

Intrusion Detection System for Mobile Ad-Hoc Networks: A Survey

Nupur Shah

M.E Student

Department of Information Technology

SVIT-Vasad India

Abstract— Today it is very important to provide a high level security to protect highly sensitive and private information. Intrusion Detection System is an essential technology in Network Security. Nowadays researchers have interested on intrusion detection system using Data mining techniques as an artful skill. So my aim is to use IDS system and improve the performance of the IDS. IDS is a software or hardware device that deals with attacks by collecting information from a variety of system and network sources, then analyzing symptoms of security problems. The main focus of Intrusion detection and prevention systems (IDPS) is to identify the possible incidents, logging information about them and in report attempts. But sometimes IDS is not able to detect some new attacks and vulnerabilities. The main aim of this report is to provide the knowledge of the IDS and also gives the survey of specification-based IDS in wireless ad-hoc network. So this report provides basic knowledge of IDS system as well as how to use MANET protocol for IDS and improve the performance of IDS and future research.

Key words: Wireless Ad-Hoc Network, IDS, MANET, AODV

I. INTRODUCTION

Intrusion Detection System (IDS) is as the part of the security and it is the essential part for any online network now days hence it is in picture. It is used as a countermeasure to preserve data integrity and system availability during an intrusion. [10]

The rapid usage and innovation of wireless networks and mobile computing applications has changed the view and scope of network security. These attacks could significantly disrupt the transmission of data which relies on full cooperation between nodes to route messages. Due to the shared nature of wireless channels, noise within the channels, and instability caused by mobility, wireless communication is much more vulnerable to attacks than wired networks Node authentication and data encryption alone are not sufficient for the security of these networks.[9] Intrusion detection techniques can be classified into anomaly detection, signature-based detection, and specification-based detection Nowadays securing the ad-hoc routing protocol is the challenging problem A mobile wireless network is unprotected due to its features of open medium, dynamic changing network topology, cooperative algorithms, lack of centralized monitoring and management point. Future research is needed to address these vulnerabilities.

II. VULNERABILITIES OF MOBILE WIRELESS NETWORKS^[1]

First one is the use of wireless links provides the network susceptible to attacks ranging from passive eavesdropping to active interfering. So wireless network is vulnerable to malicious attacks. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defence at firewalls and gateways,

attacks on a wireless network can come from all directions and target at any node. Damages can include leaking secret information, message contamination, and node impersonation.

Second, mobile nodes are self-governors that are capable of roaming independently. This means that nodes with inadequate physical protection are receptive to being captured, compromised, and hijacked.

Third, decision-making in mobile computing environment is sometimes decentralized and some wireless network algorithms depend on the cooperative participation of all nodes and the infrastructure. The lack of centralized authority means that the adversaries can exploit this vulnerability for new types of attacks designed to break the cooperative algorithms.

III. CHALLENGES OF INTRUSION DETECTION SYSTEMS IN MANETS^[7]

Intrusion detection systems developed for fixed networks are not directly implementable in the wireless network environment, and therefore research in the last few years has focused on securing MANETs with IDSs. Intrusion detection in MANETs is more complex and challenging than in fixed networks.

For example, in fixed networks, traffic is monitored at network gateways whereas in an infrastructure less MANET a node can only observe other nodes within its radio range; attackers outside this radio range can therefore escape easily. Consequently, the network-based IDS (NIDS) proposals used in fixed networks are not directly implementable in MANETs. Realizing this difficulty, researchers have proposed cooperative approaches of audit data collection and the application of intrusion detection techniques using network clustering.

Moreover, MANETs introduced a new set of routing protocols, which are significantly different from those used in fixed networks. These protocols require nodes to cooperate and act as routers; but it also means that the network's routing infrastructure is not under the control of a single management entity. This has created opportunities for attackers to identify vulnerabilities and find new ways to launch attacks.

Attacks in MANETs differ from those in fixed networks and therefore most detection methods used in fixed networks are not directly applicable; hence alterations to existing techniques. and the introduction of new methods for intrusion detection have been considered by researchers.

The limited bandwidth of MANETs in contrast to wired networks additionally makes it challenging to transfer large amount of intrusion detection data and therefore MANET IDSs have to limit the volume of data transfer required for intrusion detection.

To sum up, every phase of intrusion detection in MANETs presents additional challenges as compared to fixed networks.

IV. INTRUSION DETECTION TECHNIQUES

It is classified in main three categories: (1) anomaly-based intrusion detection also known as behaviour-based intrusion detection; (2) misuse detection, also known as Signature-based intrusion detection and (3) specification-based intrusion detection (SBID), which has been proposed recently.[6]

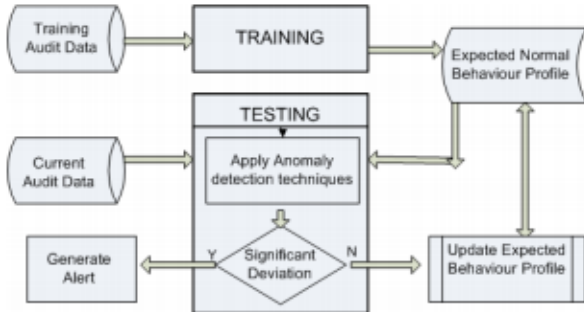


Fig. 1: Anomaly-based intrusion detection process

Figure 1 depict that it has two phases: training and testing. In training phase, it is the process of modelling the expected normal behaviour of the network or of the user. And in testing phase, it is the testing for intrusion involves comparing the normal or expected behaviour model derived during the training phase with the current model of the network or users. So anomaly based detection system is to estimate the deviation between the expected and the current behaviour to detect an intrusion in the network. so it is also called as behaviour-based intrusion detection.

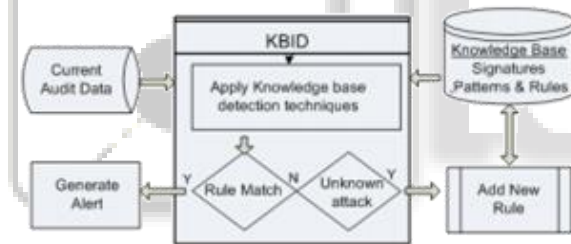


Fig. 2: Misuse-based intrusion detection process

Misuse-based intrusion detection is also called as knowledge-based intrusion detection because in Figure 2. it depicts that it maintains knowledge base which contains the signature or patterns of well-known attacks. This intrusion system generates an alarm when such attempt is detected. This system uses various methods for constructing and modelling the knowledge for intrusion detection.

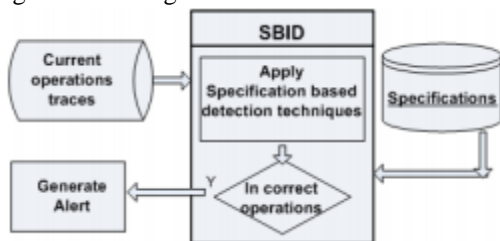


Fig. 3: Specification-based intrusion detection process

Generally, specification-based intrusion detection systems (SBIDs) first explicitly define specifications as a set of constraints. It is called hybrid system because it is the combination of misuse-based IDS and anomaly based IDS. They then uses these specifications to monitor the routing protocol operations or network layer operations to detect attacks in the network. The basic process of SBID is shown

in Figure 3. The first step extracts the specifications, which define the correct operation of (for example) the network or the MAC layer protocol through a set of constraints. The system then monitors the execution of the protocol with respect to the given specification, deviations from the specification being treated as intrusion.[6]

V. RELATED WORK

In our proposed architecture (Figure 5), every node in the mobile ad-hoc network participates in intrusion detection and response. Each node is responsible for detecting signs of intrusion locally and independently, but neighbouring nodes can collaboratively investigate in a broader range.[1]

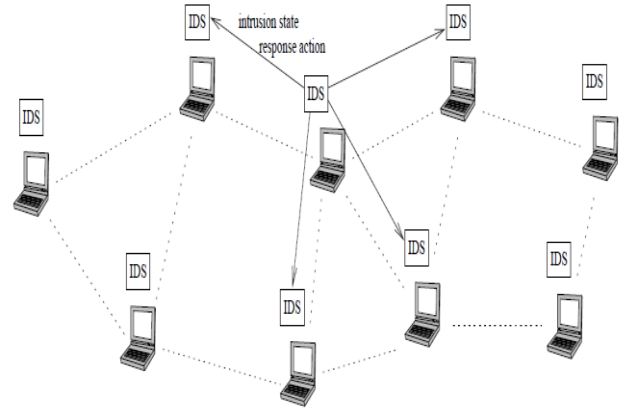


Fig. 4: The IDS Architecture for Wireless Ad-Hoc Network

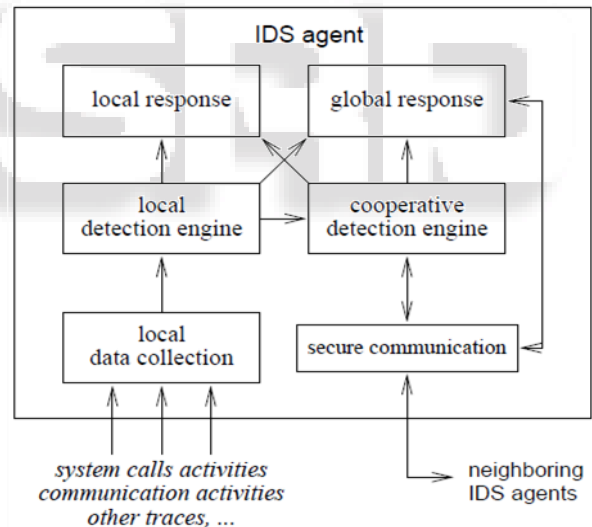


Fig. 5: A Conceptual Model for an IDS Agent

Figure 5 depicts that IDS system placed on each and every node. Each IDS agent runs independently and monitors local activities.[1]

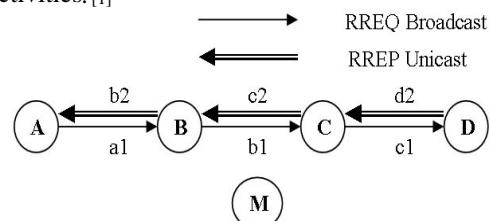


Fig. 6: AODV Scenario

They propose a specification-based intrusion detection system that can detect attacks on the AODV routing protocol Figure 6 illustrates the flow of the RREQ and RREP messages in a scenario wherein a node A wants to find a route

to a node D. (Initially, nodes A, B, C and D do not have routes to each other). A broadcasts a RREQ message (a1), which reaches B. B then rebroadcasts the request (b1). C receives the messages and broadcasts the message (c1), which arrives at the destination node D. Last, D unicasts back the RREP message to A. We call these RREQ and RREP packets a request-reply flow.^[2]

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.

Table 1: Vulnerable Fields in AODV Packets

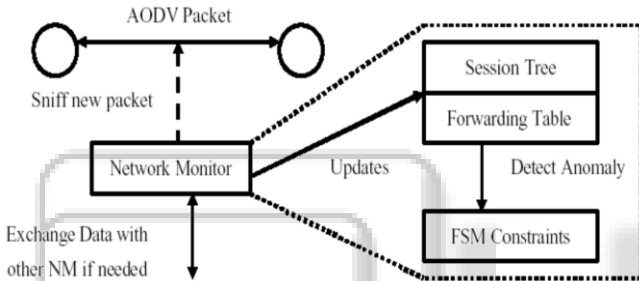


Fig. 7: Architecture of Network Monitor

Figure 7 depicts the architecture of a network monitor. Network monitors passively listening to AODV routing message and detect incorrect RREQ and RREP messages. Messages are grouped based on the request-reply flow to which they belong. A request-reply flow can be uniquely identified by the RREQ ID, the source and destination IP addresses. A RREQ or RREP message can map to a request-reply flow based on these fields as shown below.
RREQ: AODV Source address and RREQ ID
RREP: AODV Source and Destination address

A network monitor keeps track of the RREQ and RREP message last received by each monitored node and maintains the forwarding table of each monitored node.

To determine the validity of a message (sent by a node, say A), a network monitor needs to identify the corresponding incoming message to A. For unicast messages, such as RREP, a NM can map current and previous packets easily by looking their source and destination addresses in IP headers. However, in broadcast messages, such as RREQ, the destination address will always be the broadcast address (255.255.255.255). To keep track of the RREQ path, we add one more field to AODV, called previous node (PN). This field indicates the node that previously forwarded the RREQ to the current node.

Our specification-based approach for OLSR analyzes the protocol specification (e.g., RFC) 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 of the individual nodes for violation of the constraints.^[3]

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 independently establish the routing tables at each node. In OLSR, only nodes that have bidirectional (symmetric) links between them can be neighbors. Hello messages contain neighbor lists to allow nodes to exchange neighbor information, and set up their 1-hop and 2-hop neighbor lists; these are used to calculate multi-point relay (MPR) sets.

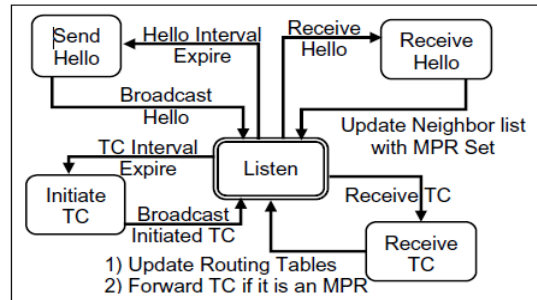


Fig. 8: OLSR Routing Finite State Automata (FSA)

We describe the constraints on the control traffic between neighbor nodes for detecting inconsistencies within the control messages.

- C1: Neighbor lists in Hello messages must be reciprocal. E.g., if node 2 is the neighbor of node 1, then node 1 must be node 2's neighbor.
- C2: The MPR nodes of a node must reach all 2-hop neighbors of the node and the MPR nodes must transmit TC messages periodically.
- C3: MPR selectors of a TC message must match corresponding MPR sets of Hello messages. E.g., if node 2 is node 1's MPR selector, node 1 must be in node 2's MPR set.
- C4: Fidelity of forwarded TC messages must be maintained.

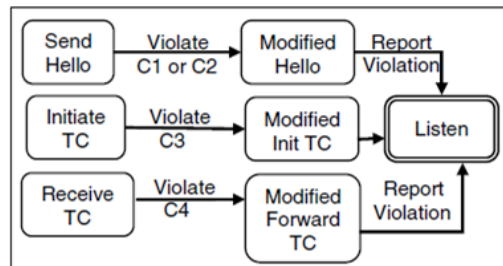


Fig. 9: Security Specification Finite State Automata

When a OLSR control message violates one of the constraints, the FSA moves from a normal state into one of the alarm states (Modified Hello State, Modified Init TC State, Modified Forward TC State) To recovery from the errors, a detector may broadcast the corrected TC message, or force the node causing the violation to resend the corrected Hello message, and thereby recover corrupted routing tables of infected nodes. Thus, the "report violation" actions in the FSA can be enhanced to perform the corrective action.

But there is some limitation which is that if there are two or more attackers try to make a correlated lie the constraints may not be able to detect it. It is same as tunnelling attack— attackers build up a virtual link between

them. But one thing they proved that is integrity of routing table at all node is not compromised.

In this paper they suggest that specification-based IDS is better IDS model to adopt in MANET compared to traditional IDS. They proposed previous two forwarders method which is used with detection rules which are built from the AODV specification.^[4]

Based on the classification of attacks on the AODV routing protocol, we classify attacks on AODV into two categories:

A. Routing Disruption and Resource Consumption

1) Routing Disruption:

By sending false routing message to victim nodes in several different ways. As a result, victim nodes are tricked into creating a false route. We call this malicious behavior as Message Deceiving or Routing Disruption. For Example, Modifying RREQ ID field, sequence number field, hop count field.

2) Resource Consumption:

By flooding RREQ messages, network resource would be consumed such as bandwidth and transmission power. Nodes flood route request messages only when nodes need to know a route to an unknown destination.

By flooding a large amount of RREQ messages to jam the network causing packet loss or delay. Consequently, the ad hoc network will suffer the loss of network resource like bandwidth and transmission power. This is called network resource consumption.

The Concepts of Previous Forwarders is that when a node receives message to forward it to the next node then that node stores the information regarding the received message and forward it to the next node so that the node have the information of previous node.

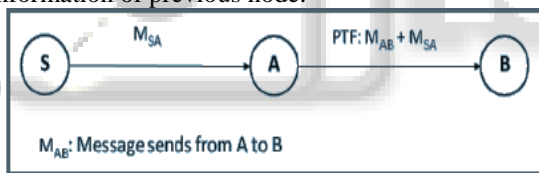


Fig. 10: Previous Two Forwarders

For example in Fig. 10, node A sends RREQ, MAB, to node B, then node B sends RREQ, MBC, to node C; node B puts the message field of MAB into MBC and forwards to node C (next node). The message field of MAB will be filled in to PN related field by node B.

Now with they use detection rule with PTF approach. That detection model consists of 5 specification rules: SP1 TO SP5.

SPECIFICATION RULE	
Number	Content
SP1	SRC belongs to PN 's neighbor list and $PN-SRC$ belongs to SRC 's neighbor list
SP2	HC increases by one to $PN-HC$
SP3	$RREQ_ID$ consists with $PN-RREQ_ID$
SP4	Seq consists with PN field
SP5	TTL decreases by one to $PN-TTL$
SP6	Source Address and Originator Address consistency
SP7	Source Address and Destination Address consistency

Fig. 11: Specification Rules

We implement the detection model at the beginning of the message handling process. When a node receives either a RREP or RREQ message, it first checks if the source address from the IP header is Orig in RREQ or the Dest in RREP. If yes, then there is no previous node field in the route message and SP6 or SP7 will be applied, otherwise the rules SP1 to SP5 will be applied.^[4]

In this paper IDS with mobile agents is The mobile agents are deigned to work as a tactical squad that conducts regular petrol missions through MANET nodes. Their approach is based on structured military command-base where agents get their instructions to police routes to detect any malicious activity. Some routes are patrolled more than others based on the calculated risk.

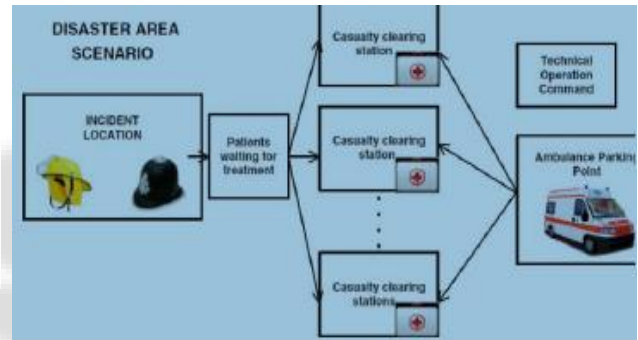


Fig. 12: zones of disaster response scenario

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehaviour report authentication (MRA). They proposed digital signature to prevent the attacker from forging acknowledgment packets. Fig. 12 presents a flowchart describing the EAACK scheme.^[5]

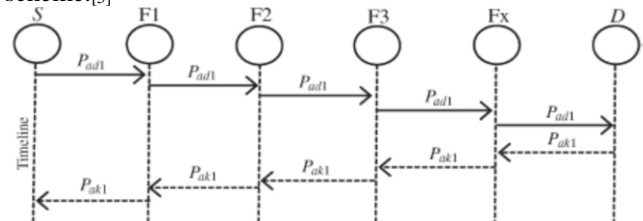


Fig. 13: System Control flow

The aim of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.^[5]

	System/ Protocol	Pros	Cons	Suitable for
1	Intrusion Detection Techniques for Mobile Wireless Networks ^[1]	The detectors in general have good detection performance.	N/A	Mobile Ad-hoc Network

2	A Specification-based Intrusion Detection System for AODV _[2]	It can effectively detect most of the serious AODV routing attacks effectively, and with low overhead.	N/A	Distributed network
3	A Specification-Based Intrusion Detection Model for OLSR _[3]	It develop the proof of satisfaction of the requirement that the integrity of routing tables of all nodes is safeguarded	If two or more attackers try to make a correlated lie the constraints may not be able to detect it.	Ad hoc Network
4	A Specification-based Intrusion Detection Model for Wireless Ad Hoc Networks _[4]	Packet delivery ration increases.	N/A	MA-NET
5	EAACK—A Secure Intrusion-Detection System for MANETs _[5]	Use digital signature to prevent the attacker from forging ack packets.	Requirement of pre-distributed keys	MA-NET

Table 2: Comparison of different IDS

ACKNOWLEDGMENT

I am very grateful and would like to thank my guide and teacher Prof. Swati Bendale for her advice and continued support without which it would not have been possible for me to complete this report. I am also very grateful and also like to thank Head of The Department Prof. Nisha V. Shah and the entire Information Technology Department, faculty and staff, for helping me in every possible manner during my course of study for this subject.

- [7] Kaushik, Shant, and Sonia Sharma. "Securing Ad hoc Networks for Intrusion Detection, A study." (2015).
- [8] Aarti, Dr SS. "Tyagi, Study of MANET: Characteristics, Challenges, Application and Security Attacks." International Journal of Advanced Research in Computer Science and Software Engineering 3.5 (2013): 252-257.
- [9] <http://www.combofix.org/what-it-is-network-intrusion-detection-system.php>
- [10] <http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection>

VI. CONCLUSION

Intrusion detection system can be used for monitoring file system for changes. Intrusion detection systems can be help full in detecting if an intrusion has been occurred and what changes are made to system. It is concluded that a specification-based concept is employed to design an intrusion detection model for MANET environment. To achieve the security goals, the proposed model provides the PTF approach where the sender node sends AODV messages together with additional information of its previous forwarder. The receiver node then verifies message integrity by comparing the information. In future by increasing the storage size we can improve the performance of IDS with high packet delivery ratio.

REFERENCES

- [1] Yongguang, Wenke Lee, and Yi-An Huang. "Intrusion detection techniques for mobile wireless networks." Wireless Networks 9.5 (2003): 545-556 Tseng, Chin-Yang, et al..
- [2] "A specification-based intrusion detection system for AODV." Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. ACM, 2003
- [3] Tseng, Chinyang Henry, et al. "A specification-based intrusion detection model for OLSR." Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2006
- [4] H.C. Lin, M.K. Sun, H.W. Huang, C.Y. Tseng, and H.T. Lin. A Specification-based Intrusion
- [5] Detection Model for Wireless Ad Hoc Networks, International Conference on Innovations in Bio-Inspired Computing and Applications, pp. 252-257. 2012.
- [6] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami. "EAACK—a secure intrusion-detection system for MANETs." Industrial Electronics, IEEE Transactions on 60.3 (2013): 1089-1098