PalArch's Journal of Archaeology of Egypt / Egyptology

Node Isolation Attack on OLSR ,Reputation Relied Mitigation

[1]Dr.B.Barani sundaram, [2]Mr.Tucha kedir, [3]Mr.Tesfaye tadele sorsa, [4]Mr.Rabira geleta,[5]Dr.Nune srinivas, [6]Adola haile genale

[1]professor & associate dean-ict-ce ,computer science department,college of informatics,bule hora university,bule hora, Ethiopia,

[2]dean ,college of informatics,bule hora university,bule hora, ethiopia,

[3]vice dean ,college of informatics,bule hora university,bule hora, Ethiopia,

[4]lecturer,department of computer science, college of informatics,

[5]assistant professor,school of electrical and computer engineering,addis ababa institute of technology, addis ababa university,addis ababa,Ethiopia,

[6] lecturer, department of information science ,college of informatics, bule hora university, ethiopia

Email: [1]bsundar2@gmail.com,[2] tuchakedir@gmail.com, [3]ttadele14@gmail.com, [4]rabirageleta2@gmail.com,[5]ns_maruthi@yahoo.com,[6]adolahaile2007@gmail.com/[6]adolahaile2019@gmail.com

Dr.B.Barani Sundaram, Mr.Tucha Kedir, Mr.Tesfaye Tadele Sorsa, Mr.Rabira Geleta,Dr.Nune Srinivas, Adola Haile Genale: Node Isolation Attack On Olsr ,Reputation Relied Mitigation -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(9). ISSN 1567-214x

Keywords: Mobile Ad Hoc Networks (Manets), Denial-Of-Service (DOS) Attack, Node Isolation Attack, Optimized Link State Routing (OLSR), Routing Protocols, SMP-OLSR

ABSTRACT

Mobile Ad Hoc Networking (MANET) is an excellent Technology which is taking its importance because of the wide range of wireless portable devices exploiting this facility. Mobile ad hoc networks are highly vulnerable to attacks due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management point. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective for handling the threats associated. Now, a day many applications are constructed with help of proactive routing protocol in MANETs using

OLSR protocol. These applications are useful for disaster relief, emergency operations, and military service and so on.

In this research a improved routing protocol for Ad hoc networks named as SMP-LSR developed from OLSR, incorporating multi-path strategy, source routing control scheme and security to mitigate a specific type of denial-of-service (DOS) attack called node isolation attack is proposed and tested . The proposed Secured Multi-Path OLSR for MANETs is based on link quality and reputation based technique to secure the OLSR nodes against the attack. The technique is capable of finding whether a node is advertising correct topology information or not by verifying its Hello packets, thus detecting node isolation attacks. The protocol is able to achieve routing security mechanism by increasing throughput, frequency and control overhead.

OLSR , guides PDU's to all end devices within the network with help of the routes available via the standard routing table, can be useful for some systems and network applications as there is no route discovery delay associated with finding a new route.

Since hardware resources are limited, it is difficult to implement the research in the real environment. Therefore, Simulation in NS2 environment is used to analyze the different scenarios and test the performance of the modified SMP-OLSR.

The expected outcome of this research is to achieve routing security against node isolation attack with improvement in packet delivery ratio, and also to reduce in packet loss rate.

1. Introduction

1.1 Background

Wireless network is a computer network with some forms of wireless connection. Known as "wireless", it is generally implemented and administrated using radio communication in the physical layer of the OSI model, without any cables. This feature makes it commonly used. The users, homes, enterprise or other organizations can save the money on introducing cables into a building. What's more, they can use the wireless networks anywhere as long as there is a wireless router. The problems in wireless network arenoticeable. The drop off of power of radio is very fast over distance. This limits the communication distance in the wireless network. The solution is to relay the messages. Noise and multipath effect also weaken the efficiency of the transmission. Channel coding is required. Mobility of the device makes the connection in the network unreliable. Vulnerability is also a big challenge for it, because the transmission is open to any user in the network MANET (Mobile Ad Hoc Network), one of the wireless networks. Every node in this network can move freely and every one of them can be chosen as a router. Challenges of this network are along, including scalability, security, lifetime of network, wireless transmissions, increasing needs of applications. Due to the new features in wireless network, routing protocols in the wired network are no longer suitable. The main objective is to get every node accessible to the network and make the data transmission successful.

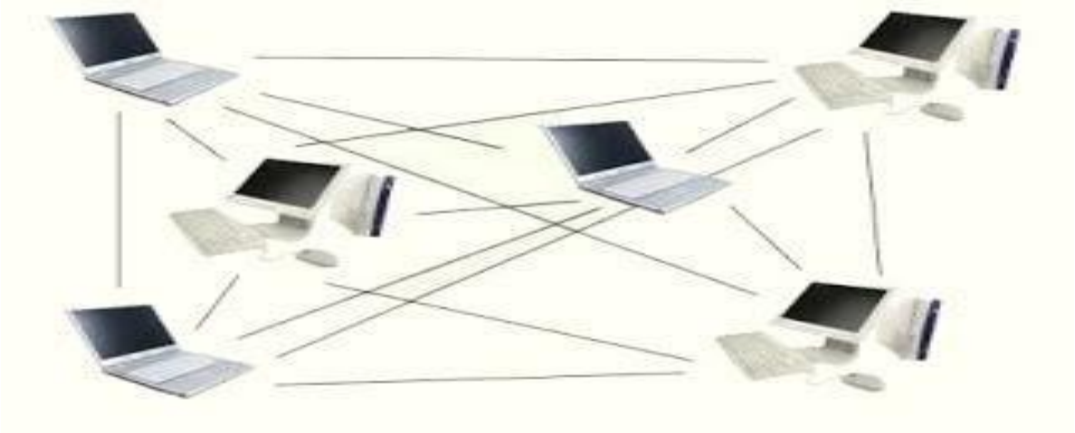


Fig. 1.1 *A Typical Mobile Ad Hoc Network [13]*

To do this, many routing protocols have been developed for ad hoc networks [1]. They can be classified according to different criteria. The most important is by the type of route discovery. It enables to separate the routing protocols into two categories: proactive and reactive. In reactive protocols, e.g. Dynamic Source Routing: (DSR [1]) and Ad hoc On-demand Distance Vector routing (AODV [1]), the routing request is sent on-demand: if a node wants to communicate with another, then it broadcasts a route request and expects a response from the destination. Conversely, proactive protocols update their routing information continuously in order to have a permanent overview of the network topology (e.g. OLSR [1]).

Another criterion for ad hoc routing protocol classification is the number of routes computed between source and destination: multipath and single path routing protocols. Unlike its wired counterpart, the ad hoc network is more prone to both link and node failures due to expired node power or node mobility. As a result, the route used for routing might break down for different reasons.

To increase the routing resilience against link or/and node failures, one solution is to route a message via multiple disjoint paths simultaneously. Thus, the destination node is still able to receive the message even if there is only one surviving routing path. This approach attempts to mainly address the problems of the scalability, mobility and link instability of the network. The multipath approach takes advantage from the large and dense networks.

The main objectives of multipath routing protocols are to provide reliable communication and to ensure load balancing as well as to improve quality of service (QoS) of ad hoc and mobile networks. Other goals of multipath routing protocols are to improve delay, to reduce overhead and to maximize network life time. Multiple paths can be used as backup route or be employed simultaneously for parallel data transmission.

Optimized link state routing (OLSR) routing protocol which is a proactive routing protocol [3] offers promising performance in terms of bandwidth and traffic overhead but it does not incorporate any security measures. As a result, OLSR is vulnerable to various kinds of attacks [3] such as flooding attack, link withholding attack, replay attack, denial-of-service (DOS) attack and colluding misrely attack.

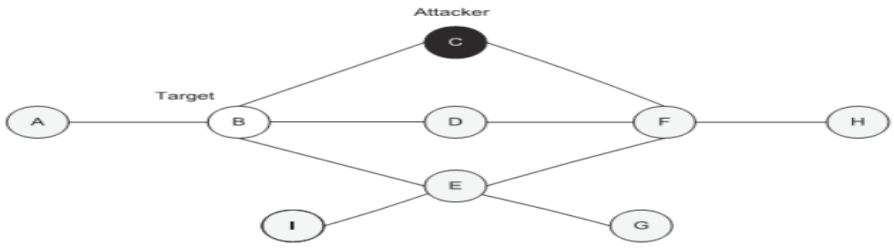


Fig. 1.2 *Topology perceived by node H before the attack [3]*

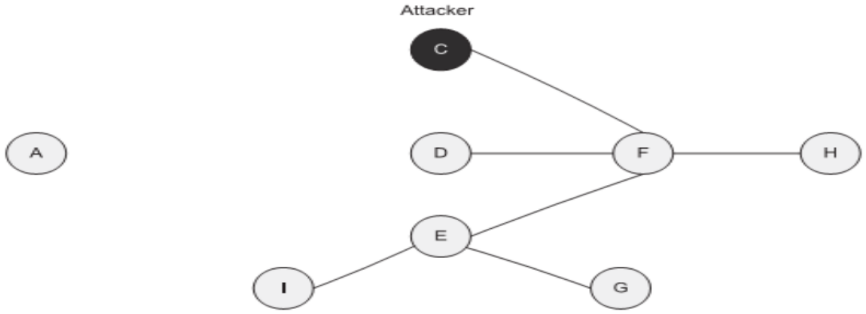


Fig. 1.3 *Topology perceived by node H after the attack [3]*

This work analyses a specific DOS attack called node isolation attack and propose a solution for it. Node isolation attack can be easily launched on Multi-Path OLSR after observing the network activity for a period of time. This work proposes a solution called Secured Multi-Path OLSR (SMP-OLSR) that is based on verifying the hello packets coming from the node before selecting it as a multipoint relay (MPR) node for forwarding packets.

1.2 Statement of the Problem

In this research work A Reputation based approach is used for preventing node Isolation attack. The mechanism is capable of finding whether a node is presenting correct network topology information or not by confirming its Hello messages.

To find multiple paths and load balancing, SMP-OLSR uses the multipath Dijkstra's algorithm. The algorithm obtains considerable flexibility and scalability by using the cost functions, route recovery and loop detection mechanisms in order to improve MANETs performances.

1.3 General Objective:

The general objective of this research paper is to Prevent Node Isolation Denial of service attack in Multi Path Optimized Link State Routing Protocol by Securing it with a Reputation based method for mobile Ad hoc network.

Specific objectives:

✓ To identify and analyze the main security issues in mobile ad hoc network protocols, specifically for OLSR.

✓ To route a message via multiple disjoint paths simultaneously and make load balancing.

✓ To modify the OLSR Protocol with Reputation Based Secure Multipath Method

✓ To Simulate the SMP-OLSR Generate Node Isolation Attack to evaluate existing OLSR and Improved SMP-OLSR.
✓ To analyze and evaluate the Performance of Both Protocols with different metrics

1.4 Scope of the Study:

There are different routing algorithms exist for packet transmission in mobile ad hoc network. Of the existing routing protocols a proactive algorithm, the Optimized Link State Routing (OLSR) protocol [1], has become one of the algorithms widely used today. This work only proposes a prevention method for DOS attack called node isolation attack on Multi Path OLSR.

2. Literature review

Several multipath routing protocols based OLSR have already been proposed. In paper [3] proposed model called EM-OLSR. The approach detects the presence of the malicious node, remove this malicious node simultaneously removing these nodes from the routing table. It uses Hardy function, in order to prevent any future attack. Along with the Hello messages and the Topology Control (TC) messages three other control packets called 2-hop request, 2-hop reply, Node Exist Query(NEQ) are also considered. Consider a specific node "A" in a network. The node would already know it's one hop and two hop neighbors

Nadav Schweitzer, Ariel Stulman, AsafShabtai and Roy David Margalit [4] proposed a method that each node will only use information available to it, without relying on any centralized or local trusted authority. The technique does not actively verify the HELLO message, rather it checks its integrity by searching for contradictions between the HELLO message and the known topology. Allows for lone MPR nominations, provided that no contradictions are found. Even in the face of contradictions, an MPR can be nominated for all 2-hop neighbors for which it is the sole access point. It cannot, however, be nominated as sole MPR for 2-hop neighbors that can be reached through other paths.

The paper assumes that TC messages cannot be spoofed and justifies this assumption due to the fact that bogus TC messages do not preclude a legitimate (attacked) victim from transmitting a valid TC that contradicts the bogus one. In essence, by publishing a fraudulent TC, the attacker discloses that he is attacking; allowing others to take preventive measures. DOS and network disruption due to fraudulent TC messages is outside the scope of this paper.

AsmaAdnane, Christophe Bidan, Rafael Timóteo de Sousa Júnior [7], They proposed a technique is which is a trust based security techniques in OLSR protocol. The nodes are trust based reasoning to each other node, the identifying the behavior of malicious node in networks. The mechanisms detect misbehavior nodes in the networks. The countermeasure and prevention mechanism is used to solve the problems of networks counter and inconsistency of the malicious node in networks. The different attackers and with few modifications, still compatible with OLSR protocol.

They have presented the solution for securing the OLSR Ad hoc routing protocol in three steps.
The first step was the analysis of the implicit trust relations in OLSR. This analysis highlights the possible measures to make OLSR more reliable by exploiting the operations and information already existing in the protocol.
To detect misbehaving nodes, they have developed in the second step, trust-based reasoning by correlating information provided in the OLSR messages received from the network. The integration of this reasoning allows each node to check the consistency of the behavior of other nodes and validate trust relationships established implicitly.
Finally, the third step complements the second by offering two complementary solutions: prevention to resolve certain vulnerabilities of OLSR protocol, and countermeasures to stop and isolate malicious nodes.
In paper [8], the authors proposed an EOLSR that is an enhancement of the basic OLSR routing protocol, which will be able to detect the presence of malicious nodes in the network. The approach assumes that all the nodes are authenticated and can participate in communication i.e., all nodes are authorized nodes. The work is trust-based to detect malicious node and verifying the correctness of the received Hello message from a neighbor node before designating it as MPR for this node. In OLSR routing protocol, every node build its routing table and learn the network topology based on the HELLO and TC messages it receives from its neighbors.
This work analyzes the pattern of HELLO message of the node that advertise all the node's 2-hop neighbors as its 1-hop neighbors and verify whether that node is malicious or not. In this technique, along with HELLO and TC messages, three other control packets called 2-hop request, 2-hop reply and node exist query (NEQ)message are used to verify the information disseminated through the Hello messages. Also, each node maintains a ONE_HOP table which consists of HELLO message sender (all nodes reached by one hop from the given node) and the receiving node's 2-hop neighbors announced in the message
Summary of Literature Survey and Research Gap
The papers discussed in the literature survey have their own assumptions in designing their approaches by adding additional control packets which leads to an increase in network traffic. Therefore, I have identified the problems to fill this gap by removing additional control traffic and nodes from the network.

3. Materials and methodology

The following methods are used as a research methodology to accomplish this work.

3.1 Research and Survey:

- Firstly, most of the relevant researches on OLSR was extensively done to highlight the areas that need improvement.

3.2 Studying NS-2 simulator

- The network simulations will be performed using network simulator NS-2. The NS-2 is software used to simulate discrete event for networks. It simulates events such as sending, receiving, dropping and forwarding packets.

NS-2 is implemented in C++ programming language with Object Tool Common Language. Although NS-2. 35 can be implemented on different Operating Systems, for my thesis work, we select a Linux platform i.e. Ubuntu LTS 12.04, as Linux provides development tools as AWK that can be employed with the simulation. To run a NS-2.34 simulation, the user must write the OTCL simulation script. NS-2 gives a visual presentation of the network by tracing stations movements and events and writing them in a file named as Network Animator file (or NAM file).

3.3 Design EMP-OLSR protocol:

- After reading and collection information about OLRS protocol, design an enhancement protocol called EMP-OLSR with multipath routing and load balancing properties. Implement the Proposed Algorithm using NS-2:
- Testing and validation:

3.4 design of mitigation scheme for node isolation attack in mpolsr

The algorithm which we proposedis a reputation based algorithm. Reputation based algorithms are dependent upon previous history to determine the reliability of neighboring nodes. It uses this factor of reliability to determine which neighbor to use when sending data to a more distant node and which neighbor to avoid.

✓ **Attacker Model**

Fake HELLO Packet generation

The attacker sends fake hello information that he is able to reach all of his two-hop neighbors with the intent of forcing the selection as a MPR, as a result causes the selection of a wrong MPR set.

✓ **General Algorithm Design**

Each node in the network under this scheme will consist of the same configuration. They will contain two tables, a neighbor table and a packet table. The neighbor table consists of the id of each neighbor and the reputation index of its neighboring nodes. After selecting a path, the source node checks the neighbor table to see if the neighboring node is an attack or not. If so, then the packet is discarded since it can't be forwarded. The second table contains all necessary information about each packet of each received packet of data.

The network in this design will be static allowing for better test results. After the initial route discovery, the nodes will not have to perform the discovery again unless a new node is added to the network.

In this case, only the neighboring nodes will be required to make changes to their neighbor table. This will allow them to conserve their power and use it for data transmission and path determination.One Attacker node will be added manually to the design to assure that a Node Isolation Attack exists in the network. This particular node will be marked as attacker node to the algorithm,but the surrounding nodes do not know of their marking. The remaining nodes must discover which of the node is attacker through behavior patterns.

- ✓ **Detailed Design**

The proposed algorithm can be broken down into several parts. These include the creation of the simulated nodes which also includes creating the neighbor list for each node, packet generation, checking the receive queue for valid packets, forwarding packets to the next hop, reputation increase or decrease, and the addition of a new node. Each of these processes is explained in more detail in the following sections.

- ✓ **Node Creation and Simulated Network Setup**

To begin the process, the simulated network is designed and configured. Each node is first created. Since the network is static, the nodes are created with specific X & Y coordinates. Each node is also given other characteristics including:

ID: The unique identifier of each node. This allows all nodes to distinguish their neighboring nodes from each other when deciding whom to send the data to for forwarding. This design has 20 nodes, numbered sequentially 0 through 19. This would be similar to using Media Access Control (MAC) address or Internet Protocol (IP) address for a unique identifier in a real world environment. A MAC address is a unique hardware address that identifies every node on the network. An IP address is a software identifier for each node on a network.

TYPE: Each node is defined as either malicious or normal. This ensures that there are a set number of participating nodes and Attacker nodes. In a real world environment normal nodes participate normally within the network, while malicious nodes participate abnormally at all.

R_INC: This is the value at which a node increases the reputation of its neighbor as a reward for successfully forwarding a packet. For testing purposes, an increment value of .1 was used. With a default value of 10, it will take 50 repetitions of successfully participating before a node can reach the maximum value.

R_DEC: The value at which a node decreases the reputation of its neighbor as punishment for dropping a packet. This implementation uses a value of 1.0. With a default value of 10, it will take only 5 repetitions of not participating within the network before the node reaches the minimum value, while it will take 50 repetitions of participating to recover for the decrements.

Note Both the increment values and decrement values can be easily changed. The less of a difference between the two numbers indicates a less restrictive policy, but is more prone to retransmissions due to more data being sent to malicious nodes. A greater difference indicates a more restrictive policy, but a participating node may be determined to be malicious if it is unable to communicate for one of various reasons.

R_MAX: This is the maximum reputation value any neighboring node can obtain for participating. This implementation uses a value of 15 as the maximum. After a node reaches this value, it can only be decremented. Any further participation doesn't allow for further incrementing.

R_MIN: This is the minimum reputation value any neighboring node can obtain for not participating. This implementation uses a minimum value of 5. Once a node reaches this value, it is ignored by all other nodes, but in receiving and sending, therefore a node at the minimal value can never participate in the network again in this design. In a real world environment, the designer can choose to reset the reputation or give the node another chance to participate after a specific time.

R_ZERO: This is the default reputation value a node assigns to all of its neighbors within the table. This implementation has a default value of 10. All nodes created at the beginning of the network setup obtain the default reputation. Any node added to the network after this point is assigned the default reputation, but the new node uses the global average of the existing nodes for its reputation table.

✓ **Packet Forwarding**

If the received packet passes all of the previous checks, it is determined to be a valid packet. It is next checked to be a data packet. If so, then the packet is added to the receiving nodes packet table for processing.

The first check in determining how to process the packet is to determine if the receiving node is the destination. If the determination is that it is the destination, then it performs the following steps.

✓ Creates and acknowledgement packet to send back to the source, verifying the receipt of the packet.

✓ Adds itself as the source of the acknowledgement and the source of the original packet as the destination.

✓ Adds the last hop of the original packet as the next hop of the acknowledgment.

✓ Increases the sequence number of the acknowledgement to distinguish it from other packets.

✓ Places the acknowledgement packet onto the sending queue of the current node.

✓ Marks the packet for removal from the receiving queue.

If the current node is not the destination then the packet must be forwarded to the next hop. When this is the case, the following steps are performed.

The current node adds itself to the route of the packet for trace-back.

Since routing tables are not used in this implementation, the node doesn't know the correct route. Therefore, the only option is trial and error. The node checks the reputation of all of its neighbors. If it finds a neighbor that is determined to be malicious, that node is ignored in the transmission process

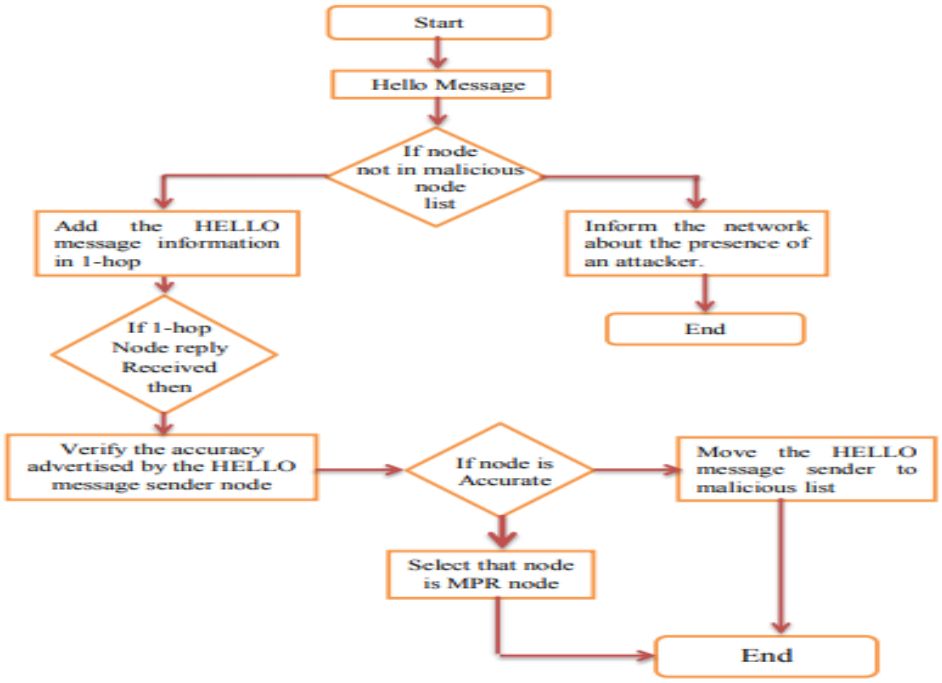
The node sends the packet to all available neighbors attempting to get a response back from the destination, excluding those neighbors that are malicious.

If the current node is the destination and the packet is an acknowledgement, then the packet doesn't need to be processed further. The only action that needs to be taken is the removal of the packet from the receive queue.

Reputation Decrease

If a node sends a packet, but doesn't get a response back, it decreases the reputation of the neighboring node regardless of fault. It is the responsibility of the neighboring node to know the correct path to send the packet. The packet must be able to travel the entire path while avoiding malicious nodes. Below is an example of the reputation topology.
Node 1 sends packet to Node 2.
Node 2 has neighbors 3, 4, and 5. Node 4 is malicious. Node 2 must recognize the maliciousness of Node 3, therefore avoiding sending the packet to him.
Node 3 received the packet from Node 2. It has the option to sending to only Node 4.
The reputation of Node 2 is decreased in the table of Node 1 since it should have recognized that Node 3 had only the option to send to Node 4, a malicious node.

Algorithm 1 HELLO Reception



4. Experiment and evaluation

Implementing A New Routing Protocol in NS To Simulate Node Isolator Behavior In [14] Implementation of a New MANET Unicast Routing Protocol in NS-2 is described. To implement our contribution we have used the details explained in this paper. In our work, we have used the nodes that exhibit Node Isolation behavior in wireless ad-hoc network that use MPOLSR protocol. Since the nodes act as an Isolator they have to use a new routing protocol that can take part in the MPOLSR messaging.
All routing protocols in NS are installed in the directory of "ns-2.29". We start the work by copying MPOLSR protocol in this directory and change the name of directory as "iampolsr".

Names of all files that are labeled as “mpolsr” in the directory are changed to “iampolsr” such as iampolsr.cc, iampolsr.h, iampolsr_m_rtable.cc, iampolr_pkt.h, iampolsr.tcl, etc.

4.1 Simulation Parameters

To take precise results from the simulations, we used UDP protocol. The source node keeps on sending out UDP packets, even if the malicious node drops them,. Therefore, we could observe the connection flow between sending node and receiving node during the simulation.

Furthermore we were able to count separately the sent and received packets since the UDP connection is not lost during the simulation. If we had used TCP protocol in our scenarios we could not count the sent or received packets since the node that starts the TCP connection will finish the connection after a while if it has not received the TCP ACK packet.

We generate a network that has 20 nodes and create a UDP connection between Node 1 and Node 14, and attach CBR (Constant Bit Rate) application that generates constant packets through the UDP connection. CBR packet size is chosen to be 512 bytes long. Duration of the scenarios is 20 seconds and the CBR connections started at time equals to 5.0 seconds and continue until the end of the simulation. We initially defined appropriate positions of the nodes to show the data flow and also introduce different mobility values for the nodes to observe the changes of the data flow in the network.

- ✓ **Evaluation of The Simulation**

The goal of simulation is to verify the reliability of the results. In the first scenario where there is Node Isolator Attack in the network, connection between Source Node 1 and Destination Node 14 is in multiple paths when we look at the simulation output using NAM. Figures below shows the different paths for data flow from Node 1 to Node 14

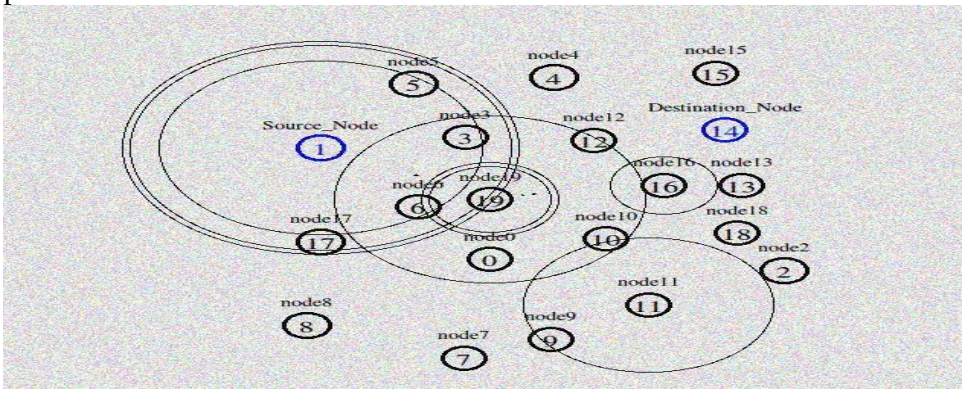


Fig.4.3 *Data flow between Node 1 and Node 14 via Node 19 and Node 16*

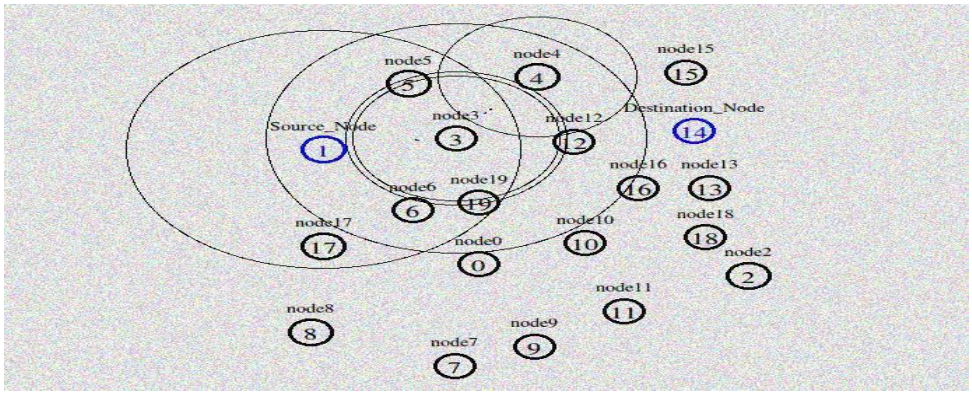


Fig.4.4 *Data flow between Node 1 and Node 14 via Node 3 and Node 4*

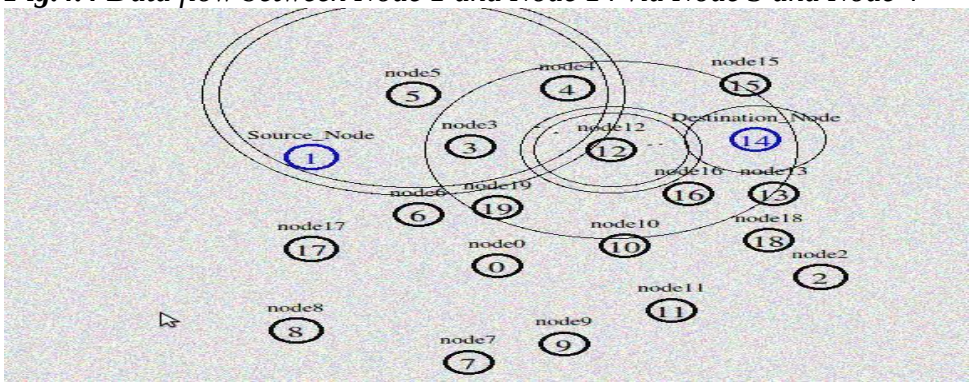


Fig. 4.5 *Data flow between Node 1 and Node 14 via Node 5 and Node 12*

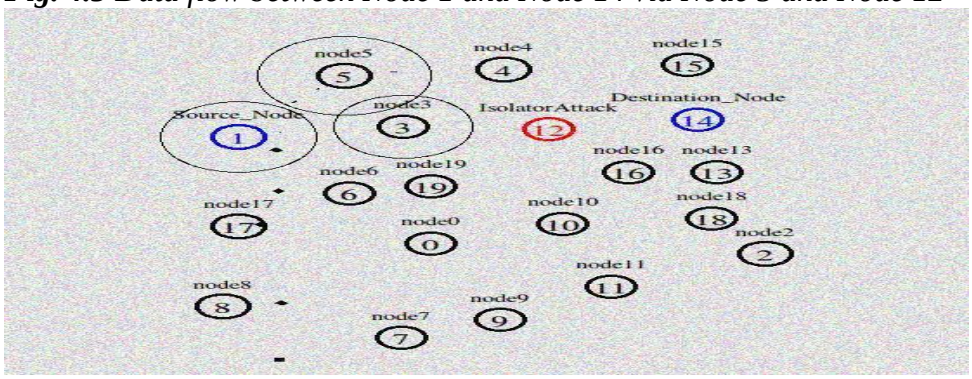


Fig. 4.6 *Data flow between Node 1 and Node 14 when there is an attacker Node 12*

In the third scenario we have provided a solution to detect and prevent the attacker from the network and the mitigation mechanism is already discussed in detail on chapter 5. Figure below shows the simulation output of secured MPOLSR protocol.

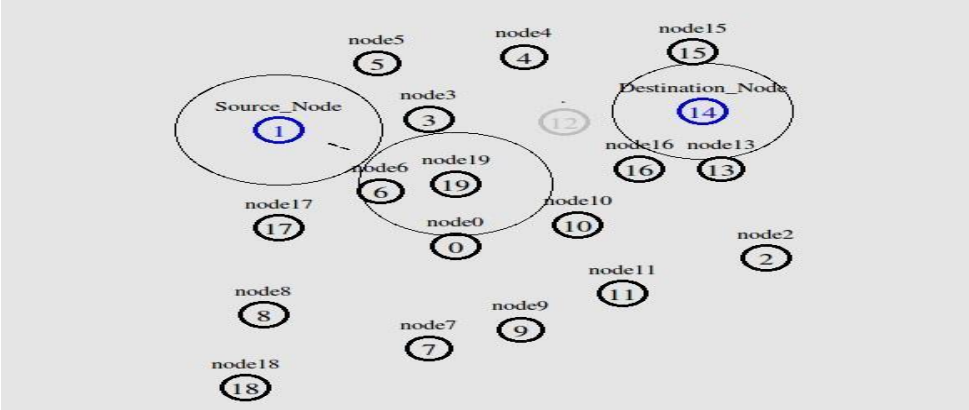


Fig.4.7 *Data flow between Node 1 and Node 14 with Secured Routing Protocol via Node 19 and Node 16*

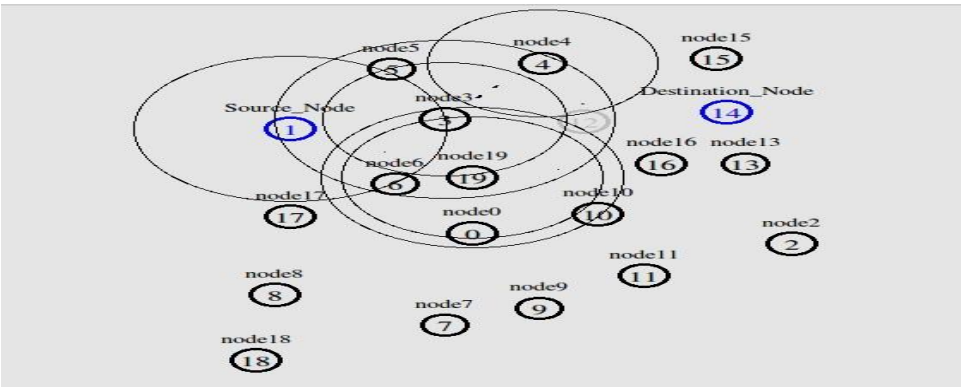


Fig. 4.8 *Data flow between Node 1 and Node 14 with Secured Routing Protocol via Node 3 and Node 4*

In the diagram above source node accepts node 12's hello message then it checks node 12 is in the malicious list since the node is in the list; source node 1 will not accept the hello message of node 12 so that node 12 will not participate in the network.

Simulation Results and Discussions

Here in this part we will discuss the simulation results under normal condition, on Node Isolation Attack Model and with Reputation Based Prevention of Attack for different performance metrics mentioned above.

Packet Delivery Ratio

Table 6.1 *Packet Delivery Ratio versus Mobility*

Mobility	5	15	25
MPOLSR	86.00	80.88	78.38
IAMPOLSR	74.34	69.00	58.88
SMPOLSR	85.25	80.75	64.06

Table 4.1 showsthat how the Packet Delivery Ratio changes when the mobility of nodes changes here from the results we can conclude that when there is more mobility in the network there will be instability therefore some data will be dropped because nodes may be out of range with short period of time.Again when Attacker is introduced to the network the Packet delivery Ratio is the minimum.

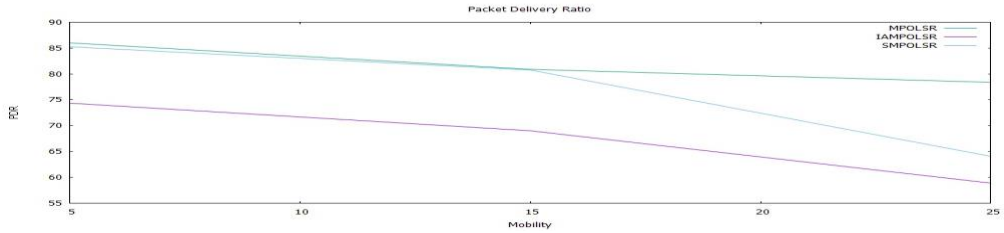


Fig.4.9 *Packet Delivery Ratio versus Mobility*

End-to-End Delay

Table 6.2 *End-to-End Delay versus Mobility*

Mobility	5	15	25
MPOLSR	21.25	27.12	44.58
IAMPOLSR	22.01	32.67	318.25
SMPOLSR	22.57	111.71	49.40

From Table 4.2 we can clearly observe that in the normal implementation which Multipath Optimized Link State Routing (MPOLSR) results a minimum delay with all the mobility options. After a Node Isolation Attack is introduced to the network which is IAMPOLSR the average end-to-end delay automatically increases along with the mobility changes. After the solution for the attack using a Reputation Based Prevention (SMPOLSR) the delay is reduced by far when compared with the Attack Model.

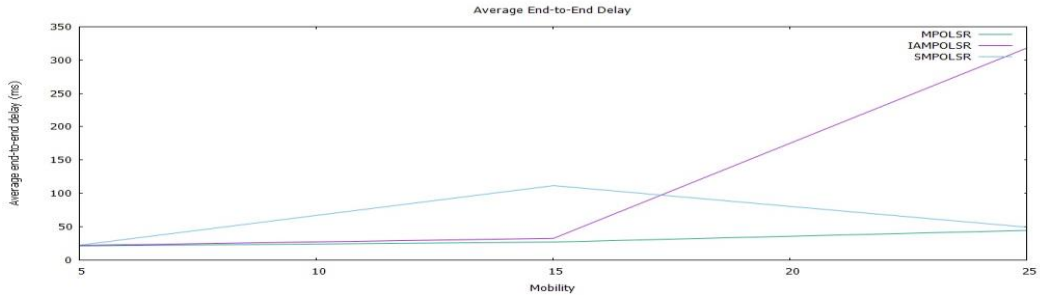


Fig. 4.10 *Average End-to-End Delay versus Mobility*

Average Throughput

Table 4.3 *Average Throughput versus Mobility*

Mobility	5	15	25
MPOLSR	70.47	67.03	64.91
IAMPOLSR	60.85	56.64	48.68
SMPOLSR	69.90	66.86	52.06

In Table 6.3 the normal implementation which Multipath Optimized Link State Routing (MPOLSR) results a maximum throughput because in normal condition the network is more robust but the throughput decreases slightly when mobility increases this occurs due to topology changes. In the Attack model which is IAMPOLSR the throughput is minimum compared with the other two. In SMPOLSR the throughput enhanced by preventing the attacker from the network to create reliable and robust network which increase throughput

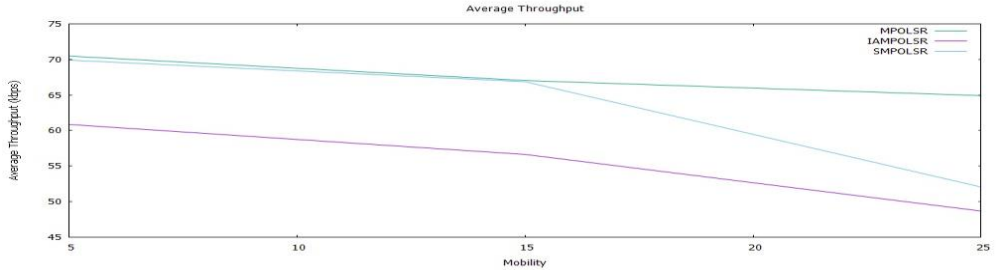


Fig. 4.11 Average Throughput versus Mobility

5. Conclusion

In this research work, we have evaluated the effects of Node Isolation Attack in MPOLSR. By taking different parameters like End-to-End Delay, Network Throughput and Packet Delivery Ratio we observe the actual impact of the attacker in the performance results.

In order to detect this attack and enhance the performance of the MPOLSR protocol we introduce the network with a reputation mechanism to verify the accuracy of the Hello message coming from neighbor nodes before the node gains a privilege in the network.

From the results when an attacker is introduced a lot of packets are dropped which shows worst performance. When the Reputation mechanism is simulated using NS2. Performance evaluation of the scheme has been carried out which shows that the network throughput and packet delivery fraction increases end-to-end delay decreases after applying the proposed scheme.

Finally, from this study we can conclude that the Reputation based mechanism to prevent node Isolation attack brings a better performance in different parameters.

5.1 Future Work

In this research work we have tried to see the effect of the attack through only a single interface in MPOLSR therefore it can be further studied in this approach again through multiple interfaces and the mechanism can be modified to solve for it.

References

Manish Sharma, JaspreetKaur, "Comprehensive Study and Review Various Routing Protocols in MANET" International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), ISSN: 2320-9798, Vol. 3, Issue 3, March 2015

L.M.MaryJelba, S.Gomathi, "Mitigating Different Attacks in OLSR Protocol – A Survey" International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), ISSN: 2320-9798, Vol. 4, Issue 6, June 2016

Megha Eileen Varghese, PerumalSankar "A Secure OLSR against Dos Attack in Ad-Hoc Networks" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN: 2320 – 3765, Vol. 4, Issue 3, March 2015

Nadav Schweitzer, Ariel Stulman, AsafShabtai and Roy David Margalit, “Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes” IEEE Transactions on Mobile Computing, ISSN: 1536-1233, Volume: 15, Issue: 1, Jan. 1 2016

M. Dhivya, A. Kanimozhi, "Improved Routing for Protection against Denial of Service Attack in Ad Hoc Networks" International Journal of Engineering Research Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 3, March – 2014.

V. R. Nisha, S.Rajeswari, "Enhanced Routing in Mobile Ad hoc Network against Denial of Service Attack" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014.

AsmaAdnane, Christophe Bidan, Rafael Timóteo de Sousa Júnior, “Trust-Based security for the OLSR routing protocol” Electrical Engineering Department, University of Braslia, Braslia, DF 70910-900, Brazil, 2013 Elsevier.

MohanapriyaMarimuthu,IlangoKrish“Enhanced OLSR forDefense against DOS Attack inAd Hoc Networks” JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 15, NO. 1, FEBRUARY2013.

B Venkata Ramana, M.V.H.Bhaskara Murthy “Enhanced Multipath Optimized Link State Routing Protocol for MANETs” IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) ISSN: 2278-8735.Volume 9, Issue 5, Ver. IV (Sep - Oct. 2014),

Ashish K. Maurya, Dinesh Singh, and Ajeet Kumar “Performance Comparison of DSR, OLSR and FSR Routing Protocols in MANET Using Random Waypoint Mobility Model” International Journal of Information and Electronics Engineering, Vol. 3, No. 5, September 2013

Ankur Sharma, Er. Rakesh Kumar “Performance Measurement and Analysis of OLSR Routing Protocol Based on Node Scenarios Using NS2 Simulator” International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 3, Issue 4, Jul-Aug 2013, pp.1067-1073.

Mazda Salmanian, Ming Li, “Enabling Secure and Reliable Policy based Routing in MANETs” Defence RD Canada Ottawa, Ontario, Canada, 2013 IEEE.

Rakesh Kumar Jha, PoojaKharga “A Comparative Performance Analysis of Routing Protocols in MANET using NS3 Simulator” I. J. Computer Network and Information Security, 2015, 4, 62-68.

F. J. Ros and P. M. Ruiz, “Implementing a New Manet Unicast Routing Protocol in NS2”, December, 2004, http://masimum.dif.um.es/nsrt-howto/pdf/nsrthowto.pdf, 25 July 2005.

Jiazi Yi “Multipath routing protocol for mobile ad hoc networks” Jun 2015