A Specification-based Intrusion Detection Model for OLSR

Insha Altaf
Dept. of IT, National Institute of Technology, Srinagar, J&K, India
insha.altaf39@gmail.com

Insha Majeed
Dept. of IT, National Institute of Technology, Srinagar, J&K, India
insha333@gmail.com

Abstract—**In this paper, we in introduce a specification based intrusion detection model for detecting attacks on routing protocols in MANETs. Intrusion detection is a viable approach to enhancing the security of existing computers and networks. Briefly, an intrusion detection system monitors activity in a system or network in order to identify ongoing attacks. Intrusion detection techniques can be classified into anomaly detection, signature-based detection, and specification-based detection. In anomaly detection, activities that deviate from the normal behavior profiles, usually statistical, are flagged as attacks. Signature-based detection matches current activity of a system against a set of attack signatures. Specification-based detection identifies system operations that are different from the correct behavior model. Our specification-based approach analyzes the protocol specification of an ad hoc routing protocol to establish a finite-state-automata (FSA) model that captures the correct behavior of nodes supporting the protocol. Then, we extract constraints on the behavior of nodes from the FSA model. Thus, our approach reduces the intrusion detection problem to monitoring the individual nodes for violation of the constraints. Such monitoring can be performed in a decentralized fashion by cooperative distributed detectors, which allows for scalability. In addition, since the constraints are developed based on the correct behavior, our approach can detect both known and unknown attacks.We choose OLSR (Optimized Link State Routing) [10] as the routing protocol for the current investigation.**

Keywords— Access control, AODV, storage node, Optimized Link State Routing,Topology Control, hop,finite-state-automata,MANET,OLSR.

I. INTRODUCTION TO OLSR

OLSR is a proactive table-driven link-state routing protocol developed by INRIA [10]. The protocol is a refinement of traditional link state protocols employed in wired networks; in the latter, the local link state information is disseminated within the network using broadcast techniques. This flooding effect will consume considerable bandwidth if directly employed in the MANET domain, and therefore, OLSR is designed to optimally disseminate the local link state informationaround the network using a dynamically established sub-network of multipoint relay (MPR) nodes; these are selected from the existing network of nodes in the MANET by the protocol.

OLSR employs two main control messages: Hello messages and Topology Control (TC) messages to disseminate link state information. These messages are periodically broadcast in the MANET in order to establish the routing tables at each node independently. In OLSR, only nodes that have bidirectional (symmetric) links between them can be neighbors. Hello messages contain neighbor lists to allow nodes to exchange neighborinformation, and set up their 1-hop and 2-hop neighbor lists; these are used to calculate multi-point relay (MPR) sets[1].

An MPR set is a 1-hop neighbor subset of a node to be used to reach all 2-hop neighbors of the node. OLSR uses MPR sets to minimize flooding of the periodic control messages. Nodes use Hello messages to announce their MPR sets together with 1-hop neighbor sets. When a node hears its neighbors choosing it as an MPR node, those neighbors are MPR selectors of the node, and the node will announce its MPR selector set to the network by broadcasting TC messages[2].

TC messages are forwarded by MPR nodes to all nodes of the network. When a node receives a TC message, it will note that the originator of TC message is the "last-hop" toward all MPR selectors listed in the TC message. The links are then added into the topology table. Using its topology table, the node can set up its routing table by recursively traversing the (last-hop to node, node) pairs in its topology table (see Figure 1) and picking up the shortest path with the minimal hop count. Therefore, each node of the network can reach all other nodes[3].