol in the presence of attacks in the network. But in the presence of attacks the delay is minimum for SAR protocol when compared with AODV protocol.

5. Conclusion

The proposed routing protocols are Ad Hoc On-demand Distance Vector (AODV) routing protocol and Secure aware Ad Hoc Routing (SAR) protocol. In these protocols the network performance is good for SAR protocol in the presence of attacks in the network. But the network performance for AODV routing protocol is not as much good as SAR protocol in the presence of attacks in the network. The future work is to optimize the output obtained by using SAR protocol in the presence attacks in the network with the output obtained by using AODV routing protocol in the absence of attacks in the network by using the Neural Network approach respectively.

References

[1] Chandni Garg, Prashant Rewagad, “Analysis Of Black Hole And Worm Hole Attack On Aodv Routing Protocol In Manet,” Asian Journal of Computer Science And Information Technology, 2013

[2] Chris Karlof, David Wagner,”Secure routing in wireless sensor networks: attacks and countermeasures,” Published by Elsevier, 2003

[3] L. Hu and D. Evans, “Secure aggregation for wireless networks,” in Proc. Workshop Security and Assurance in Ad Hoc Networks, 2003

[4] Jaspal Kumar, M. Kulkarni, and Daya Gupta, ” Secure Routing Protocols in Ad Hoc Networks: A Review,” Special Issue of IJCCT Vol. 2, 2010

[5] Kemal Akkaya, Mohamed Younis, “A survey on routing protocols for wireless sensor networks,” Published by Elsevier, 2005

[6] Sankardas Roy, Maurto Conti, Sanjeev Setia, and Sushil Jajodia, ”Secure Data Aggregation in Wireless Sensor Networks,”IEEE TRANSACTION ON INFORMATION FORENSICS AND SECURITY,VOL.7, 2012

Authors’ Biography

S. Archana received the B.E. degree from the Department of ECE, PSR Engineering College, Anna University, Chennai, India, in 2013. She is currently working toward the Master degree in the Department of ECE. National Engineering College, An autonomous institution, Kovilpatti, India. Her current research includes Security against the attacks, secure data aggregation.

A. Saravana Selvan received B.E (ECE) from PGP College of Engineering and Technology, Periyar University in 2003 M.E (Applied Electronics) from Department University, Anna University of Technology, Tirunelveli in the year 2011. He is pursuing as Asst Professor (SG) in National Engineering College, India. He has more than 10 years of teaching experience. His area of interest includes VLSI Design, processors, controllers and sensor networks.