A Novel Technique to Prevent Node Isolation Attack in Wireless Ad Hoc Networks using OLSR Protocol

I. Lavanya
M.Tech Student
Department of Computer Science Engineering
UCEK, JNTUK, Kakinada, India

Abstract— Mobile Ad Hoc Network (MANET) is a kind of wireless ad hoc network and is infrastructure-less network of mobile devices connected wirelessly. MANET consists of Peer-to-Peer, self-forming, self-healing network. Generally different routing protocols are available for MANET, the widely used protocol is Optimized Link State Routing (OLSR) Protocol. These algorithms are mainly focusing on routing efficiency, resulting causes various attacks in the network. One of the major attacks is DOS attack called Node Isolation Attack in OLSR. We proposed a novel solution to prevent the DOS attack and to reduce the network overhead by minimizing the fictitious nodes in the network and also select an alternative path.

Key words: MANET, OLSR protocol, Node Isolation attack, Fictitious Node

I. Introduction

MANET is a network that contains a group of mobile devices which exchanges data. There is no centralized authority to control the MANET and no predefined infrastructure for MANET. The nodes can flow freely and at any time it can connect to different nodes. Sending packets from one device to another is done via a chain of intermediate nodes. Mobile nodes have limited resources like bandwidth, Energy limited operation, dynamic topologies and variable infrastructure.

Routing is a process by which the packets are transfer from source to destination. Routing protocol identifies the routes between the nodes and broadcast information which choose the routes between any two nodes on a network. There are different routing protocols existing in MANET. Routing protocols can be categorized into two types: Proactive and Reactive routing protocols. The routing protocols in MANET are attaining to handle a number of nodes with restricted resources.

Proactive routing protocols uses link-state routing algorithms which floods link state information throughout the network frequently. Proactive routing protocol finds route in advance for all sources and destination pairs. And it maintains the information up to date by exchanging the control packet from their neighbors. The examples of proactive routing protocols are DSDV, OLSR, and WRP etc.

Reactive routing protocols minimize overheads that are present in proactive routing protocols. It uses distance-vector routing algorithm and establishes the route to given destination only when there is a data to transmit that means it finds the route only on demand. There are number of reactive routing protocols available in MANET like DSR, AODV, TORA and LMR etc.

II. OLSR Protocol

The Optimized Link State Routing (OLSR) is a proactive routing protocol developed for MANETs. And it's a table-driven protocol. It is an extension of link state protocol in that it reduces the size of control packet as well as the number of control packets required for transmission. Although OLSR is quite efficient in bandwidth utilization and in path calculation, it is vulnerable to various attacks [2].

Two types of messages are used in OLSR protocol to discover and disseminate link state information throughout the network. They are:

- HELLO message
- TC (Topology Control) message

Each node periodically broadcasts its Hello messages contains the information about its neighbors and their link status (bidirectional, unidirectional, MPR). Hello messages are received by all 1-hop neighbors. After successful transmission of hello messages each node constructs its MPR selector table, consists of destination address, destination MPR, and MPR selector sequence.

MPR means Multi Point Relay is a node which selected by its 1-hop neighbors to retransmit all broadcast messages received by it. That means each node decide which of its neighbors can flood LS packet. These nodes are known as MPRs. Only MPR node can retransmit, other nodes don't transmit. When every node select their MPR, these information need to be transmitted to other nodes so that other is also having the information about which is the MPR of which node.

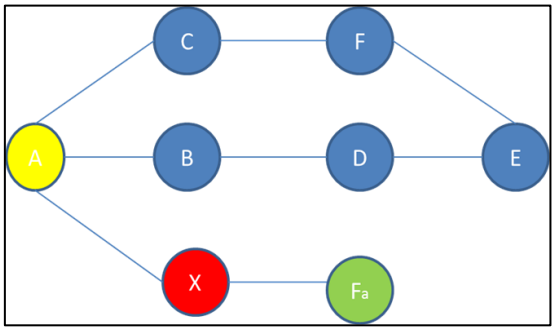

Fig. 1: Example of Node Isolation Attack, A is victim, X is an attacker, and F_a is a fictitious node

Topology control (TC) packets contain the information about network topology. These packets contain the MPR Selector set of a node, and are broadcasted by every node in the network, both periodically and when changes in the MPR Selector set is detected. The packets are loaded in the network using the multipoint relaying mechanism. Each and every node in the network receives TC packets, from which they extract information to build a topology table from these routing tables are constructed.

A. Node Isolation Attack

OLSR is concentrating on routing efficiency resulting causes various attacks in network. Those are called Denial of Service (DoS) attack. One major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological information of the network is known by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim [3].

In order to attack the victim, the attacker will send fake HELLO message. This HELLO message claims that the sender node is in close proximity to all of the victim's 2-hop neighbors. It is also advertises a fictitious node in order to attain the belief of victim. Based on MPR selection rules in OLSR protocol the victim will appoint the attacker as its MPR.

From figure:1 ADJ(A)={B, C, X} and ADJ2(A)={F, D}. Based on OLSR a must select MPR(A)={B, C,X} so that ADJ2(A) is covered. Suppose x is interested in isolating victim A. Then X declares a fake HELLO message containing ADJ(X)={A, F, D, F_x}. Finally A conclude that (F, D) are its 2-hop neighbor, and these are the immediate neighbors of X. So that A decides to select X as a sole MPR for (F, D, F_x) instead of selecting B and C. Here A cannot conclude X is being malicious.

Then the attacker isolate the victim by not including the victim in its TC message then subsequently deny communication services to the victim. So that, other nodes cannot find the path to the victim node. Thus other nodes in the network will reach an assumption that the victim node has moved out from the network. After that remaining nodes in the network will stop sending messages to the victim node. But victim node will continue messaging to other nodes in the network via its attacker MPR. And this malicious node means X will not forward any messages from victim to other nodes in the network. Thus the attacker will isolate the victim from the rest of the network.

III. Related Work

A. Digital Signature

Raffo et al. [4] propose a mechanism to improve the security of the OLSR routing protocol against external attackers. In their solution, each node signs its HELLO and TC messages. These signatures are later used by others to prove their own HELLO and TC messages. The resulting solution prevents devices from declaring imaginary links with known nodes. This solution functions correctly but is expensive in terms of overhead and signing messages requires extensive computation, a cumulative factor that grows as the size of the network increases. Another problem is the fact that all nodes are required to know each other in advance in order to share their public keys. This prevents the network from evolving naturally from the various nodes that appear at a certain place and time.

B. Sequence Number of TC messages

In [6], Kannhavong et al. propose that every node inspect its MPRs' TC messages to see whether it has been included. The attacker MPR will generate fake HELLO messages and broadcast it, but will not generate fake TC message; thereby isolating the node from rest of the network. TC message is the control message used to disseminate the topology information among all nodes in the network. After successful transmission of TC messages of all MPR nodes in the network, each node knows all nodes' MPR set and hence obtains knowledge of the whole network topology [6]. As a node can hear its MPR's transmission it can check for the TC messages generated by its MPR.

During node isolation attack, TC message is not generated by the attacker MPR. The absence of the TC message from its MPR has to be checked thoroughly by a node. Absence of TC message indicates an anomaly. By checking the sequence number of TC message and HELLO message generated by the attacker MPR, the victim node can identify the anomaly. Sequence number is given to both HELLO and TC messages. When there is no attack the TC message and HELLO message has been observed periodically. When there is an attack, the HELLO message is periodic but the TC message is not periodic. The sequence number of TC message is not incrementing at the time of attack. In this way, if a node has detected that its MPR fails to generate TC message, a node can judge that its MPR is trying to isolate it [6]. Using this method a node can identify the source of attack.

This solution is elegant, but it has a number of drawbacks. First, this scheme is only effective against a single attacker but it fails in situations involving two consecutive colluding attackers.

C. DCFM Technique

Denial Contradictions with Fictitious Node Mechanism (DCFM) relies on the internal knowledge acquired by each node during routine routing, and augmentation of fictitious nodes. DCFM utilizes the same techniques used by the attack in order to prevent it [3]. In DCFM the integrity of HELLO message is checked by searching for contradictions in HELLO message with the known topology.

DCFM has three contradiction rules:

1) A victim must confirm that all nodes declared in the HELLO message of attacker must not be among the victim's 1-hop neighbors
2) For each node in the HELLO message, check
   - Existence of 1-hop neighbors not mentioned in HELLO message
   - Also, they are located at-least 3-hop away from victim.
   - If above conditions are satisfied then check whether the attacker has appointed any other MPR to cover those nodes.
3) Victim must treat a HELLO message containing all the 1-hop neighbors as an attack

First and second rules are used to identify the contradiction. Nodes that violate these two rules are treated as malicious. Third rule is used as a preventive measure.

DCFM introduces fictitious nodes in order to prevent nodes in the network from disseminating false information about their connectivity to others. In that case a legitimate node (a) uses fictitious node (F_a) to prevent the attack. Fictitious node cannot be declared, F_a is only known to the legitimate node where as all other nodes treat fictitious node as real node. This leads to all nodes will have

an entry for F_a in their routing table and all routes from or to F_a must pass through a. Therefore, based on the MPR selection rules in OLSR, a will be the MPR to F_a. Thus the attacker will be compelled to appoint a as its MPR. This is impossible to identify through a's TC message.

IV. Proposal of DCFA Technique to Prevent the Node Isolation Attack in OLSR Protocol

Our proposed method is DCFA means Denial Contradiction with Fictitious node and Alternative path. This mechanism also follows the same rules used by DCFM. During the node isolation attack, the DCFA mechanism is coming into the picture. DCFA mechanism replaces a malicious node with fictitious node in the network or else finds second best alternative path from where the attack will found. The main purpose of this mechanism is to prevent the node isolation attack by selecting alternative path and minimizing the network overhead by reducing the number of fictitious node in the network.

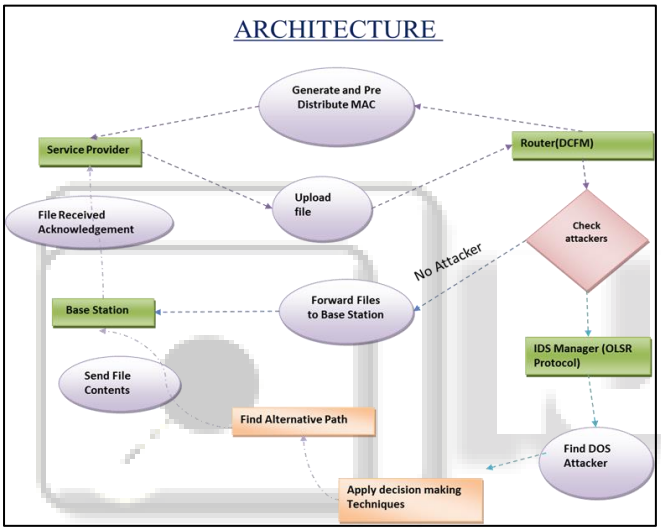

Fig. 2: Working of DCFA mechanism

There are 2 phases in DCFA

- Training phase: If the packet flow is normal then DCFA in training phase
- Testing phase: If there is any error then DCFA enters into the testing phase and checks which type of error was happened.

Algorithm:

1) Isolate Nodes in the network.
2) Select Destination node.
3) Find route between source and destination.
   - Random weights are assigned.
   - Path is calculated by using Dijkstra shortest path algorithm.
4) Source sends a file to the receiver
   If (flow is normal)
   Destination node receives the file and sends an acknowledgement.
   else (Malicious node)
   DCFA method is executed.
5) File received successfully.

Each Router generates its MAC/IP address and distribute over the network. Sender uploads a file and finds a route from source to destination by using OLSR protocol. IDS manager monitor the network and pass information to OLSR protocol. DCFA Checks the errors, if there is more than one attack occurs in the selecting path then apply decision making techniques and select alternative path. After receiving data, receiver sends an acknowledgement back to the source node.

V. Conclusion

This paper focuses on preventing node isolation attack, a type of Denial of Service (DoS) attack in OLSR protocol. We proposed mechanism called DCFA utilizes same techniques used by the DCFM. This mechanism is to prevent a node isolation attack in which the attacker manipulates the victim into appointing the attacker as a sole MPR, giving the attacker control over the communication channel. The main purpose of this mechanism is to prevent the node isolation attack by selecting alternative path and minimizing the network overhead by reducing the number of fictitious node in the network.

References

[1] BR, A.K., Reddy, L.C. and Hiremath, P.S. (2008) Performance Comparison of Wireless Mobile Ad-Hoc Network Routing Protocols.
[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks,"
[3] Nadav Schweitzer, Ariel Stulman, Member, IEEE, Asaf Shabtai and Roy David Margalit, "Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes".
[4] Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, "An advanced signature system for olsr," in Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks.
[5] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the olsr protocol".
[6] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Analysis of the node isolation attack against olsr-based mobile ad hoc networks".

