Prevention of Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems

Hicham Zougagh, University Moulay Slimane, Beni Mellal, Morocco
Noureddine Idbourk, University Cadi Ayyad, Marrakesh, Morocco
Rida Zoubairi, University Moulay Slimane, Beni Mellal, Morocco
Rachid El Ayachi, Sultan Moulay Slimane University, Beni Mellal, Morocco

ABSTRACT

In a mobile ad hoc network, a source node must rely on intermediate nodes to forward its packets along multi-hop routes to the destination node. The performance of a mobile ad hoc network is closely related to the capability of the implemented routing protocol to adapt itself to unpredictable changes of topology network and link status. One of these routing protocols is optimized link state routing protocol which assumes that all nodes are trusted. However, in a hostile environment, the OLSR is known to be vulnerable to various kinds of malicious attacks. Without having any control on packet forwarding, an intermediate node can behave selfishly or maliciously to drop packets going through it. Therefore, in this article, the authors propose a new technique for the selection of multipoint relays whose aims to provide each node the ability to select alternative paths in order to reach any destination two hops away.

KEYWORDS

INTRODUCTION

A wireless ad hoc network is a collection of nodes using a wireless medium to communicate, and cooperate together to make possible communication between any pair of nodes, without using any pre-existing infrastructure. In order to enable communication between pair of nodes in such a MANET, a routing protocol is used.

The MANET working group converged on the development of two protocol families: proactive protocols, including the Optimised Link State Routing (Clausen and Jaquet, 2003), reactive protocols; including Ad hoc On-demand Distance Vector routing (David & Johnson & Hu & Maltz, 2007), Dynamic Source Routing (Perkins and Bhagwat, 1994), and Topology dissemination based on reverse-
path forwarding (Ogier & Lewis & Templin, 2004). The main objective of the routing protocol is to discover the network topology to ensure that each node is able to acquire an up-to-date map of the network in order to compute routes. Furthermore, one way to secure a mobile ad hoc network at the network layer is to secure used routing protocols, in order to prevent possible attacks.

OLSR (Clausen and Jaquet, 2003) is a proactive routing protocol for MANET, i.e. all nodes need to maintain a consistent view of the network topology. Thus, they are vulnerable to a number of disruptive attacks in the presence of malicious nodes. Attacks like identity spoofing, link withholding, link spoofing, miserly attack, wormhole attack and Black hole attack. As a result, it is also necessary to provide security schemes for OLSR.

In this paper, we focus on the Black Hole attack in which an intermediate node drops packets passing through it. The motivation of the dropper node is the preservation of its resources, such as its limited battery, while at the same time using the resources of others to deliver its data. In our approach, we present an improved MPR selection algorithm that can reduce the number of malicious nodes trying to be selected as Multipoint Relay by maintaining its Willingness fields equal to Will always.

The remainder of this paper is organized as follows: Section 2 provides a short overview of OLSR, section 3 introduces previous works done in the area, followed by section 4 which presents the attack model. Section 5 describes how our approach copes with the packet droppers, followed by Section 6 where we present simulations results. Finally, we conclude and highlight future directions.

THE PROPOSED PROTOCOL

Optimized link state routing (OLSR) (Clausen and Jaquet, 2003), is one of the most important proactive routing protocols designed for MANET. Each node uses OLSR in order to perform periodic exchange of messages to get information about network topology. The key concept of OLSR is the use of multipoint relay (MPR) to ensure efficient flooding.

To detect its neighbors with whom it has a direct link, each node, at regular intervals (Hello Interval seconds) broadcasts hello messages, containing the list of known neighbors and their link status (symmetric, asymmetric, Multi-Point Relay or Lost). These messages are broadcasted by all nodes and heard only by immediate neighbors; they are never relayed any further, i.e. these packets have a Time-To-Live (TTL) value of 1.

In addition to information about neighbor nodes, periodic exchange of HELLO messages allows each node to maintain information describing each link between neighbor nodes and those who are two hops away. Based on these information’s, each node selects independently its own set of Multi-Point Relay (MPR) among its one-hop neighbors so that the MPR covers all two-hop neighbors.

Topology Control (TC) messages are also broadcasted by MPR-nodes at regular intervals (TC_Interval second). Thus, a TC message contains the list of neighbors that have selected the sender node as a MPR (MPR Selector Set). Furthermore, an Advertized Neighbor Sequence Number (ANSN), is used by nodes in order to verify if information contained in TC messages is up-to-date. TC messages are flooded to all nodes and take advantage of the existence of Multi-Point Relay to reduce the number of retransmissions.

Using information contained in the TC message, a node generates a topology tuples (T\textunderscore des\_adr, T\textunderscore last\_adr, T\textunderscore seq, T\textunderscore time). The set of these tuples is denoted the “Topology Set”. Here T\textunderscore des\_adr is the destination address, T\textunderscore last\_adr is the address of the node that generated the TC message, T\textunderscore seq is a sequence number of the TC message and the T\textunderscore time is the time duration after which the topology tuple expires (Clausen and Jaquet, 2003).

Based on the information in the topology set, the node calculates its routing table. Each entry in the table consists of R\textunderscore des\_adr, R\textunderscore next\_adr, R\textunderscore dist, and R\textunderscore iface\_adr. Such entry specifies that the node identified by R\textunderscore dest\_adr is estimated to be R\textunderscore dist hops away from the local node. It specifies also that the symmetric neighbor node with interface address R\textunderscore next\_adr is the next hop node in the route to R\textunderscore des\_adr, and that this symmetric neighbor node is reached through the local interface
Centrality-Based Connected Dominating Sets for Complex Network Graphs
[www.igi-global.com/article/centrality-based-connected-dominating-sets-for-complex-network-graphs/124036?camid=4v1a](www.igi-global.com/article/centrality-based-connected-dominating-sets-for-complex-network-graphs/124036?camid=4v1a)

A Training Method of Convolution Neural Network for Illumination Robust Pedestrian Detection