Distributed Evidence-driven Message Exchange intrusion detection Model for MANET

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 make two major contributions for intrusiondetectionsystems (IDS) in MANET. First, we propose a practical and effective messageexchangemodel: DistributedEvidence-driven MessageExchangingintrusiondetectionModel (DEMEM) for MANET. DEMEM overcomes the challenges to Distributed IDS architecture of MANET, where detectors do not have sufficient data to detect routingattacks. Instead of adopting costly promiscuous monitoring, detectors in DEMEM simply intercept routingmessages and validate these routingmessages in order to detectroutingattacks. Also, DEMEM segregates the duties of security agents and routing services to avoid modifying the routingprotocols. The efficient Evidence-driven messageexchange mechanism provides sufficient Evidence in order to perform scalable Distributedintrusiondetection at each node.

Second, we integrate DEMEM into a proactiveroutingprotocol in MANET, OptimalLinkStateRouting (OLSR) with four practical assumptions, and three New proposed ID messages specifically for OLSR.The detectionmodel shows that by validating consistency among related routingmessages according to these detectionconstraints, detectors can precisely detect both known and unknown routingattacks in OLSR. We observe that if detectors within two hops can exchange their routing information, they will have sufficient evidence for detectingviolations of constraints. So we propose three ID messages for DEMEM in OLSR to provide the essential ID messageexchange service. ID-Evidencemessages guarantee each detector has sufficient evidence for detecting violations of constraints; ID-Forwardmessages trigger the selected forwarders sending ID-Evidencemessages while the detector observes newevidence in order to minimize messageoverhead, and ID-Request handles message loss. Thus, DEMEM not only performs practical, scalable, and accurate intrusiondetection in OLSR but also tolerates message loss with low messageoverhead.

Keywords— Access control,intrusiondetectionModel AODV, storage node, Optimized Link State Routing,forwarded packetsTopology Control,DEMEM,DRETA,routingpackets, hop.

I. INTRODUCTION TO MANETS

A. THREATS OF MANET

A few studies have been done on the vulnerabilities of MANET protocols [3]. There are two sorts of packets transmitted in a MANET: routingpackets, which are utilized for looking after courses, and datapackets, which are the real information communicated in the middle of source and destination. By and large, a MANET has numerous characteristic properties that make it more defenseless against attacks than wired networks. As a matter of first importance, each node in a MANET capacities as a switch that is in charge of routing and packet conveyance. On the off chance that a node is traded off and misuses the participation among mobilenodes, the entire network will bring about calamities, including inaccurate routingtopology and conveyance disappointments. Second, all nodes in a MANET offer publicchannels in which attackers can undoubtedly focus on any casualty node without going through physical security lines at portals. Third, the topology of a MANET is progressive and eccentric because of mobility. At long last, a MANET is a completely Distributed environment that does not have an approved focal point to accept message rightness. In light of the last two attributes, a malevolent node can send off base routing data to its encompassing nodes to bring about routing disappointments without being seen by others. In planning protocols, accepting that each node will send amend messages and that each node is collaborating to forward right messages makes a MANET vulnerable to attacks. It is evident that a degenerate node can without much of a stretch endeavor these presumptions to break the collaboration of all nodes [1].