International Conference on Machine Learning and Computational Intelligence-2017
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 7 | ISSN : 2456-3307

An Intrusion Detection System for MANETS

Insha Majeed, Sakshi Arora
Department of Computer Science Engineering Shri Mata Vaishno Devi University Katra, Jammu and Kashmir, India

ABSTRACT

Mobile Ad hoc Networks (MANETs) are very important and unique applications as they does not require a fixed network infrastructure and moreover both works of transmitter and a receiver are done by single node. Nodes are able to communicate directly with each other or through their neighbours to relay messages. MANETs can be envisioned for military and emergency communication due to their capability of cooperative routing but are also more vulnerable to routing attacks than wired networks. Thus it is imperative to develop an efficient intrusion-detection mechanisms to protect MANETs. To detect new routing attacks in MANETs we have applied specification based intrusion detection approach that defines normal behaviour of the protected networks. In this paper, we propose a complete distributed intrusion detection system that consists of four models for MANETs with formal reasoning and simulation experiments for evaluation. Optimal Link State Routing (OLSR) is representative of a proactive, link-state routing protocol of MANETs, and the Ad Hoc On Demand Distance Vector (AODV) is the other popular, reactive, request-on- demand routing protocol. Both OLSR and AODV have IETF RFCs.

Keywords : AODV, Topology Control, RREP, RERR, hop, OLSR, DEMEM, DRETA.

I. INTRODUCTION

A. Mobile Adhoc Network

MANET is a set of wireless mobile nodes with no pre-established infrastructure. They can be applied to various popular wireless technologies including cellular phone services, disaster relief, emergency services, battlefield scenarios, and other applications because MANETs have mobile nodes with reliable routing services. Moreover, MANETs are decentralized networks with unpredictable network topology because of node mobility. Because of decentralisation nature all mobile nodes need to discover the dynamic topology and deliver messages by themselves and mobile nodes in MANETs act as both hosts and routers. The mobile nodes set up the routing tables by exchanging routing messages with each other and then deliver data packets for others. The most fundamental and critical issue related to MANETs is to develop a system to maintain routing tables reliably. The dynamic nature and cooperativeness of MANETs presents extensive challenges for network security.

B. Vulnerabilities in MANET

Because of the characteristics discussed above network-based access control mechanisms such as firewalls cannot be directly implemented as they do not have well defined boundary and make MANETs more vulnerable than normal wireless networks with base stations. A MANET is trust-all-peers design assuming every node to provide accurate routing information and acts as a router to cooperatively forward packets. Ad hoc networks are vulnerable to several routing attacks: address spoofing, black hole,

man-in- the-middle, modification of packets, and distributed denial-of- service (DDoS).

C. Cryptographic Approaches in Securing MANET

Largely research about securing MANET routing protocols use cryptographic approaches based on public key infrastructure (PKI). For example, ARAN[37] and SAODV[42] apply PKI on AODV to generate digital signature to protect the integrity of its routing messages. A secure OLSR protocol also uses digital signature to guard OLSR routing messages. PKI is also applied to protect other routing protocols of MANETs. The cryptographic approaches do not cover up critical fields, for example hop count, the value of which will change over time. Another limitation is that they cannot prevent insider attacks. Therefore, some other mechanism has to be developed to set off the limitations of cryptographic approaches, and develop the Intrusion Detection to secure MANET routing.

D. New challenges of IDS in MANET

MANET with such features and limitations poses difficult challenges in developing IDS for MANET as compared in wired networks. First, the characteristic of nodes tobe honest and cooperative can be advantageous for malicious node to launch many routing attacks. Second, thedistributed network without centralized admin in MANET, the IDS will not detect the routing attacks if all distributed detectors does not have monitoring information from others. Third, the detectors will require up-to- date evidence in real-time to detect the attacks with low false positive and negative rates but is difficult due to highly dynamic and unpredictable mobility. The attacks can propagate and paralyze the network quickly due to the lack of trust management between nodes.

E. Contributions

Our proposed Intrusion Detection System (IDS) detects insider attacks on MANET routing protocols, and it is the first complete IDS with several innovative models including two intrusion detection models, a message exchange model, and an authentication model. This effectual ID system can overcome the challenges discussed above and adapt to the unique MANET environment with low message and computation overhead. We apply a specification based detection approach to correctly detect routing attacks that contravene detection constraints. The constraints define the normal behaviours of the target routing protocol and violations of these constraints are potential routing attacks. The distributed detectors use these constraints to detect corrupt routing messages, causing the violations, and then correct the corrupt message contents to stop the attacks. MANET nodes generally have less computational power and bandwidth. MANET is very susceptible to message overhead generated by IDS. First, we put forward two specification-based intrusion detection models for two representative routing protocols: OLSR and AODV. Then we propose distributed intrusion detection models to improve the first two models and make them practical and scalable.

II. RELATED WORKS

A. Introduction

Security mechanisms, like authentication services and access control cannot alone deter all possible attacks such as insider attacker. Therefore we need the security mechanisms which can deal with bad insider nodes possessing valid key and access rights. Intrusion detection provides second line of defense.The routing works for MANETs can be characterized as: first category is based on authentication-based approaches such as Authenticated Routing for Ad-Hoc Networks (ARAN)[37], Ariadne[17], and Secure AODV[42]. The work in second category are IDSes targeted at mobile ad hoc networks like MANET IDS framework,

statistical anomaly based IDS for detecting insider attacks, and security analysis for selected protocols. The last category is malicious packet dropping detection. MANET needs to detect selfish nodes and enforce cooperative participation as routing services require cooperation among all nodes. In this category, either statistical or reputation-based approaches are used.

B. Authentication Approaches

The cryptographic approaches [17][2][42] [37][31][41] proposes authentication protocols for controlling the routing data message exchange in several protocols. Authenticated Routing for Ad-Hoc Networks (ARAN)[37] assume that each node has its own public and private key distributed by a trusted server. Zapata and Asokan[42] proposed Secure AODV, which uses asymmetric cryptography to secure the AODV routing protocol. To prevent replay attacks Adjih[4] proposed a secure OLSR protocol which uses a signed time stamp to validate the freshness of a message. Papadimitratos and Haas has proposed a secure link state routing for mobile ad hoc networks[31]. These works use public key based signatures to keep the header readable and to protect routing message header from being modified. Adrian Perrig proposed TESLA[2] which is a symmetric key based broadcast authentication protocol. Hu proposed Ariadne[17], more secure version of Dynamic Source Routing (DSR), which applied TESLA to reduce computation overhead.

C. IDS Approaches in Mobile Ad-hoc Net-works

Distributed cooperative IDSs are proposed for MANETs to determine the lack of central authority. Zhang and Lee[43] proposed first integrated IDS architecture in 2000. For statistical anomaly detection Huang and Lee[6] in 2003, presented a cooperative cluster-based architecture. Sterne [11] presented a cooperative intrusion detection architecture for addressing the challenges in MANET. For misuse detection within MANETs Subhadhrabandhu[12] evaluated several selection strategies for placement of IDS modles. Ramanujan[34] presented a system which can detect, avoid, as well as recover from malicious attacks. Based on mobile agent technology Kachirski and Guha[3] describes a wireless IDS. An IDS approach based on a stateful analysis of AODV control packet streams was employed by Gwalami[14]. This approach applies State Transition Analysis Technique (STAT) [19], Peng Ning and Kun Sun[28] presented an examination of insider attacks in the AODV protocol.

Several IDS approaches are proposed for detecting malicious packet dropping for MANETs (i.e. both routing and data packets). [8][9][26][27] used the method of assigning a value to the “reputation” of a node and using this information to hoe out misbehaving nodes and use only trusted and verifiably fine nodes. [7] and [36] are credit and statistics-based approaches to solve packet dropping problems in MANET respectively. To find out whether nodes are not forwarding packets at the desired rate because of congestion or because of malicious behaviour a statistical approach is presented by Rao and Kesidis in [35] using estimated congestion at intermediate nodes.

D. Specification based Intrusion Detection Systems

In wired network Intrusion detection systems have imployed two models: anomaly based and signature based approaches. A signature-based IDS[19][25] can monitor activities on the network and then compares those with known attacks. An anomaly based IDS [6][7][36][43][5] can monitor the network traffic and compare it with normal behaviour patterns statistically. A new approach ideal for new environments, such as MANETs is the specification based approach. A specification based IDS detects attacks (including known and unknown) according to normal behavors of protected services, such as routing services in MANETs. To do this, the IDS first analyzes the protected protocol specification, and

introduces vulnerabilities of the protocol, including useful descriptions of exploits in the protocol. Second, the IDS provides detection rules to enforce the protocol normal behavior. Since malicious nodes have limited known attack methods to take advantage of protocol vulnerabilities, their attacks will cause the violations of the rules and be detected. Thus, the specification based IDS can achieve much lower false positives and negative than those by an anomaly based IDS. And the specification based IDS is able to detect new or unknown attacks which a signature based cannot detect.

III. A SPECIFICATION-BASED INTRUSION DETECTION MODEL FOR AODV

A.Introduction

AODV, a reflex and stateless routing protocol, builds up routes when wanted by the source node is helpless against different sorts of attacks [28]. The determination based intrusion detection procedure is proposed to identify attacks on AODV. The approach utilizes the limited state machines to determine AODV routing conduct and distributed network screens for recognizing run-time infringement of the details. One extra field called sequence number in the protocol message is proposed to empower the checking. In our calculation, we utilize a tree information structure and a node shading which successfully recognizes the genuine attacks continuously, with least overhead.

B. Overview of AODV

AODV builds up routes on demand by a source node utilizing Route Request (RREQ) and Route Reply (RREP) messages. Route Request (RREQ) message has RREQ ID (RID) that is broadcast by a node to discover a route to its destination . Turn around route to the source node in the routing tables is set up and sequence number is refreshed by a node when it gets RREQ message. A route answer (RREP) is unicast back to the source node when the node is the destination or the node has a route to the destination that meet the freshness necessity. The sequence number (SN) in AODV tells about freshness of the routing data and furthermore ensures circle free routes. Sequence number can be expanded just under two conditions: 1.when RREQ is broadcast by the source node and 2. the destination node answer with a RREP. The hop count (HC) is incremented by 1when a message(RREQ or RREP) is forwarded each hop. Route blunder packets (RERR) are spread to the start node along the turn around route when a link is broken, and all other nodes will drop the section in their routing tables. Figure 3.1 shows how Aodv works.The estimations of the fields in the routing messages are signified in Table3.1.

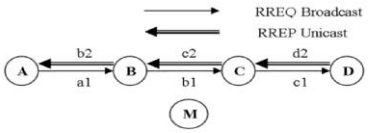

Figure 3.1. AODV state

Table 1. RREQ and RREP values

Type	RREQ			RREP		
Msg	a1	b1	c1	d2	c2	b2
IP.Src	A	B	C	D	C	B
IP.Dst	255	255	255	C	B	A
HC	0	1	2	0	1	2
AODV.Dst	D			D		
SN.Dst	0 (Unknown)			61		
AODV.Src	A			A		
SN.Src	100					
RREQ ID	20					

C. The vulnerable Fields for AODV Control Messages

AODV is proficient and adaptable as far as network performance, yet it enables attackers to effortlessly publicize misrepresented route data to divert routes and to dispatch different sorts of attacks. In each AODV routing packet, some basic fields, for example, hop count, sequence numbers of source and destination, RREQ ID, IP headers and additionally IP locations of AODV source and destination,are fundamental to redress protocol execution. Any abuse of these fields can make AODV malfunction. Table 2 shows defenseless fields in AODV routing messages and the impacts when they are altered.

Table 2. Aodv fields

Field	Modifications
RREQ ID	Increase to create a new RREQ request.
Hop Count	If sequence number is the same, decrease it to update other nodes' forwarding tables, or increase it to invalidate the update.
IP Headers as well as AODV Source and Destination IP Addresses	Replace it with another or invalid IP address.
Sequence Number of Source and Destination	Increase it to update other nodes' forward route tables, or decrease it to suppress its update.

Some of the attacks are underneath:

- ✓ Single Attacks are:Forging Sequence Number,Forging Hop Count
- ✓ Examples of Aggregated Attacks

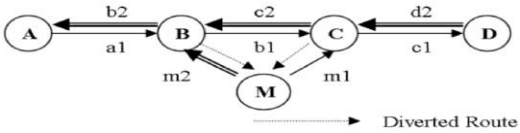

Figure 3.2. Man in the Middle Attack

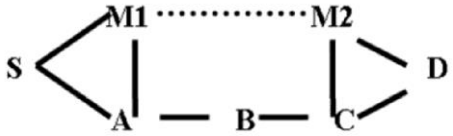

Figure 3.3. Tunnelling Attack

D. Specification-based Monitoring of AODV

Specification-basd observing contrasts the conduct of items and their related security specifications that catch the right conduct. Specification-based detection does not recognize intrusions specifically - it identifies the impact of the intrusions as run-time infringement of the specifications. The specification-based detection approach has been effectively connected to screen security-basic projects [23], applications, and protocols[22].

1. Assumptions

We utilized the accompanying suppositions:

1. MAC locations and IP locations of all versatile nodes are enrolled and authenticated with the network screens.
2. Network screens can cover all nodes and play out all required functionality.
3. Every network screen are dependable and can simply convey safely and dependably.
4. Every node neither drops AODV messages nor sticking remote channels.

2. The Finite state Machine Constraints

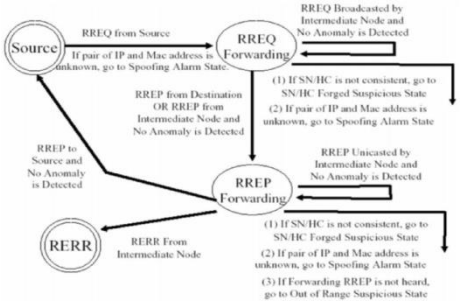

Figure 3.4. Normal State Diagram

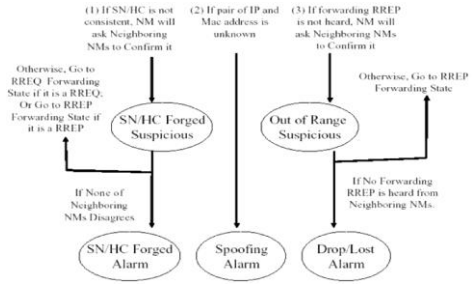

Figure 3.5. Alarm and Suspicious State Diagram

IV. A SPECIFICATION-BASED INTRUSION DETECTION MODEL FOR OLSR

Optimized Link State Routing (OLSR) is a proactive table-driven routing protocol created by INRIA [10]. The protocol is a refinement of conventional link state protocols utilized in wired networks; in the last mentioned, the neighborhood link state data is spread inside the network utilizing broadcast strategies. This flooding impact will devour impressive data transmission if specifically utilized in the MANET area, and in this way, OLSR is intended to ideally disperse the nearby link state data around the network utilizing a progressively settled sub-network of multipoint transfer (MPR) nodes; these are chosen from the current network of nodes in the MANET by the protocol. OLSR utilizes two principle control messages: Hello messages and Topology Control (TC)

messages to disperse link state data. These messages are intermittently broadcast in the MANET keeping in mind the end goal to build up the routing tables at each node freely. In OLSR, just nodes that have bidirectional (symmetric) links between them can be neighbors. Hi messages contain neighbor records to permit nodes to exchange neighbor data, and set up their 1-hop and 2-hop neighbor records; these are utilized to compute multi-point hand-off (MPR) sets.

Figure 4.1. A route from Topology Table

Table 4.1. Hello and TC Messages' Critical fields

Message Type	Critical fields
Hello Message	1-hop neighbor list MPR sets
TC Message	MPR selectors Advertised neighbor sequence number (ANSN)

A. OLSR Vulnerabilities and Attacks

A few examinations have been done on the vulnerabilities of OLSR [15][4]. When all is said in done, an attacker can manufacture packets, block and adjust packets experiencing it, or decline to forward packets, causing bargains of confidentiality, integrity, and avaixlability. In this work, we just concentrate on those vulnerabilities that could trade off the integrity of the network, i.e., the routing tables in the nodes. In OLSR, each node infuses topological data into the network through HELLO messages and TC messages. In this way, a malevolent node can infuse invalid HELLO and TC messages to disturb the network integrity, making packets route inaccurately or to the benefit of the attacks.

Table 4.1 showcases the basic fields in the TC message and the Hello message on which the calculation of the routing table depend. The 1-hop neighbour list in Hello message is utilized by its neighbour to make the 2-hop neighbor rundown an MPR set. The sender's MPR set is MPR sets in hello message. The MPR selector in TC message is utilized as a part of figuring routing tables at nodes accepting the messages.

In this manner, an attack can:

1) provide an off base 1-hop neighbor list in a Hello message
2) provide an off base MPR set in a Hello message
3) provide off base MPR selectors in a TC message
4) modify the MPR selectors and ANSN before it forwards a TC message

B. Intrusion Detection Model

Here we portray our specification-based way to deal with recognizing OLSR attacks. Specification-based detection is especially reasonable for identifying attacks on network protocols on the grounds that the right conduct of a protocol is generally very much characterized and is archived in the protocols specification. Utilizing network observing, test is to separate a reasonable modal of conduct from the protocol specification; can be checked at runtime. We initially list suppositions utilized, & after that presents the right conduct modal of OLSR under these presumptions.

C. Assumptions

We expect a distributed ID design which permits helpful detectors to wantonly screen the Hello and TC messages, and also exchange their neighborhood information when important. IDS detectors in this design can screen all Hello and TC messages sent by each node of the network, dependably exchange IDS information effectively, and won't be traded off. We accept OLSR is the main routing protocol in the network and each node has just a single network interface.

D. Correct Behavior Model of OLSR

Figure 4.2 demonstrates the FSA model of the OLSR protocol that characterizes the right operation of an OLSR node in dealing with control activity. At this

point when node gets a Hello control message, it will refresh its neighbors rundown and MPR set. A node refreshes the topology and routing table when it accepts the Topology Control message. What's more, the node will forward the TC on the off chance that it is an MPR node. Also, a node will occasionally broadcast Hello and TC messages.

We depict the requirements on the control activity between neighbor nodes for identifying irregularities inside the control messages.

1. Neighbor's record in Hello message must be complementary. E.g., if node 2 is the neighbor of node 1, at that point node 1 must be node 2's neighbor.
2. The MPR nodes of a nodeshould achieve each of the 2-hop neighbors of the node & the MPR nodes are to transmit TC messages intermittently.
3. MPR sets of Hello messages must match relating MPR selectors of a TC message. E.g., if node 2 is node 1's MPR selector, node 1 must be node 2's MPR.
4. Forwarded TC message's Integrity must be kept up.

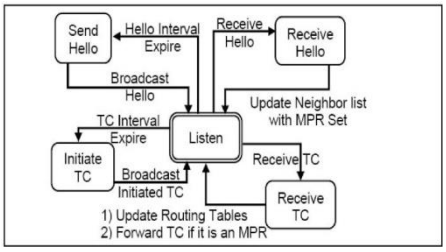

Figure 4.2. Routing Finite State Automata (FSA) for OLSR

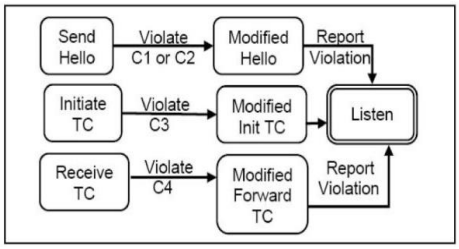

Figure 4.3. Finite State Automata for Security Specification

At the point when an OLSR control messages abuse any of the limitations, the FSA goesfrom an ordinary state to some caution states (Modified Init TC State, Modified Forward TC State, Modified Hello State).

Figure 4.3 (an expansion of FSA in Figure 4.2) delineates FSA utilized by the specification-based intrusion detection system.

E. Temporary Inconsistency

When the topology changes links are made or evacuated so temporary violation of imperatives C1, C2 and C3 may happen in a brief timeframe. To maintain a strategic distance from false cautions, the detector is tosit tight for the two nodes on the two sides of a link to take in the new link status before declaring an irregularity as attack. Also, when a link between node An and node B is made, node A refreshs the status of A-B link and sends Hello message, isn't predictable with past Hello message of node B. Again the detector is to sit tight for B to get new Hello message from An and send another Hello message mirroring the expansion of link A-B.

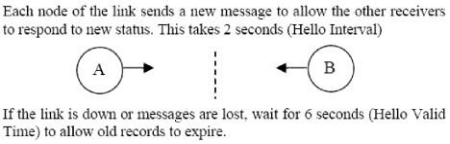

Figure 4.4. Resolving temporary inconsistency

Table 4.2. Important Parameters for Temporary Inconsistency

Constraint Alert thresholds		OLSR Default Parameters	
C1 (1-hop neighbors)	12 sec	Hello message sending interval	2 sec
C2 (2-hop neighbor vs MPR)	12 sec	Hello message valid time	6 sec
C3 (MPR vs MPR selector)	15 sec	TC message sending interval	5 sec
C4 (Forwarded TC)	0 sec	TC message valid time	15 sec

F. Limitations

For a solitary attack or non-related attacks, the model can identify all attacks since we catch all conceivable approaches to change a solitary message at once. Be that as it may, if at least two attackers dispatch an associated attack in which inaccurate data is provided to various nodes reliably, the limitations will be

unable to distinguish it. For instance,when attackers claim to be neighbours but are not there might not be distinguishable infringement.

G. OLSR Detection Model's Analysis

Here we dissect the OLSR protocol & the proposed detection model to demonstrate that the arrangement of limitations C1 — C4 can distinguish attacks in MANET.

Table 4.3 depicts the procedure for building up the routing table from the point of view of a node.

Table 4.3. OLSR Routing Table Establishment

1. Exchange 1-hop neighbor lists by Hello messages
2. Establish 2-hop neighbor lists by 1-hop lists
3. Generate MPR sets by 2-hop neighbor lists and announce them with Hello messages
4. MPR nodes generate TC messages advertising the nodes (MPR selectors) that can be reached by the MPR nodes.
5. MPR nodes forward TC messages so that they will reach all nodes in the network.
6. Generate topology and routing tables from MPR selector sets

As indicated by the RFC [10] (OLSR protocol), every node keeps up a topology a link set, utilized for figuring of route table. The link set has the link data of its 1-hop neighbor, developed from the Hello messages it gets. The topology has topology tuples as T[HoldingTime], T[DestAddr], T[LastHopAddr], T[Seq], which demonstrate that we can achieve T[DestAddr] through T[LastHopAddr]. A topology set is built from TC messages a node gets. The node processes the route table from its topology and link set.

Lemma 1: Under suppositions in D, all great nodes will have a right link set if imperative C1 holds.

Lemma 2: The MPR selector field of a TC message created by a MPR node must be right if limitation C3 holds.

Lemma 3: The MPR selector fields of all TC messages must be right if requirements C3 and C! Hold.

Lemma 4: For a node x, which is a n-hop neighbor of an alternate node y, x will get TC messages of y with n-1 forwarding if C2 holds.

V. DEMEM: DISTRIBUTED EVIDENCE-DRIVEN MESSAGE EXCHANGE INTRUSION DETECTION MODEL FOR MANET

A. Introduction

In this segment, we make two noteworthy commitments for intrusion detection systems (IDS) in MANET. To start with, we propose a handy and viable message exchange model: Distributed Evidence-driven Message Exchanging intrusion detection Model (DEMEM) for MANET.

DEMEM beats the difficulties to distributed IDS engineering of MANET(as depicted in segment 3 and 4), where detectors don't have adequate information to identify routing attacks. Rather than receiving expensive wanton observing, detectors in DEMEM just capture routing messages and approve these routing messages keeping in mind the end goal to identify routing attacks. Additionally, DEMEM isolates the obligations of security specialists and routing administrations to abstain from changing the routing protocols. Second, we coordinate DEMEM into a proactive routing protocol in MANET, OLSR (Optimal Link State Routing) [10]. DEMEM in OLSR utilizes detection requirements talked about in segment 4 [39]. The detection model demonstrates that by approving consistency among related routing messages as indicated by these detection imperatives, detectors can definitely distinguish both known and obscure routing attacks in OLSR. Three ID messages for DEMEM in OLSR are proposedto give the basic ID message exchange benefit, which is the fundamental suspicions of past detection models in area 3 and 4. ID-Evidence messages ensure each detector has adequate evidence for identifying infringement of limitations; ID-Forward messages trigger the chose forwarders sending ID-Evidence messages while the detector watches new evidence so as to limit message overhead, and ID-Request handles message misfortune. Along these lines, DEMEM not just performs down to earth, scalaxble, and exact

intrusion detection in OLSR yet additionally endures message misfortune with low message overhead.

B. Distributed Evidence-driven Message Exchange intrusion detection Model

DEMEM is a strong, adaptable, and low message exchange overhead intrusion detection model for MANET. DEMEM beats the difficulties said in area A through the accompanying three principle includes: a distributed engineering, an intrusion detection layer, and an evidence-driven message exchange system.

C. Distributed IDS Architecture

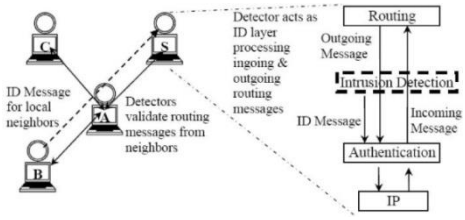

Figure 5.1. Architecture of DEMEM

DEMEM gets adjusted to the distributed and helpful behavior of MANETs. Each DEMEM node goes about as a detector screens its 1-hop neighbors by approving route messages it gets for intrusion detection purposes. So that, when a node sends a routing message, the majority of its neighbours approve the accuracy of the message. As found in Figure 5.2, node A is detector and screens nodes B, C, and S and similarly nodes B, C, and S are detectors that screen other nodes. Notwithstanding checking exercises inbetween 1-hop neighbors, 2-hop neighbors will need to exchange their watched data by customized ID (Intrusion Detection) messages to accumulate enough evidence for detection purposes. This approach takes out confounded topology upkeep and costly questionable want on observing required by progressive agreebable intruzion detection [43].

D.DEMEM in OLSR

1.Routing Attack Methods in OLSR

A proactive routing protocol (OLSR)uses periodic Hello and Topology Control (TC) messages to set up a total network topology. OLSR gives a hearty and finish routing topology and endures message misfortune caused by portability and clamor.

OLSR, the calculation of routing tables relies upon three basic fields in Hello and TC messages: 1-hop neighbors and MPRs in Hello message and also MPR selectors in TC messages. A node can send three sorts of essential OLSR messages: Hello, started TC, and forward TC messages. In this way, an attacker has four attack techniques against OLSR routing:

1. Forging 1-hop neighbors in a started Hello;
2. Forging MPRs in a started Hello;
3. Forging MPR selectors in a started TC; and
4. Forging MPR selectors in a forwarded TC.

The initial three attack strategies have a place with the main sort of attack model, and the fourth one has a place with the second kind of attack model.

2. Specification-based Intrusion Detection

In MANET, nodes sharing incomplete topology data and covered topology data from their routing packets must be steady. Despite the fact that it is hard to identify attacks propelled by forging started routing packets, substance of these fashioned packets won't be predictable with veritable routing packets that have covering routing data. In this way, the detector can recognize these fashioned packets by approving consistency among related routing messages. The specification-based intrusion detection model [39] in area 3 portrays four requirements (see Figure 5.2) to approve the rightness of Hello and TC messages in OLSR.

First constraint (C1)	Neighbors in Hello messages must be reciprocal
Second constraint (C2)	MPRs must reach all 2-hop neighbors
Third constraint (C3)	MPR selectors must match corresponding MPRs
Fourth constraint (C4)	Fidelity of forwarded TC messages must be maintained

Figure 5.2. 4 detection constraints

DEMEM helps the model [39] resolve this assumption with a practical message exchange technique.

3. Implementing DEMEM in OLSR

To make the model in segment 4 down to earth and successful, three Intrusion Detection (ID) messages are made for OLSR i.e, ID-Evidence, ID-Forward, and ID-Request messages. We additionally exhibit the components for taking care of three ID messages, particularly inside the Evidence Manager and the Forwarding Manager.

E.DEMEM FSM for OLSR

In OLSR, the Evidence Manager handles ID-Evidence, Hello and TC messages and records evidence in these messages. A Forwarding Manager can send three ID messages under three conditions appeared in Figure 5.4. The Validation Manager approves Hello and TC messages in view of the three limitations & related evidence from the Evidence Manager. In the event that the Validation Manager recognizes message irregularities that damage these requirements and the enduring time of irregularities surpasses the caution limits of the limitations, the Response Manager will perform legitimate attack recuperation.

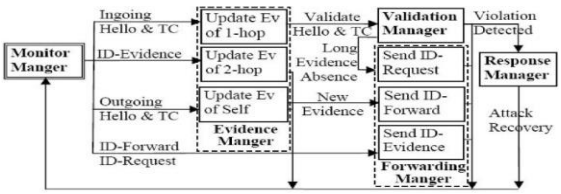

Figure 5.3. FSM within a DEMEM detector

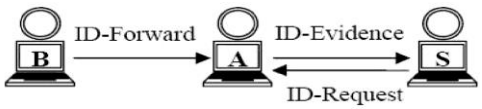

Figure 5.4. ID messages

Forwarding Manager: When the Validation Manager doesn't have adequate evidence fron a normal ID-Evidence message, it accept that the message is lost. The Validation Manager triggers the Forwarding manager to broadcast an ID-Request message to ask for the lost ID-Evidence message. Also the Forwarding Manager broadcasts an ID-Forward message when new evidence is sensed by Evidence manager in Hello message. And the Forwarding Manager broadcasts an ID-Evidence message for the neighbor when it gets message from the neighbors.

4 commonsense presumptions in light of existing works:

1. OLSR is the routing protocol and each node has one network interface. Various Message Interface Declaration (MID) and Host and Network Association (HNA) messages are not utilized here.
2. The substance of forwarded routing messages and the node personality in all routing and ID messages are authenticated by DRETA in part 6. In this manner, Constraint 4 of every 2 used to distinguish attack technique 4 out of 5.4.1 is secured here.
3. No deliberate packet dropping. A few trustworthy strategies [7][36] have been created for distinguishing ordinary unicast information packet drop attacks and also to broadcasting routing messages. We expect that detectors have been used to recognize purposefully packet dropping. DEMEM can likewise endure ordinary packet misfortune or drop.
4. No plotting attackers. Plotting attacks can make virtual links to perform worm-opening attacks. A few works [17] address this kind of attack. Likewise, included virtual links don't influence the presence of other ordinary routing links.

VI. DISTRIBUTED ROUTING EVIDENCE TRACING AND AUTHENTICATION INTRUSION DETECTION MODEL FOR MANET (DRETA)

A. Introduction

We propose the utilization of the DRETA (Distributed Routing Message Tracing and Authentication intrusion detection) model to give an effective and low-overhead insurance. DRETA has a distributed engineering, a detector in every node to screen and approve route messages. Isolated from the network layer, DRETA has a free layer, to block routing messages. Symmetric keys requiring much lower calculation overhead than public keys are utilised by DRETA, to give authentication administrations to all routing message. DRETA receives one-way key chain[16] and delay key disclosure[2] procedures for symmetric keys to be distributed in public channels like Public Key Infrastructure (PKI) does. Validation Messages (VMs), which utilize HMAC[24] are proposed for the integrity of forwarded messages.

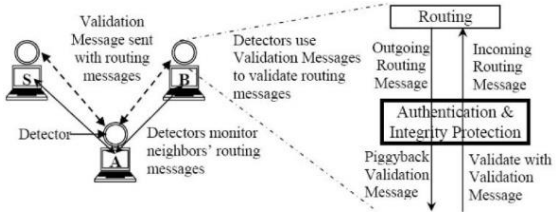

Figure 6.1. Validation Messages and Distributed detectors used to validate routing messages

We have implemented DRETA on two representative routing protocols i.e, OLSR and AODV. DRETA can protect the forwarded TC messages in OLSR and forwarded ID-Evidence messages in DEMEM.

B. Background

In section 2 and 3, we have introduced the Optimized Link State Routing protocol (OLSR)[10] and Ad-hoc On-demand Distance Vector routing protocol (AODV)[32] two representatives of proactive and on-demand routing protocols of MANET. We introduce one-way key chain[16] and delay key disclosure[2] techniques, which are adopted by DRETA.

2. Finite State Machine for DRETA

R'Msg: Forwarded Outgoing Routing Message(Sender is Not Originator)Ro Msg: Originated Outgoing Routing Message(Sender is Originator)

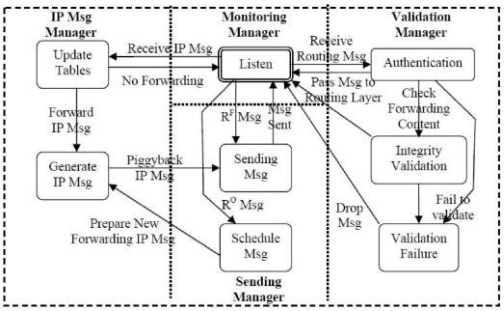

Figure 6.2. Finite State Machine within a node with DRETA

DRETA Implementations

Here we talk about executions of DRETA with AODV, OLSR, and DEMEM.

C. DRETA in AODV

DRETA have two security limitations to keep AODV messages from being malevolently changed when they are made (i.e, the msg originator is the noxious node). To begin with, DRETA never permit a middle of the road node to answer to a RREP on the grounds that the halfway node isn't the orignator of RREP. Likewise, the route information of destination in the middle of the road node might be obsolete, and it is troublesome & costly to approve the routng information. Subsequently, it is substantially more secure to just enable the destination to answer a RREP. Second, the nodes overlook Sequence Numbers of the destination in RREQ and RERR on the grounds that the no. may likewise be obsolete and along these lines not reliable.

In case the originator gives wrong data in its AODV message, mistaken data purposes routing harm to the originator itself. If the originator builds its SN an extensive amount, it won't influence AODV

operation. Accordingly, attackers can't profit by malicious started AODV messages. The DRETA can thus secure forwarded AODV messages and also authenticated all AODV messages, DRETA effectively ensures the integrity of Aodv message.

D. DRETA in OLSR

OLSR has two primary routing messages, non-forwarded. DRETA in OLSR gives authentication to all messages:Hello messages and TC messages, and gives forwarded message insurance to TC message. In OLSR, just MPR nodes forward TC messages, so ETM (Evidence Tracing Messages) and KFM (Key Forwarding Messages) are just forwarded by MPR nodes. Subsequently, DRETA secures the forwarded TC messages in OLSR and averts attacks utilizing attack technique 4 in Figure 6.1.

E. DRETA in DEMEM

DEMEM forestalls attacks utilizing one of the initial three attack strategies in Figure 6.1. DRETA authenticates the three ID messages(ID-Evidence, ID-Forward, and ID-Request). Since the ID-Evidence message is a forwarded message, DRETA secures the integrity of the ID-Evidence message. In this way, DRETA and DEMEM agreeably guarantee the integrity of the routing messages in OLSR.

F. Experiment

We executed DRETA in GloMoSim, a reenactment intended for MANETs.

1. Experiment condition

GloMoSim bolsters 802.11, different routing protocols in MANETs, (for example, AODV and OLSR), and Ground Reflection (Two-Ray) radio model.DRETA utilizes the SHA-1 hash function to produce MACs and HMACs. The hash value estimate is 10 bytes and the key measure is 8 bytes. The key terminate time is 1 second.

2. Performance Metrics

We characterize three performance measurements to gauge DRETA's overhead:

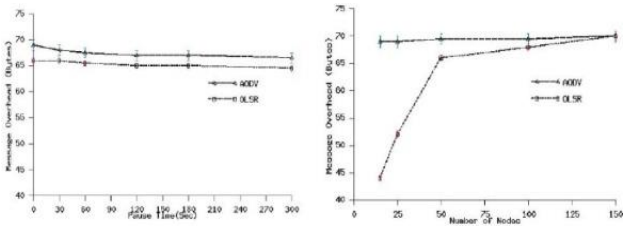

Figure 6.3. Message Overhead

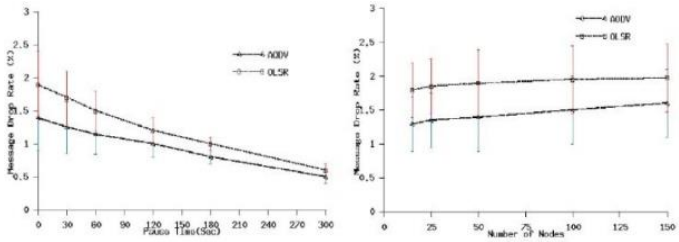

Figure 6.4. Routing message delay

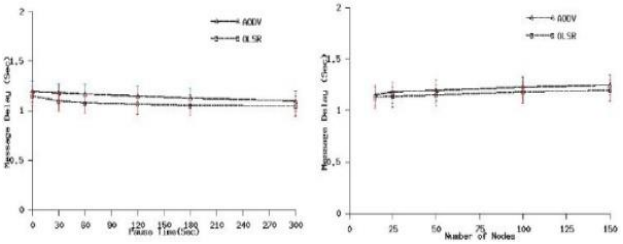

Figure 6.5. Detection accuracy

VII. CONCLUSIONS

In this paper, we developed four intrusion detection models which can be integrated with each other to become a complete intrusion detection system for MANETs.

Table 7.1

AODV	OLSR	DEMEM	DRETA
Model is based on tracing the procedure of flooded routing messages.	Model accurately detects routing attacks in OLSR.	A scalable distributed IDM, designed to efficiently and effectively detect attacks in real-time.	A message authentication model with low computational overhead.
previous node and session tree techniques used to trace the route request and response flow and record the routing data in the flow.	The model proposes four detection constraints according to OLSR specification and successfully detects OLSR routing attacks	adapts to the decentralized networks of MANETs and allows distributed detectors to have sufficient routing data for detecting attacks with low message overhead.	Uses symmetric keys, but achieves functionality of public key systems by integrating one-way key chaining, one-way hash functions, and delay key disclosure. It also proposes Validation Messages.
Detectors can detect any maliciously changed content according to the traced routing data.	the model detects routing attacks with no false positives and negatives	Implemented in OLSR with three ID messages, It can tolerate temporary inconsistency. Have very low false positives, no false negatives, and low message loss or delay.	Implemented DRETA for AODV routing messages, OLSR TC messages, and DEMEM ID messages in OLSR. DRETA successfully integrates our all other work in one piece.

VIII. FUTURE WORK

Here we discuss several future works that our proposed IDS does not support.

First, this IDS only supports attack recovery by an individual node, and we can develop a reputation-based cooperative intrusion response model for DEMEM and DRETA. Second, we can apply DEMEM and DRETA to the other two routing protocols, DSR(Dynamic Source Routing)[21] and TBRPF(Topology Broadcast based on Reverse-Path Forwarding)[30]. Third, we can develop an extension of DRETA for tolerating message loss and minimizing message dropping. Finally, we will develop detection of tunneling routing attacks from correlated attackers, which cannot be detected by our proposed IDS.

IX. REFERENCES

[1]. R. Canetti A. Perrig, D. Tygar, and D. Song. The TESLA broadcast authentication protocol. Cryptobytes, 5(2):2–13, 2002.

[2]. DEMEM: Distributed Evidence-driven Message Exchange intrusion detection Model for MANET. In Proceeding of the 9th International Symposium Recent Advances in Intrusion Detection (RAID), Hamburg, Germany, 2006.

[3]. O. Kachirski abd R Guha. Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks. In 36th Annual Hawaii International Conference on System Sciences (HICSS 2003).

[4]. C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo. Securing the OLSR protocol. In Med-Hoc-Net 2003.

[5]. Yi an Huang and Wenke Lee. Attack Analysis and Detection for Ad Hoc Routing Protocols. In Proceedings of International Symposium Recent Advances in Intrusion Detection (RAID) 2004.

[6]. Yi an Huang and Wenke Lee. A Cooperative Intrusion Detection System for Ad Hoc Networks. In Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN) 2003.

[7]. Farooq Anjum and Rajesh R. Talpade. LiPad: Lightweight Packet Drop Detection for Ad Hoc Networks. In Proceedings of IEEE 60th Vehicular Technology Conference 2004.

[8]. S. Buchegger and J. Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Distributed Ad hoc Networks. In Proceedings of MobiHoc 2002.

[9]. L. Buttyan and J.-P. Hubaux. Stimulating Cooperation in Self-organizing Mobile Ad Hoc Networks. Technical Report DSC/2001/046, Swiss Federal Institute of Technology, Lausanne, 2001.

[10]. T. Clausen and P. Jacquet. Optimized Link State Routing Protocol. IETF RFC 3626.

[11]. Daniel Sterne et. al. A General Cooperative Intrusion Detection Architecture for MANETs. In Proceedings of the 3rd IEEE International Information Assurance Workshop 2005.

[12]. Dhanant Subhadhrabandhu et. al. Efficacy of Misuse Detection in Adhoc Networks. In Proceedings of SECON 2004.

[13]. K. Bhargavan et al. VERISIM: Formal Analysis of Network Simulations. IEEE Transactions of Software Engineering, 28(2):129, 2002.

[14]. Sumit Gwalani, Kavitha Srinivasan, Giovanni Vigna, Elizabeth Belding-Royer, and Richard Kemmerer. An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks. In Proceedings of Computer Security Applications Conference 2004.

[15]. Andreas Hafslund, Andreas Tonnesen, Roar Bjorgum Rotvik, Jon Andersson, and Oivind Kure. Secure Extension to the OLSR protocol. In In OLSR Interop and Workshop 2004.

[16]. N. Haller. The S/Key one-time password system. Internet Society 1994.

[17]. Yih-Chun Hu, Adrian Perrig, and David Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In Proceedings of MobiCom 2002.

[18]. Yih-Chun Hu, Adrian Perrig, and David Johnson. Packet leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. In Proceedings of INFOCOM 2003.

[19]. K. Ilgun, R. Kemmerer, and P. Porras. State Transition Analysis: A Rule-based Intrusion Detection Approach. IEEE Transactions of Software Engineering, 2(13):181–199, 1995.

[20]. H. S. Javitz and A. Valdes. The SRI IDES Statistical Anomaly Detector. In Proceedings of the IEEE Symposium on Research in Security and Privacy 1991.

[21]. David Johnson and David Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing, 1996.

[22]. C. Ko, P. Brutch, and J. Rowe et al. System Health and Intrusion Monitoring Using a Hierarchy of Constraints. In Proceeding of International Symposium Recent Advances in Intrusion Detection (RAID) 2001.

[23]. C. Ko, M. Ruschitzka, and K. Levitt. Execution Monitoring of Security-Critical Programs in Distributed Systems: A Specification-based Approach. In Proceedings of the 1997 IEEE Symposium on Security and Privacy, May 1997.

[24]. H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. IETF RFC 2104.

[25]. U. Lindqvist and P. Porras. Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST). In Proceedings of the 1999 Symposium on Security and Privacy.

[26]. S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In Proceedings of MobiCom 2000.

[27]. P. Michiardi and R. Molva. Core: A Collaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. In Communication and Multimedia Security 2002 Conference.

[28]. P. Ning and K. Sun. How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad hoc Routing Protocols. In Proceedings of IEEE Information Assurance Workshop 2003.

[29]. Jorge Nuevo. A Comprehensible GloMoSim Tutorial. 2004.

[30]. R. Ogier, F. Templin, and M. Lewis. Topology Broadcast based on Reverse-Path Forwarding. IETF RFC 3684.

[31]. Panagiotis Papadimitratos and Zygmunt J. Haas. Secure Link State Routing for Mobile Ad Hoc Networks. In Proceedings of IEEE

Workshop on Security and Assurance in Ad Hoc Networks 2003.

[32]. Charles Perkins, Elizabeth Belding-Royer, and Samir Das. Ad Hoc On Demand Distance Vector (AODV) Routing. IETF RFC 3561.

[33]. Mohapatra Prasant and Krishnamurthy Srikanth. Ad Hoc Networks: Technologies and Protocols.

[34]. R. Ramanujan, S. Kudige, T. Nguyen, S. Takkella, and F. Adelstein. Intrusion-Resistant Ad Hoc Wireless Networks. In Proceedings of MILCOM 2002.

[35]. R. Rao and G. Kesidis. Detection of malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited. Brazilian Journal of Telecommunications, 2003.

[36]. У. Rebahi, V. Mujica, C. Simons, and D. Sisalem. SAFE: Securing packet Forwarding in ad hoc networks. In 5th Workshop on Applications and Services in Wireless Networks 2005.

[37]. Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Elizabeth Belding-Royer, and Clay Shields. A Secure Routing Protocol for Adhoc Networks. In Proceedings of International Conference on Network Protocols (ICNP) 2002.

[38]. Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, and Karl Levitt. A Specification-Based Intrusion Detection System For AODV. In Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN) 2003.

[39]. Chinyang Henry Tseng, Tao Song, Poornima Balasubramanyam, Calvin Ko, and Karl Levitt. A Specification-based Intrusion Detection Model for OLSR. In Proceeding of the 8th International Symposium Recent Advances in Intrusion Detection (RAID), Seattle, 2005.

[40]. Shiau-Huey Wang, Chinyang Tseng, Calvin Ko, and Karl Levitt. A General Automatic Response Model for MANET. In Proceeding of First IEEE International Workshop on Next Generation Wireless Networks 2005 (IEEE WoNGeN '05).

[41]. S. Yi, P. Naldurg, and R. Kravets. Security-aware routing protocol for wireless ad hoc networks. In Proceedings of ACM MobiHoc 2001.

[42]. M. G. Zapata. Secure ad hoc on demand (SAODV) routing. IETF Internet Draft, 2001.

[43]. Y. Zhang and W. Lee. Intrusion Detection in Wireless Ad Hoc Networks. In Proceedings of MobiCom 2000.