UTILIZING FICTITIOUS NODES IN OLSR PROTOCOL FORMITIGATING DENIAL OF SERVICE ATTACKS

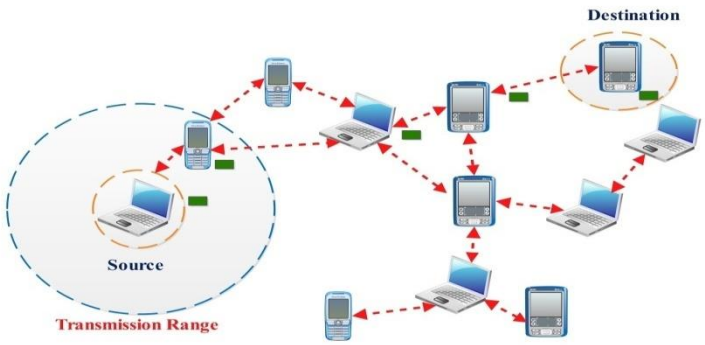
[1]CH.GEETHA MADHURI, [2]K.PRIYA,[3]N.BHAVYA SAI,[4]A.AKHIL,[5]I.NAGA JYOTHI
Bachelor of Technology
Department of Computer Science and Engineering,
Dhanekula Institute of Engineering and Technology, Vijayawada, India

Abstract : With the most focus of analysis in routing protocols for Mobile Ad-Hoc Networks (MANET) engaged towards routing potency, the ensuing protocols tend to be prone to numerous attacks. Over the years, stress has additionally been placed on up the protection of those networks. Different solutions are planned for various forms of attacks; however, these solutions typically compromise routing potency or network overload. One major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker our solution is to defend the OLSR protocol from node isolation attack by using identical techniques utilized by the attack itself. Through in-depth experimentation, we tend to demonstrate that 1) the planned protection prevents quite ninety-five % of attacks, and 2) the overhead needed drastically decreases because the network size will increase until it is non-discernible. Last, we suggest that this type of solution can be extended to other similar DOS attacks on OLSR.

I. INTRODUCTION

There is a rapid escalation in the field of mobile computing as there are widely available wireless devices which are inexpensive. Within the transmission range there are nodes which will communicate with other nodes in the same range directly in MANETS. However, nodes outside one another's range must rely on some other nodes to relay messages. Thus, a multi-hop situation happens, wherever many intermediate hosts relay the packets sent by the supplied host to create them reach the destination node.

A Simple MANET looks like:



The characteristics of MANETS are Wireless medium, Dynamic topologies, peer-to-peer nature, Infrastructure less network, Limited computing resources, Limited Bandwidth. Applications, where MANETS are being used, are Military services, Education, Sensing, and Gaming. As MANETS are dynamic nature, this causes a network to open for attacks and unreliability. The major challenges of MANETS are Topology maintenance, Scalability, Routing in dynamic topology, Security and privacy, Energy efficiency, lack of central infrastructure.

DENIAL OF SERVICE:

A DOS attack is an attack which shut down a system or network or making inaccessible to its users. This is accomplished by creating much traffic in the network or by sending a lot information that leads to crashing of system. If the bandwidth of given node exceeds then also, the network traffic occurs.

General methods of DOS attacks:

Flooding services

Crashing services

Whenever there is a too much traffic from the server to the buffer causes system to slowdown and stop suddenly. These are called Flooding attacks. Some popular attacks are buffer overflow attack, ICMP flood. An attacker can target a system by draining its resources, storage, space, bandwidth, system memory. The DOS attacks on the network are done by changing the routing information or changing system configuration which leads to direct attack on integrity of data.

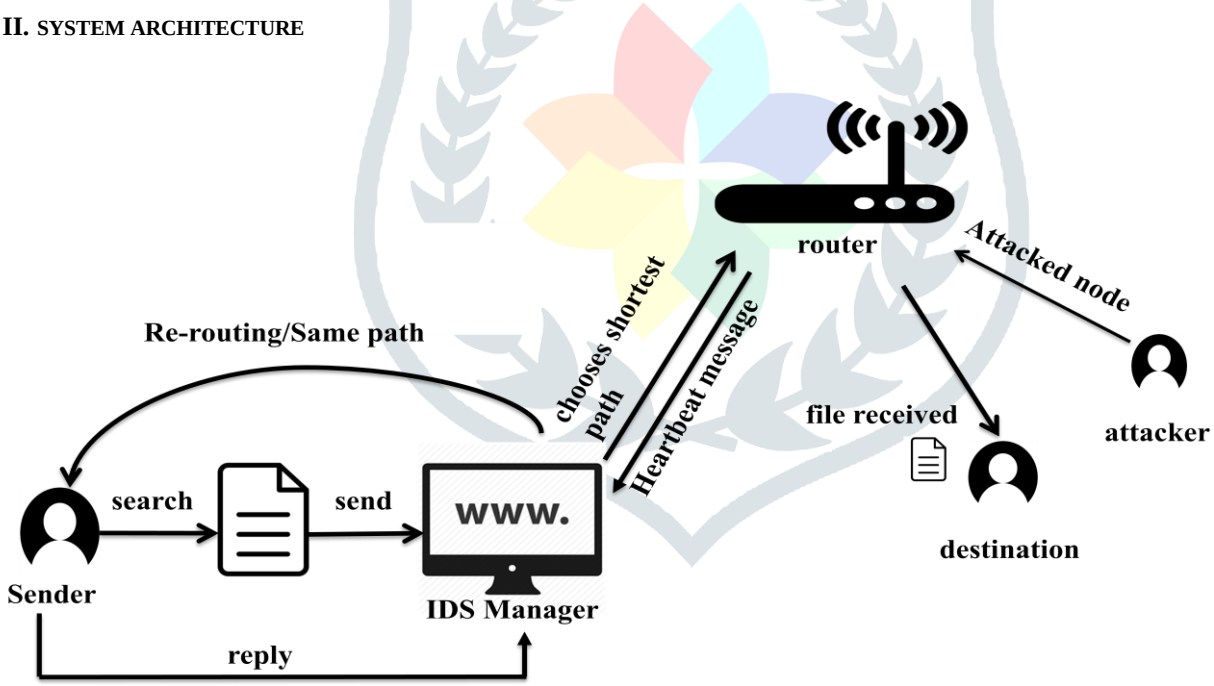
NODE ISOLATION ATTACK:

It is one of the type of DOS, it has the capability of compromising the OLSR protocol which is vulnerable to many attacks. In this attack, an attacker intentionally isolates a selected node from network. In this attacker exploits the fact that a node always prefers a minimal set of MPR. To attack a victim, the attacker simply sends a fake HELLO message. This HELLO message will identify the network topology. It also acts as a fictitious node, so that victim node can get a belief. Then, the victim node will transfer the message to attacker by using the MPR selection rules. This fraudulent MPR will not forward any messages to victim to other nodes, then that node i.e. victim node will be isolated in the network.

OLSR OVERVIEW:

The Optimized Link State Routing Protocol is an IP routing protocol which is used for reducing network overhead for MANET's. Based on specific set of rules the OLSR selectively retransmits the messages to the destination. To discover a network in a topology the OLSR uses two types of messages HELLO and TC i.e. Topology Control. This HELLO message is responsible for declaring a node's knowledge that is present in its surrounding and broadcasting it to other nodes. Any node that receives the broadcast signal and responds back to sender will be classified as a **one-hop neighbor.** Based on HELLO and TC messages received by each node present in the network maintains their network topology. It then discovers each node, calculates and stores the minimal distance assuming itself as the source and the discovered node as the destination resulting in the shortest path to the destination

II. SYSTEM ARCHITECTURE



III. PROPOSED WORK

Our proposed solution is referred as Denial Contradictions with Fictitious Node Mechanism (DCFM) which depends on the internal information non-heritable by every node throughout routine routing, and augmentation of virtual (fictitious) nodes. Moreover, DCFM utilizes constant techniques utilized by the attack to stop it. The overhead of the extra virtual nodes diminishes as network size will increase, that is according to general claim that OLSR functions best on massive networks.

DCFM is unique in that all the information used to protect the MANET stems from the victim's internal knowledge, without the need to rely on a trusted third party. In addition, the same technique used for the attack is exploited in order to

provide protection. By learning local topology and advertising fictitious nodes, a node can deduce suspect nodes and refrain from nominating them as a sole MPR, thus, sidestepping the essential element of the attack

ADVANTAGES:

- The attacks in the mobile which contains nodes can be successfully averted by using this Denial Contradictions with Fictitious Node Mechanism.
- Whenever there is an attack in the chosen path then we can re-route using the different path or can continue in the same path by considering the attacked node as a fictitious node.
- Even though, the attackers are present in the path during transmission. The message will be sent to destination without any eavesdropping or packet dropping.

IV. IMPLEMENTATION

SOURCE:

A sender uploads a file to receiver and then isolates the nodes in the network by using the IP address of the router.

IDS MANAGER:

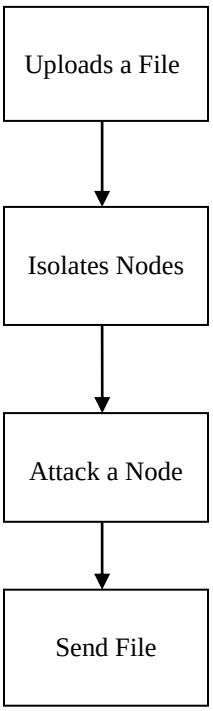
Intrusion Detection System (**IDS**) is a software application or device that monitors network or system activities for malicious activities or policy violations. It contains all the routing information and if the attacking are done the information to the sender about the attacking is given by IDS Manager.

ROUTER:

Router contains all the nodes from the source to destination. The job of the router is to use the OLSR protocol for transmitting the data in shortest and best path and router will be communicating with the IDS Manager continuously.

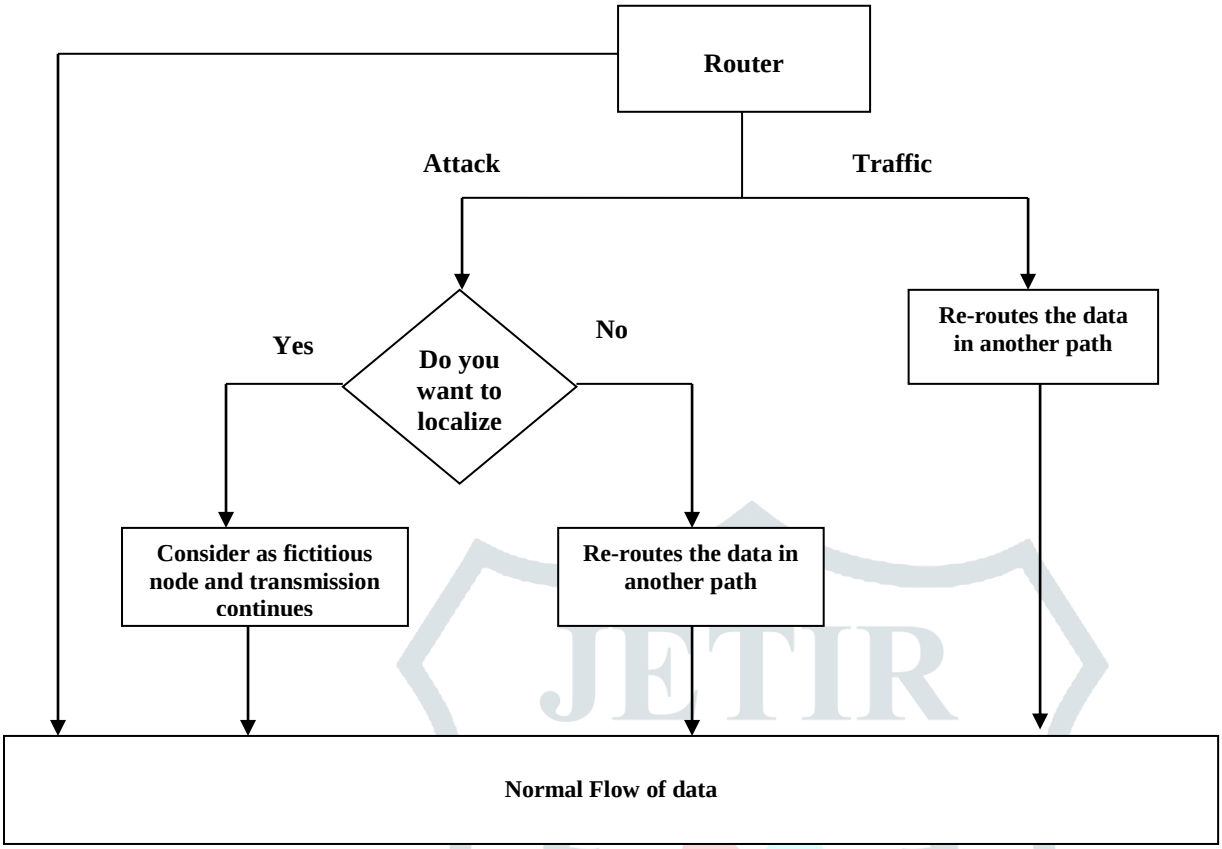
ATTACKER:

The Attacker can change or forge the data by attacking the nodes in the routing path. Attacker can also attack one or more nodes in the selected path these type of attacks leads to the denial of service attacks.



Beginning the process, the sender first uploads a file i.e. is to be sent to the destination node. Later, isolation of nodes is done to activate the nodes present in the network. Then the file is sent to the source through the router by finding out the shortest path using Dijkstra's algorithm. The Dijkstra algorithm is used to find the shortest path from source to destination. This algorithm is used as it gives the best results and it is less complex.

If there are no attacks or malicious nodes in the selected path, then it results in Normal flow of data and the receiver receives the message from the sender. In the IDS Manager there will be information about the normal flow data which is sent to the receiver.



WORKING OF ROUTER

While the data is passing through the nodes present in a network, if there is any malicious node present it results in Denial of service attack. There are two possible cases for the occurrence of denial of service attack. One is to encounter a malicious node and the other is witnessing traffic at a particular node. If a malicious node is discovered, then there are two possible ways of sending the data to the destination without dropping of the packet.

Whenever an attack has occurred then, the information about the attack is given to the IDS Manager then, IDS Manager will generate an acknowledgement to the sender that attack has occurred in the selected path and asks the sender to choose whether, will continue in the same that is localizing or to transmit the data in a new path.

One is considering the attacked node as fictitious node and proceeding with the data transmission and the other process is to reroute the path to transmit the data to the destination. Another possible case for denial of service of attack is the occurrence of traffic. Whenever traffic is observed at a node then the router automatically reroutes the path in which the data is to be sent.

V. CONCLUSION

By using this technique that is DCFM one need not to depend on any trusted third party. It is used to protect MANET's from any attacks by using its internal knowledge and prevents from a attack called Node isolation attack. By learning local topology and advertising fictitious nodes, a node can deduce suspect nodes and refrain from nominating them as a sole MPR, thus, we can reduce the essential element of the attack. This DCFM prevents the attacks successfully, mainly where all the nodes in a network are mobile and DCFM is also of low cost. This DCFM also uses the contradiction rules for preventing these attacks. If the network increases in size, then it leads a overhead to DCFM but this overhead can be reduced by using OLSR because it can work best in this type of large network. As there is an escalation in attacks in MANET's this DCFM provides a solution to reduce this type of attacks, provide security of data and transmit the data to destination without any packet dropping.

VI. REFERENCES

[1] Devish Malik, Krishna Mahajan and M.A . Rizvi “Security for Node Isolation Attack on OLSR by Modifying MPR Selection Process” 2014 First International Conference on Networks & Soft Computing.

[2] Mohanapriya Marimuthu and Ilango Krishnamurthi "Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks" JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 15, NO. 1, FEBRUARY,2013.

[3] A. Nadeem and M. Howarth, “A survey of manet intrusion detection & prevention approaches for network layer attacks,” IEEE
Commun. Surveys Tuts., vol. 15, no. 4, pp. 2027–2045, Oct.-Dec.2013.