# A Specification-based Intrusion Detection Model for AODV

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

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

**Abstract--This paper describes the first specification based approach applying on intrusiondetection in mobile ad hoc networks. In particular, we employ specification-based techniques to monitor the ad hoc on-demand distancevector (AODV) routingprotocol, a widely adopted ad hoc routingprotocol.A mobile ad hoc Network (MANET) is a mobile mesh network in which mobile wireless nodes are both hosts and routers so they can communicate without base stations. Because of this cooperative routing capability, MANETs have envisioned for military and emergency communication, but become more vulnerable to routingattacks than wired networks. If a malicious node propagates forged routing information in a MANET, the node can easily paralyze the network or hijack valuable routes. Due to MANET's particular routing characteristics, defending routingattacks is challenging and critical in MANET. Traditional cryptographic authentication schemes are not sufficient due to insider routingattacks. Intrusiondetection systems are ideal for insider attacks, but most of them are designed for wired networks and thus they can neither directly deploy in MANETs nor effectively detect new routingattacks in MANET. So we apply specification based intrusiondetection approach that defines normal behavior of the protected networks to detect new routingattacks in MANETs. Therefore, we proposed a complete distributed intrusiondetection system that consists of four models for MANETs with formal reasoning and simulation experiments for evaluation.**

***Keywords***— Access control, AODV, storage node, Optimized Link State Routing,Topology Control,RREP, RERR, Hop Count.

## I. INTRODUCTION

AODV is a reactive and statelessroutingprotocol that builds up routes just as craved by the sourcenode. AODV is powerless against different sorts of attacks [2]. This paper examines a portion of the vulnerabilities, particularly talking about attacks against AODV that control the routingmessages. We propose an answer in light of the detail based intrusiondetectiontechnique to identify attacks on AODV. Quickly, this methodology includes the utilization of finitestatemachines for determining right AODV routing conduct and disseminated networkmonitors for distinguishing run-time infringement of the details. Also, one extra field in the protocolmessage is proposed to empower the monitoring. We show that our calculation, which utilizes a treedatastructure and a node shading plan, can successfully identify the greater part of the genuine attacks in realtime and with minimumoverhead. This work is the primary push to apply particular based detectiontechnique to identify attacks in ad hoc network that control routingmessages to accomplish the attack objective. In this paper, we show the specification of AODV that portrays the substantial stream of AODV routingmessages. In addition, distributednetworkmonitors are utilized to monitor whether the nodes fit in with the determination [1].

## II. VULNERABILITIES IN AODV

AODV is powerless against a wide range of sorts of attacks [8]. In this area, we inspect particular vulnerabilities in AODV that permit subversion of routes. What's more, we give a few attack situations that adventure the vulnerabilities to rouse our exploration [2].

### A. OVERVIEW OF AODV

The Ad hoc On-interest DistanceVector (AODV) routingprotocol is a reactive and statelessprotocol that builds up routes just as coveted by a sourcenode utilizing RouteRequest (RREQ) and RouteReply (RREP) messages. At the point when a node needs to discover a route to a destinationnode, it telecasts a Routerequest (RREQ) message with an interesting RREQ ID (RID) to every one of its neighbors. At the point when a node gets a RREQ message, it redesigns the sequencenumber of the sourcenode and sets up converse routes to the sourcenode in the routingtables. In the event that the node is the destination or the node has a route to the destination that meet the freshness necessity, it unicasts a routereply (RREP) back to the sourcenode [3].