MITIGATING DYNAMIC DENIAL OF SERVICES ATTACK IN WIRELESS SENSOR NETWORKS

Chirag H Bhatt[1], Prof. Dushyantsinh B. Rathod[2], Dr. Samrat Khanna[3]
[1] Faculty of Engineering, Computer Engineering Department, Shree Saraswati Education Sansthan
[2] Research Scholar, Rai University
[3] HOD Department of I.T., ISTAR, V V Nagar
Gujarat, India.

Abstract: Wireless Sensor Network (WSN) refers to a network designed for special application for which it is difficult to use a backbone network since there is no proper infrastructure in network.Security threats are high due to wireless medium in WSN. Since mobility of sensor nodes are very low in WSN, we have worked on a pro-active routing protocol namely OLSR.Dynamic Denial of Service attack is one of the most popular attacks in WSN.so a technique to prevent it is necessary to improve performance Of network.the idea behind our technique is to make routing table of malicious node empty so it can't send packets to any node in network.

Index Terms: Wireless Sensor Network, Dynamic Denial-of-Service (DDoS), optimized link stare routing (OLSR).

I. INTRODUCTION

Wireless sensor network has a broad field of applications such as remote monitoring, environmental sensing and target tracking.it consist of a low power sensor nodes equipped with one or more sensors. When the sensor nodes are placed randomly in the hostile environment, and security becomes ex-tremely important factor. The sensed data of the sensor node is prone to different types of attack before reaching to the destination. WSN is highly vulnerable to attack because it consist of various recourse constrained devices with their low battery power, less memory and associated low energy. [1].these attacks can be roughly divided into two categories: routing attacks and forwarding attacks.

The goal of Routing attack is to prevent legitimate nodes from constructing the correct routing tables. This can be accomplished by disrupting the establishment of routing tables, diverting direction of packet forwarding, or tampering the routing information being exchanged among nodes. [2]

In contrast, the packet forwarding attacks maliciously inject excessive data or control packets in the network that saturate the network link bandwidth and computing resources. The overwhelming network traffic prevents the innocent legitimate users from accessing network based services.for example, malicious nodes constantly send data packets.hence resources of network are wasted and it can't be used by legitimate users. [2].

Although there are many strategies available to provide security in in wired network, they can't be directly used in wireless sensor network since lack of infrastructure in WSN.it is more challenging in WSN to satisfy the common security environments such as information confidentiality, data integrity and service availability. Research has been conducted in past few years that tries to integrate security solution on top of secure routing protocols. However, still this process is going on.

In this paper we have proposed a novel approach to improve the impact of Dynamic DoS attack in WSN based on OLSR routing protocol. OLSR inherits the stability of link state routing protocol.

The rest of the paper is organized as follows. Section 2 describes the DDoS attack in brief. Section 4 describes working of OLSR protocol. A brief review of related work is presented in section 5.section 6 contains our proposed scheme.in section 7 we have discussed analysis of simulation results. And section 8 concludes the paper.

II. DYNAMIC DENIAL OF SERVICE ATTACK

Denial-Of-Service (DoS) attacks are particularly damaging since both communication bandwidth and node resources are rare in WSN. In addition to their ability to take down a network rapidly, DoS attacks directed at bandwidth and end node resources are easy to takeoff. So, the availability of WSN has been challenged by Denial of Service (DoS) attack. [3]

The DoS attacks that target resources can be grouped into three broad scenarios. [3]

The first attack scenario targets Storage and Processing Resources. This is an attack that mainly targets the memory, storage space, or CPU of the service provider. Consider the case where a node continuously sends an executable flooding packet to its neighborhoods and to overload the storage space and exhaust the memory of that node. This prevents the node from sending or receiving packets from other genuine nodes.

The second attack scenario targets energy resources, specifically the battery power of the service provider. A malicious node may continuously send a bogus packet to a node with the purpose of consuming the victim's battery energy and avoiding other nodes from communicating with the node.

The third attack scenario targets bandwidth. Consider the case where an attacker located between multiple communicating nodes wants to waste the network bandwidth and disturb connectivity. This consumes the resources of all neighbors that communicate, overloads the network, and results in performance degradations.

Dynamic DoS attack (1) Dynamic DoS Attack Using Node Mobility: The control of DoS attacks may be spread by the mobility of malicious nodes. As shown in Fig. 1(Left), a malicious node m attacks its three neighbors v1; v2 and v3 first. After node m avoids the communications between its neighbors and other cooperative nodes, node m may move to another place, as shown in Fig. 1 (Right), continuing to launch DoS attacks against its new neighbors. If the malicious node m moves into an area with a higher node density, then more cooperative nodes may become the victims of DoS attacks.

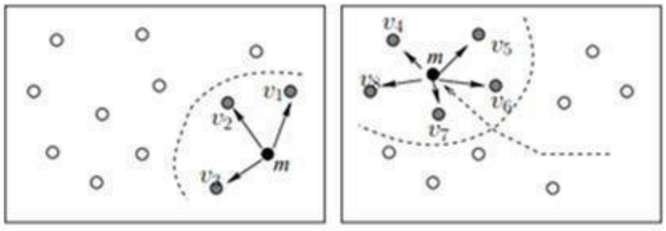

Fig 1-DoS attack enhanced by malicious nodes movement

(2) Dynamic DoS Attack Using Power Management: When malicious nodes have the ability to adjust their transmission powers dynamically, then they can change their transmission ranges to enlarge the attack coverage. For example, in Fig.2, source node s needs to communicate with a destination node d. Then node s sends route discovery requests to its neighbors. When a malicious node m receives the forwarded request message, it can immediately increase its transmission power such that it can reach node s in one hop by increasing transmission range from R to Next node m can unicast a route reply message to node s and claim itself only one- hop away from the destination d. This is a variant of BlackHole attack but more aggressive in that it disturbs the cooperative nodes beyond one-hop neighborhood.

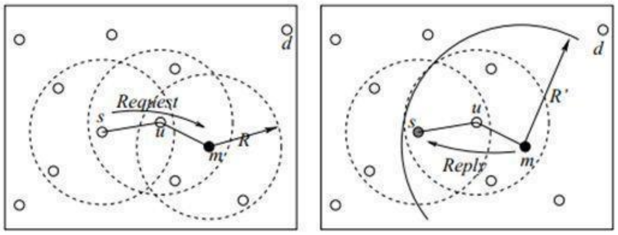

Fig:-2 DoS attack enhanced by dynamic power control.

(3) Dynamic DoS Attack Using Worm-like Propagation: We believe that a malicious may be even able to compromise other cooperative nodes by probing defenselessness and sending some self-executable codes, such as worms. A malicious node can compromise its neighbors, then these compromised neighbors become interior attackers. Further, these compromised nodes may be used to compromise their neighbors continuously. By his way, DoS attacks can spread to a large area of the network or even the entire network.

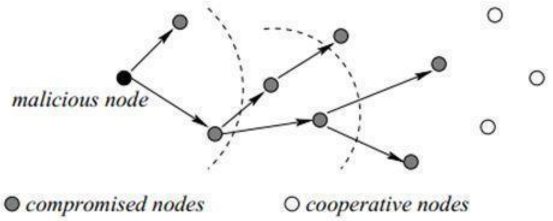

Fig:-3 DoS attack propagation by compromising immediate neighbors.

Instead of compromising the immediate neighbors, a malicious node may take the advantage of its cooperative neighbors to forward its malicious codes to the nodes of two-hop away, as shown in Fig. 4. By this selective compromisation, a malicious node can propagate DoS attacks even faster. In a more severe case, cooperative nodes are isolated with each other, while malicious nodes and newly compromised nodes can communicate via these isolated cooperative nodes. In other words, adversaries may deploy an overlay network on the original network efficiently by propagating DoS attacks dynamically and selectively.

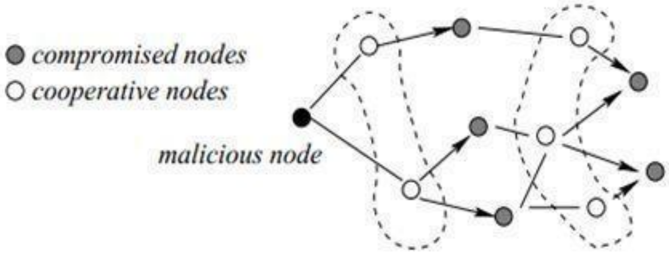

Fig:-4 DoS attack propagation by compromising non-adjacent nodes.

III. OPTIMIZED LINK STATE ROUTING PROTOCOL (OLSR)

OLSR is a proactive routing protocol. It is optimization on pure Link state routing protocol. It reduces amount of data sent in a message and number of transmission required to flood a message.

Working: [4]

- Each node periodically broadcasts its HELLO message.
- Each node generates their MPR set using Hello message and announce it in subsequent Hello message.
- Receiver nodes of HELLO packet generates their MPR selector table and Neighbor table.

- Each node broadcasts specific control messages called Topology control messages to declare its MPR selector set.
- Receiver nodes of TC message generate their Topology table.
- Each node generates its Routing table using its Neighbor table and Topology table.
- While packet forwarding, packet of any node will be forwarded by its MPR neighbors only.

HELLO Message:

- It is sent periodically by each node.
- It contains information about neighbors and their link status.
- It permits each node to get knowledge of its neighbors up to two hops.so that they can select their Multipoint Relays.
- It contains sequence number and expiry time. It is used to create their Neighbor table.

MPR selection:

- Multipoint Relays are set of one hop neighbors that covers all two hop neighbors.
- Goal of MPR selection :
  - Cover all two hop neighbors with MPR.
  - Try to find minimum sized MPR.
- It is recalculated when there is any change in Bidirectional link in one or two hop neighbor set.
- When any node receives this MPR selection list, it will create its MPR selector table.

TC message:

- It is periodically sent by each node to declare its MPR selector list.
- It is retransmitted before schedule when there is any change in MPR selector list.
- It is used to generate topology Table by neighbors of TC message sender.

Topology table Each entry in this table consist of:

- Address of a destination
- Last-hop node to that destination (sender of TC message)
- Corresponding MPR selector set sequence number.

Calculations in Topology Table: Upon Receipt of a TC message following procedure is executed in Topology table.

- if there exist some entry in the topology table whose last-hop address corresponds to sender of TC message and sequence number in TC message is greater than in topology table then that topology entry is removed.
- for each MPR selector address in the TC message :

  – if there exists some entry in the topology table whose destination address to the MPR selector address and the last-hop address of that entry corresponds to the originator sender of TC message,then the holding time of that entry is.

  – otherwise, a new topology entry is recorded in the topology table.

Routing Table:

- It is created using Neighbor Table and Topology Table.
- All entries in neighbor table are directly copied to Routing Table.
- If a last-hop address of any node N in topology table corresponds to destination address in routing table then routing table is updated N.

IV. RELATED WORK

There are many research projects are going on in this field. We have gone through some of the research work in this field. Based on the approaches used in different research work, the strategies are concludes as follows.

In the first approach, a defense mechanism is proposed which has a flow monitoring table (FMT) at each node. FMT contains flow id, source id, destination id and packet sending rate. Data transfer rate is calculated for each flow at the intermediate nodes. With each flow, the updated FMT is sent to the destination. After monitoring the MAC (Media Access Control) layer, the destination sends the Explicit Congestion Notification (ECN) bit to alert the sender nodes about the congestion. [5]

After seeing these packets with ECN marking, the sender nodes reduce their sending rate. If the channel becomes clogged continuously due to some sender nodes do not reduce their sending rate, it can be found by the destination using the updated FMT. It checks current sending rate with the previous sending rate of a flow. When both the rates are same, the corresponding sender of the flow is considered as an attacker. Once the DDoS attackers are found, all the packets from those nodes will be rejected.

The second approach is to use a dynamic method for cluster-based intrusion detection system. Some special nodes called cNodes, are chosen to observe and to report DoS attack activities to the cluster head. But the limitation of this approach is attacker may attack in cNode itself. [6]

The third approach is to use the presence of multipath in these networks to split the initial message in fragments. To combine these fragments that are sent in different paths. With the fragments combination, the message is rebuilt at destination even if all fragments are not reached the destination. To evaluate the proposed method, a logical model is used. It is based on stochastic automata networks formalism (SAN) . [7] In the fourth approach, author discussed through an attack model, that it is easy for a malicious node to launch the node isolation attack to isolate an OLSR node. This attack allows at least one attacker to prevent a specific node from receiving data packets from other nodes that are more than two hops away. The proposed solution called EOLSR, which is based on OLSR, uses a simple verification scheme of hello packets coming from neighbor nodes to detect the malicious nodes in the network. The most important merit is that it achieves degradation in packet loss rate without any computational complexity or promiscuous listening. [8]

V. PROPOSED SCHEME

In the previous work DDoS attack is prevented by maintaining malicious node list. But it is not necessary that we always have list of malicious nodes.it is probable that malicious node changes its id dynamically.so we have proposed a scheme which will work in dynamic environment. We have made some changes in existing OLSR protocol as shown below.

Assumptions:

- Every sensor node has been assigned source id while deploying the network.
- Every sensor node has list of IDs of other nodes in the network.
- The link between any pair of nodes is symmetric.
- Entry in routing table for any pair of network is symmetric.
- Route establishment is necessary before sending packets.

In our proposed scheme every node maintains a list called Net-work List. Which maintains IDs of all the nodes in network.and when any node receives HELLO packet it follows algorithm described in table 1.

The idea behind this scheme is to make routing table of malicious node empty. When any node doesn't accept the HELLO packet, the malicious node is not there in neighbour list of that node. Since entries in all these routing tables are symmetric malicious node will not have entry for that node in neighbour list. And link status of that node in routing table is set to 0.thus at the end of process neighbour table of malicious node remains empty and routing table has link status 0 for all entries.

TABLE I: ALGORITHM 1

```
HELLO reception

If originator node is in Network list then
Populate first hope Neighbour table
Populate two hope Neighbour table
Select MPR set
Populate MPRselector table
Generate TC message and flood it
Update topology table
Update Routing Table
Else
Discard the received HELLO message
End If
```

For example as shown in Fig:-5 all BLUE colored nodes are Legitimate nodes in network and a RED node is malicious node.so when HELLO message is received from RED node, BLUE node will simply drop it and thus RED node will not have route for any other legitimate node so it can't send packets to any node.

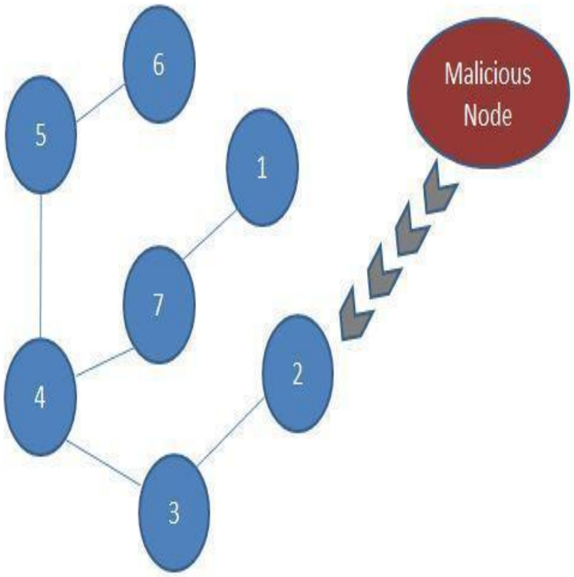

Fig:- 5

VI. SIMULATION MODEL AND RESULT

We have tested impact of proposed scheme by simulating it in NS2.we have generated random topology with parameters shown in table 2. In the simulation of attacked scenario. We have 30 nodes in network and 1 malicious node whose packet rate ishave 30 nodes in network and 1 malicious node whose

TABLE II
PARAMETERS OF SIMULATION

Parameters	Value
channel type	Channel/WirelessChannel
radio-propagation	Propagation/TwoRayGround
network interface	Phy/WirelessPhy
MAC type	Mac/802:11
interface queue type	Queue/DropTail/PriQueue
link layer type	LL
antenna model	Antenna/OmniAntenna
max packet in ifq	50
routing protocol	OLSR
simulation time(default)	100
Default HELLO interval	2
Default TC interval	5
grid size	750*750
traffic source	cbr
packet size	512 byte
transmission protocol	UDP
Nodes	30
packet rate	30

packet rate 125 packets/second.and it attacks on a node in a network.Due to which the receiver node can't receive packets from legitimate sender. Performance is measured for three different scenarios.for each scenario performance of original network with existing OLSR, attacked network with existing OLSR and attacked network with Improved OLSR is measured.

Scenario 1: Varying V_{max}

Observation 1: Throughput

Figure 6 shows when malicious node attacks on network, throughput decreases. But if we use Improved OLSR throughput is increased as compared to existing OLSR.

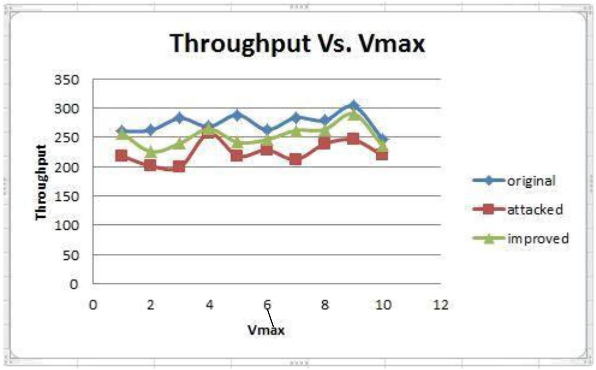

Fig 6.

Observation 2: Packet delivery Ratio

As the graph shows when malicious node attacks in the network, PDR decreases.but if we use Improved OLSR PDR is increased as compared to existing OLSR.

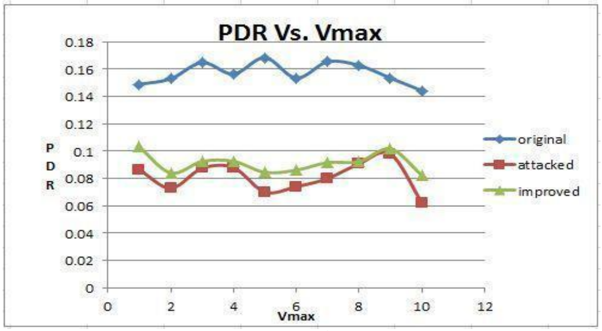

Fig 7

Observation 3: End to End Delay

As the graph shows end to end delay increases when the malicious node attacks the network.But same attack happen in Improved OLSR end to end delay is lower as compared to existing OLSr.

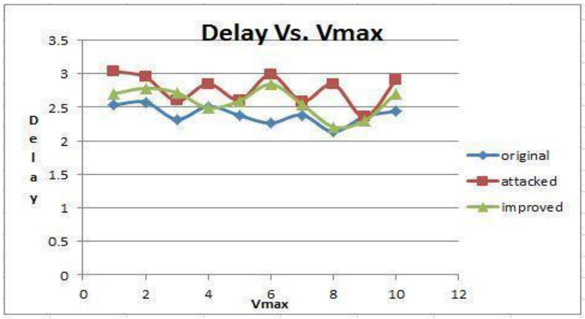

Fig 8

Observation 4: Network Routing Load

It seems that when the responsibility of routing protocol increases, the normalized routing load increases but we have measured the normalized routing load of existing OLSR and Improved OLSR both. And the simulation results so that increment in normalized routing load of Improved OLSR is neglible .Because we have not added any extra control information to be flooded to prevent the attack.

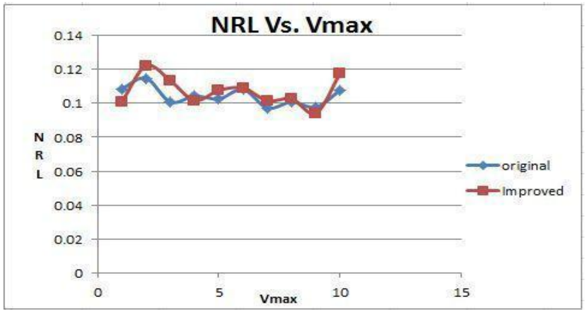

Fig 9

Scenario 2:Varying Pause Time To test the proposed scheme for network with different mobility we have simulated the environment for different pause time and it is observed that it behaves same as scenario 1 except the end to end delay.it is observed that the behaviour of OLSR is uncertain for that case.figure 10, 11 and 12 shows its behaviour.

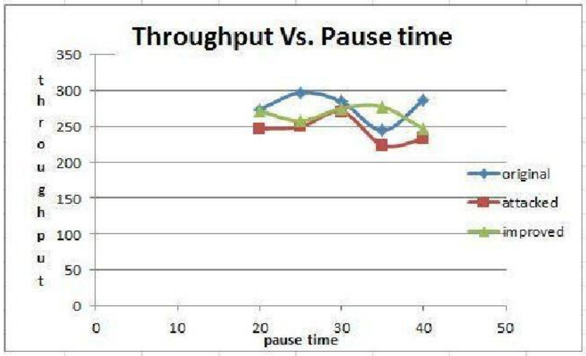

Fig 10

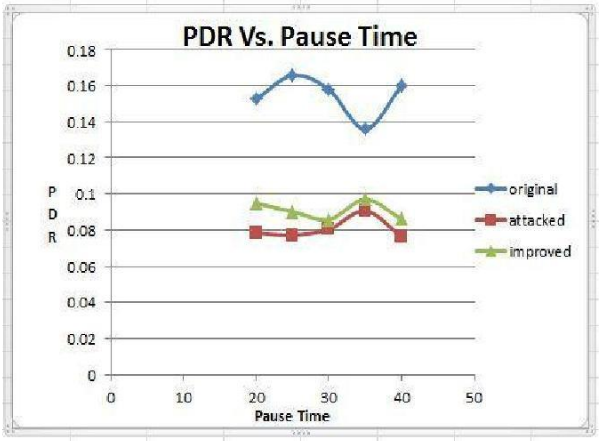

Fig 11

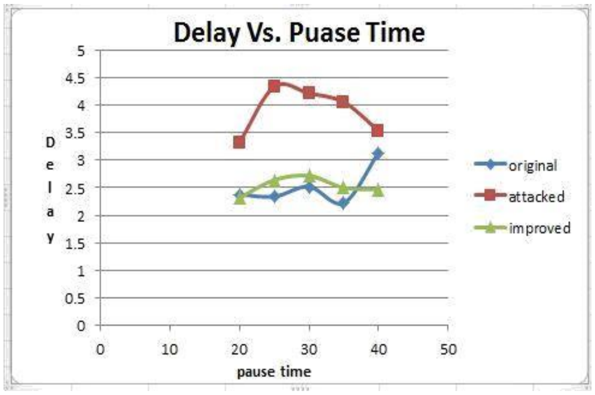

Fig 12

Scenario 3: Varying Simulation Time It is required to verify that improved OLSR Performs well for different simulation time.and simulation result shows that it performs same as scenario 2.figure 13, 14 and 15 shows its behaviour.

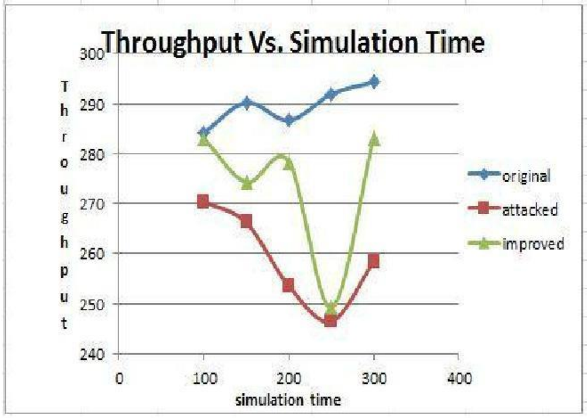

Fig 13

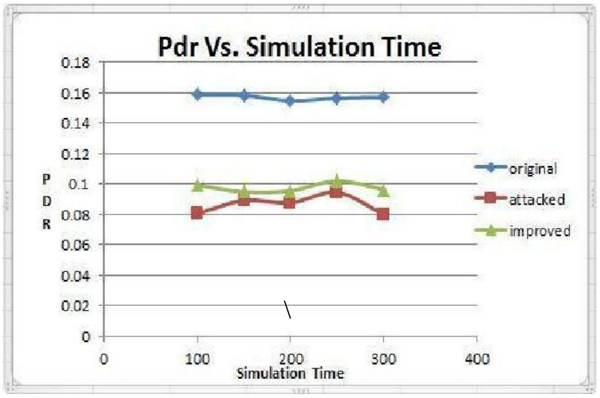

Fig 14

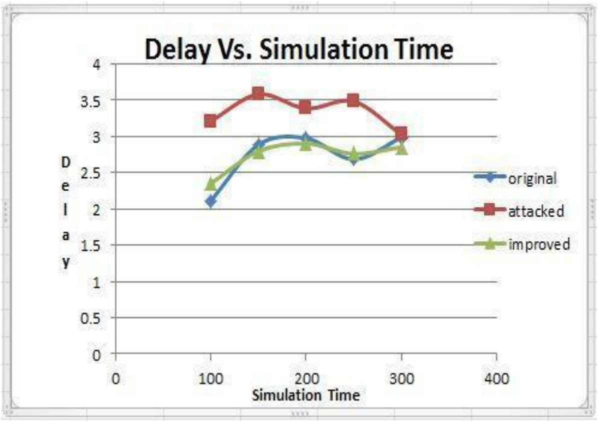

Fig 15

From the simulation results and analysis it is concluded that improved OLSR reduces the impact of Dynamic DoS attack in wireless sensor network.

VII. CONCLUSION

Security in wireless sensor network is ongoing research field since there is no infrastructure in it and the wireless medium is highly vulnerable. Modification in routing protocol is one of the possible approach to prevent this attack.so we modified existing OLSR and from the simulation it is observed that this modification can decrease the impact of attack.

REFERENCES

[1] Saurabh singh and Dr.harsh kumar verma,Security for Wireless sensor network(IJCSE)ISSN:0975-3397.

[2] Mohanapriya Marimuthu and Ilango Krishnamurthi ,Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks,2013 ,ISSN:0975-9646
, IJSCIT.

[3] Fei Xing Wenye Wang,Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks Military Communications Conference, 2006. MILCOM 2006. IEEE

[4] P.jacquet, P. mulhethaler, T. clausen,"Optimized Link State Routing Protocol For Ad Hoc Networks", hipercom project, INIRIA rocquencourt.

[5] S.A.Arunmozhi, Y.Venkataramani ,DDoS Attack and Defense Scheme in Wireless Ad hoc Networks,IJNSA, Vol.3, No.3, May 2011.

[6] Malek Guechari, Lynda Mokdad Dynamic Solution for Detecting Denial of Service Attacks in Wireless Sensor Networks,IEEE ICC 2012 - Ad-hoc and Sensor Networking Symposium.

[7] Lynda Mokdad, Jalel Ben-Othman, Performance evaluation of security routing strategies to avoid DoS attacks in WSN,Globecom 2012 - Next Generation Networking and Internet Symposium.

[8] Mohanapriya Marimuthu and Ilango Krishnamurthi ,Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks,2013 ,ISSN:0975-9646
, IJSCIT.