Prevention of Node Isolation Attack in Mobile adhoc Network

Jefin Liza James[1], Bino Thomas[2]

[1]*Student, Dept of Computer Science & Engineering, St. Joseph's College of Engineering & Technology, Palai, Kerala, India*

[2]*Assistant Professor, Dept of Computer Science & Engineering, St. Joseph's College of Engineering & Technology, Palai, Kerala*

Abstract - *Mobile ad hoc network (MANET) is a wireless communication system of continuously self-configuring and infrastructure-less network of mobile devices. The mobile devices in MANET can move independently in any direction at any time. Routing protocols is required for message exchange in MANET. The most widely used routing protocol for MANET is OLSR (Optimized Link State Routing) Protocol. It is efficient in bandwidth utilization and path calculation. But it is vulnerable to many types of attacks. In this project, a method called DCFM (Denial Contradictions with Fictitious Node Mechanism) is applied to prevent node isolation attack in OLSR protocol. Node isolation attack is a type of Denial of Service (DOS) attack. Node isolation attack occurs when the topology of the network is known by the attacker. The DCFM method use the same tactics employed by the attacker to prevent attack.*

Key Words: MANET, OLSR Protocol, Node Isolation Attack, Fictitious Node

1. INTRODUCTION

Usage of mobile devices is tremendously increasing in the present world. Many networks use mobile devices for data exchange. Mobile Ad Hoc Network (MANET) is a type of network that contains a group of mobile devices which exchanges data. Mobile devices are the nodes in MANET. There is no central authority to control the MANET. No predefined infrastructure is defined for MANET. The nodes in MANET exchange messages through intermediate nodes. Each node in a MANET is free to move independently in any direction at any time. The nodes can join and leave the MANET as they wish. Therefore the communication links between the nodes changes frequently. Each node will act as a router because they deal with the forwarding of data of all other nodes in the network. Each device must continuously maintain the information required to properly route traffic. The network may contain multiple numbers of transceivers in between the nodes. This results in a highly dynamic and autonomous topology. Routing protocols is required for message exchange in MANET. There are two wide categorization of routing algorithms used for packet transmission in the network. They are Reactive Protocol and Proactive Protocol. Reactive protocol finds route for message transmission on demand. AODV and DSR are examples of reactive protocols. Proactive protocol is table driven. It maintains a routing table that contains the destinations in the network and the optimal path to the destination. OLSR, DSDV and OSPF are examples of proactive protocols.

1.1 OLSR Protocol

The main requirement of MANET is that all the nodes in the network must recognize each other even in motion. The most widely used routing protocol is OLSR (Optimized Link State Routing) protocol. It is efficient in bandwidth utilization and path calculation. It is a type of proactive protocol. OLSR is the optimization of the classical Link State Routing (LSR) Protocol. It is used to reduce network overhead. Classical Link State Routing Protocol propagates messages by flooding it in the network. This lead to the duplication of messages in the network and thus network overhead is created. In OLSR the duplication and overhead is reduced by selective transmission of data. By the introduction of a concept called Multi Point Relays (MPR) the selective transmission is achieved by OLSR protocol. MPRs are the subset of 1-hop neighbors of a node. Through the MPR, a node can access its 2-hop neighbor. OLSR protocol achieves optimization by appointing minimum number of MPRs for a node. Nodes selected as MPRs are those which has connection with maximum number of 2-hop neighbors. MPRs are the forwarding agents for control packets throughout the network. A node will select an MPR only if it covers all the 2-hop neighbors of the node. The minimal MPR set is the forwarding agent that allows forwarding of control messages and data packets by less duplication and also covering the whole network. Two types of messages are used in OLSR to discover the network topology. They are HELLO message and TC (Topology Control) message. HELLO message will declare a node's knowledge about its surroundings. It list out the 1-hop neighbors of the node. A node broadcast their HELLO message in the network. Other nodes that receive and respond to the HELLO message are the 1-hop neighbors of the sender node. Neighbor nodes know each other by exchanging HELLO messages, which reflect the local connectivity. HELLO messages are used in the selection of the MPR set for routing connectivity. TC message lists out the nodes that had made the sender as their MPR. Nodes maintain the topology based on HELLO and TC messages.

1.2 Node Isolation Attack

OLSR protocol is vulnerable to many types of attacks. Node isolation attack is such an attack that is capable to compromise OLSR protocol. It is a type of Denial of Service (DoS) attack. DoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. In node isolation attack an attacker purposely isolates a victim node from the network. In this attack, the attacker exploits the fact that a node always prefers the minimal set of MPRs. In order to attack the victim the attacker will send a fake HELLO message to the attacker. This HELLO message claims that the sender node is in close proximity to all of the victim's 2-hop neighbours. It also advertises a fictitious node in order to attain the belief of victim. Therefore, according to the MPR selection rules the victim will appoint the attacker as its MPR. Then the attacker will not include the victim in its TC message. And this fraudulent MPR will not forward any messages from the victim to other nodes in the network. Thus the victim will get isolated in the network.

2. DENIAL CONTRADICTIONS WITH FICTITIOUS NODE MECHANISM (DCFM)

DCFM is an efficient mechanism to prevent node isolation attack in OLSR protocol. The very first requirement of DCFM is that each node in the network will only use the information available to it. The node will not rely on any centralized or local trusted authority. In this method the integrity of the HELLO message received from MPRs is checked by the node. Integrity of HELLO message is checked by searching for contradictions in HELLO message with the known topology. Absence of contradiction is a criterion for MPR selection. DCFM assumes that the TC message cannot be spoofed. It means that TC message of the attacker will not be fake. The attacker will not preclude the victim's name from its TC message. It will surely contain the name of the victim. It is because a fake TC message will get contradicted when compared with the legitimate TC message of the victim. This contradiction will disclose the attacker. So other nodes in the network can take preventive measures. But a fake HELLO message gives no chance of suspicion to the victim. It is a more tricky way to isolate a legitimate node. DCFM uses contradiction rules to find out fake HELLO messages. It also employs a fictitious node to pin-point the attacker node. Thereby DCFM use the same trick employed by the attacker to prevent node isolation attack.

Contradiction rules test whether the sender of HELLO message is trustworthy. There are three contradiction rules. If they are satisfied the sender is trustworthy.

The three contradiction rules are :

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 :
   a. Existence of 1-hop neighbors not mentioned in HELLO message
   b. Also, they are located at-least 3-hop away from victim
   c. 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. As per the second contradiction rule, if there is no MPR employed by the attacker to cover the 3-hop neighbors of victim then the malicious node can be caught easily. A table named TC table is referred in order to find out the 3-hop neighbors of the victim that are not mentioned in attacker's fake HELLO message.

2.1 Using Fictitious Node by DCFM

DCFM employs fictitious nodes as the next step of prevention of node isolation attack. Thereby using the same tactic used by the attacker. DCFM employs fictitious nodes for prevention whenever the attacker somehow manages to satisfy the contradiction rules. A legitimate node will declare a fictitious node as its 1-hop neighbor. All other nodes in the network do not know that the newly declared node is unreal. They consider the fictitious node as real. The attacker node also considers it as real. So all other will include the fictitious node in their routing table. And the sole MPR to the fictitious node will be the node who declared it (the victim node). The fictitious node is 3-hop distance away from attacker. Therefore, the attacker is also compelled to accept the victim node as its sole MPR to the fictitious node. This can be verified as impossible through victim's TC message. Thus the attacker's lie can be caught. Addition of fictitious node ensures that there will be at least one 3-hop node included in the fake HELLO message that is to be covered by the attacker using an MPR.

3. RESULT

DCFM is the mechanism used to prevent node isolation attack in OLSR protocol. It exhibits better performance. DCFM employs two stages of prevention mechanism. First stage is the contradiction rules used to select MPRs. Second stage is the declaration of fictitious node by legitimate nodes. This is done when the attacker nodes somehow manages to satisfy the contradiction rules. Using these two features DCFM prevents node isolation attack in OLSR protocol. As the number of nodes increases, the network overhead will decrease in the MANET environment. When DCFM is implemented, for larger networks the number of fictitious nodes, MPRs and TCs will be more. As the node density increases the network overhead decreases. Charts shown below emphasize on the reduction of network overhead when large networks were used.

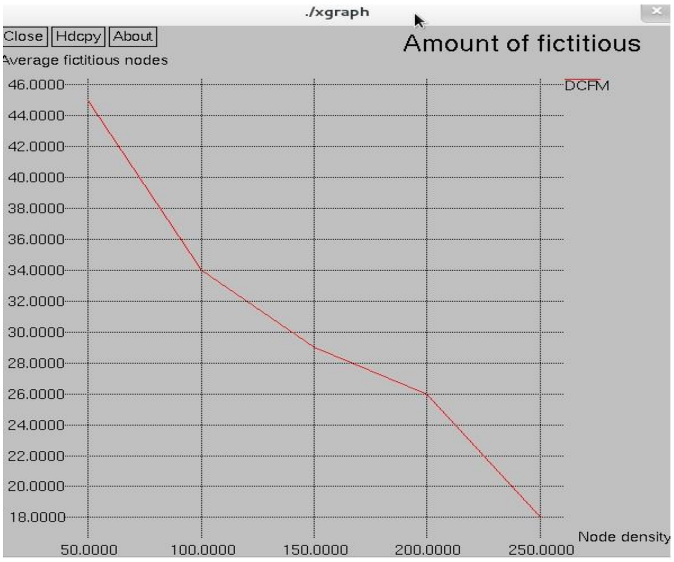

Chart -1: Amount of Fictitious Nodes

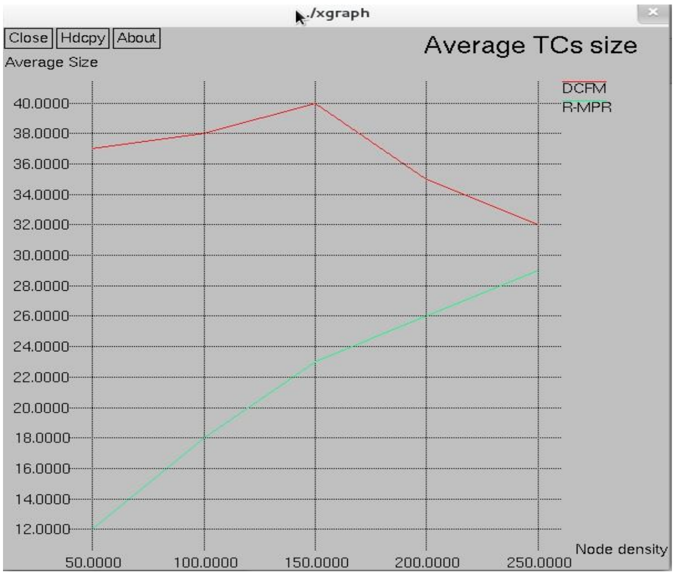

Chart -2: Average TC size

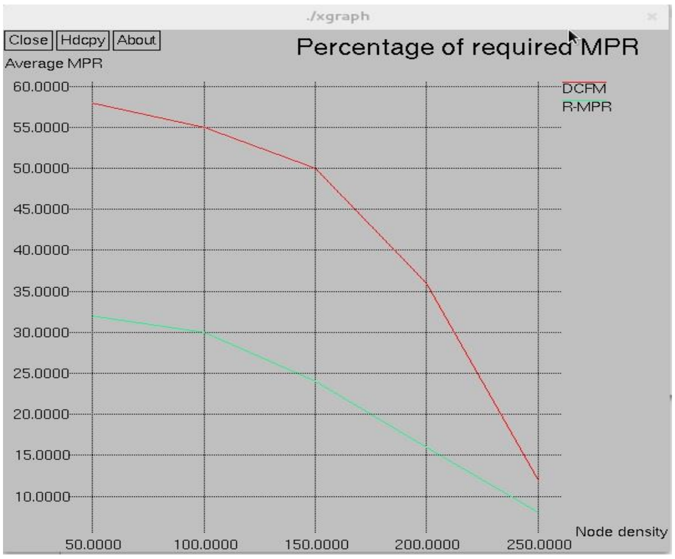

Chart -3: Percentage of required MPR

4. CONCLUSIONS

MANET is a group of mobile devices that communicates wirelessly without any predefined infrastructure and centralized authority. OLSR is the most widely used routing protocol in MANET. But it is vulnerable to many kinds of attacks. This project focuses on preventing node isolation attack; a type of Denial of Service (DoS) attack in OLSR protocol. Denial Contradictions with Fictitious Node Mechanism (DCFM) is the method used to prevent node isolation attack. The DCFM method suggests three contradiction rules to avoid the attack. DCFN mechanism assumes that the attacker will broadcast TC message for sure. Else the attacker will be caught because of the absence of TC message. MPR candidates that do not follow the contradiction rule will be considered as malicious. DCFN also use a fictitious node in order to identify attacker who was somehow able to follow the contradiction rules. Thus DCFM prevent node isolation attack in OLSR protocols.

REFERENCES

[1] Nadav Schweitzer, Ariel Stulman, Member, IEEE, Asaf Shabtai and Roy David Margalit, Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes, 2015.

[2] D. Malik, K. Mahajan, and M. Rizvi, Security for Node Isolation Attack on OLSR by Modifying MPR Selection Process, in Networks Soft Computing (ICNSC), 2014 First International Conference on, Aug 2014, pp. 102–106.

[3] Y. Jeon, T.-H. Kim, Y. Kim, and J. Kim, Attack-Tolerant OLSR Against Link Spoofing, in Proceedings of the 2012 IEEE 37th Conference on Local Computer Networks (LCN 2012), ser. LCN '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 216–219.

[4] B. Kannhavong, H. Nakayama, and A. Jamalipour, Nis01-2: A Collusion Attack Against OLSR-based Mobile ad hoc Networks, in Global Telecommunications Conference, 2006.

[5] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, Securing the OLSR Protocol, in Proceedings of Med-Hoc-Net, 2003, pp. 25–27.

[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, in Computer Networks, 2006 International Symposium on, 2006, pp. 30–35.

[7] M. Marimuthu and I. Krishnamurthi, Enhanced OLSR for Defense Against DoS Attack in ad hoc Networks, Communications and Networks, Journal of, vol. 15, no. 1, pp. 31–37, Feb 2013.