ISSN:0975-9646



# A Study on Intrusion Detection in Mobile Ad Hoc Networks

R.Amutha

*Assistant Professor*
*Department of Computer Science*
*PSG College of Arts and Science, Coimbatore.*
*TamilNadu ,India.*

M.Savithri

*Assistant Professor*
*Department of Computer Science*
*Dr. N.G.P. Arts and Science College, Coimbatore.*
*TamilNadu, India*

***Abstract*— Intrusion detection for mobile ad hoc network (MANET) is a complex and difficult task due to the nature of the network. The mobile ad hoc network is vulnerable due to its features of open medium, cooperative algorithms, dynamic changing topology, lack of centralized monitoring and management point. The mobile ad hoc networks (MANETs) combine wireless communication with high degree of node mobility. Intrusion detection system (IDS) monitors system activities and detect intrusions are used to implement security mechanisms. Distributed systems are used in multiple building which may locate thousands of miles apart. This type of communication may be a path way for intrusion. This paper describes some issues of intrusion detection for wireless ad hoc network and reviews the main solutions.**

**General Terms-Intrusion Detection**

***Keywords*— MANET, IDS, AODV, DSR,DSDV, Intrusion Detection.**

## I. INTRODUCTION

Wireless networking is the medium of many applications and it allows many sophisticated functionalities. A MANETs consist of collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on continual arbitrary basis. The data link layer functions manage the wireless link resource and coordinate medium access among neighboring nodes. The Medium Access Control (MAC) protocol is essential to a wireless ad hoc network because it allows mobile nodes to share a common broadcast channel. MANETs are more vulnerable to attack than wired networks as well as it introduces new security risks. As the part of risk management we must be able to identify these risks and take necessary action. Intrusion detection is part of security for MANETs. There are many Intrusion detection systems are proposed for wired networks but which are not applicable for MANETs directly. New approaches need to be developed or else existing approaches need to be adopted for MANETs. In this section we examine some issues of intrusion detection system of MANETs and proposed IDS for MANETs.

## II. INTRUSION DETECTION SYSTEMS

Intrusion defined as a set of actions that attempt to compromise the integrity, confidentiality and availability of a resource [1] and an intrusion detection system is a system for the detection of such iterations. IDS consists the following components: data collection, detection and response. The first component data collection is responsible for collection and pre-processing and transferring data to common format [2]. IDS use inputs from different data source such as system logs, network packets, etc. The second component detection is used to analyses the data and to detect intrusion attempts and the detected intrusions are sent to the response component.

There are many intrusion detection techniques used. The first technique is anomaly based intrusion detection which profiles the symptoms of normal behaviours of the system such as usage frequency of commands, CPU usage for programs. It detects intrusion as anomalies. The second technique Misuse based intrusion detection compares current system activities with known attack signatures. This technique does not detect new attacks. The last technique is specification based intrusion detection. In this technique, a set of constraints on a program or a protocol are specified and intrusions are detected as runtime violations of these specifications. It provides the detection of known and unknown attacks with a lower false positive rate [3] and detects new attack that does not follow system specifications. When an intrusion is detected, an appropriate response is triggered according to the response policy. Responses to detected intrusions can be passive or active. Passive responses simply raise alarms and notify the proper authority. Active responses try to mitigate effects of intrusions.

## III .INTRUSION DETECTION ISSUES IN MANETS

Different characteristics of MANETs make conventional IDSs ineffective and inefficient for this new environment. There are some issues which should be taken into account when IDS is being designed for MANETs.

Lack of Central Points: MANETs does not have entry points like as routers, gateways, etc. These are present in wired networks and can be used to monitor all network traffic that passes through them. Any node of a MANET can see only a portion of a network. The packets which send or receive are within its radio range. The intrusion detection in MANET should be distributed and cooperative [4]. This leads to some difficulties.

Mobility: MANET nodes leave the network and move independently. The topology may change frequently which is unreliable in traditional techniques of IDS.

Wireless Links: In wireless networks IDS agent needs to communicate with other IDS agents to obtain data. IDS traffic could cause congestion and limit normal traffic, so IDS agent need to minimize their data transfer [5]. Due to limitations in Bandwidth ineffective IDS operations may occur.

Limited Resources: There are different kinds of MANET devices such as laptops, PDAs and mobile phones. The variety of nodes generally with scarce resources, affects effectiveness and efficiency of the IDS agents they support. The detection algorithm can take into account with limited resources. For ex, misuse based algorithm detection algorithm must take into account memory constraints for signatures and anomaly-based detection algorithm needs to be optimized to reduce resource usage.

Lack of a Clear Line of Defences and Secure Communication: In MANETs attacks can come from any directions [4]. There are no central points on MANETs where access control mechanisms can be placed. To avoid attackers to learn the IDs traffic it can be encrypted [5]. But Cryptography and authentication are difficult tasks in a mobile wireless environment since they consume significant resources.

Cooperativeness: Routing protocols in MANET are highly cooperative. Which helps the target of new attacks? For example, a node can pretend to be as a neighbor to the other nodes and participate in decision mechanisms, possibly affecting significant parts of the network.

## IV PROPOSED IDSS

MANETs use different kinds of intrusion detection methods. The common intrusion detection method is specification based detection which detects attacks against routing protocols & DoS attacks. In Hierarchical IDS is also a kind of distributed and cooperative architecture. In this, the network can be divided into zones, clusters where come nodes have responsibility than other nodes in the same group [6]. There are some proposed IDSs for MANETs.

*A. Distributed and Cooperative IDS:*

Every node has an IDS agent which detects intrusions locally, for global detection it needs a broader search. An IDS agent can either trigger a global response or local response whenever an intrusion is detected. RIPPER and SVM – Light [7] classification algorithms are evaluated using detection rate and false alarm rate metrics of AODV, DSR and DSDV protocols.

B. *Cooperative IDS using Cross-Feature Analysis in MANETs [8]*

In cross-feature analysis, train the classification model Ci [8] from normal data based on exploring the correlation between each feature and all other features. Each feature fi is analyzed and compared with the predicted values of fi. Some rules are applied based on statistics such as number of incoming/outgoing packets on the monitored node and are pre-computed for known attacks which is implemented on the NS-2.

C. *Zone-Based Intrusion Detection System [9]*

In these IDS, the network is divided into zones based on geographic partitioning to save communication bandwidth [9]. The nodes in the zone are called intra zone nodes and that works as bridge to other zones are called as inter zone nodes (gateway). To make final decision and to send alarms the gateway nodes are responsible for global aggregation and correlation. Intra zone nodes carry out local aggregation and correlation. Gateway nodes use the following similarities in the alerts to detect intrusions: classification similarity (classification of attacks), time similarity (time of attack happening and time of attack detection), and source similarity (attack sources). Source similarity is the main similarity used, so the detection performance of aggregation algorithm could de-crease with the increasing of the number of attackers.

D. *Intrusion Detection Using Multiple Sensors [10]*

This is an important feature for MANETs which have lower bandwidth than wired networks. A modular IDS structure is proposed that distributes the functional tasks by using three mobile agent classes: monitoring, decision-making and action-taking. The advantages of this structure are increased fault-tolerance, communication cost reduction, improved performance of the entire network, and scalability [10].

E.*Specification-Based IDS for AODV [11]*

This approach use network monitors which are assumed to cover all nodes. Whenever nodes moving out of the current network monitoring area are also assume d out of range of network. Some other assumptions are i) Network monitors know all nodes' IP and MAC addresses, and MAC addresses cannot be forged. ii) Network monitors and their messages are secure. iii) if some nodes do not respond to broadcast messages, this will not cause serious problems [11]. NS-2 network simulation, profiling network QoS (Quality of Service) to reduce false positives by separating packet loss, packet error, and packet generation through defining reasonable thresholds for the current profile, and refining NM architecture using via a P2P (peer-to-peer) approach.

*F.DEMEM: Distributed Evidence-driven Message Exchanging ID Model [12]*

DEMEM is a distributed and cooperative IDS in which each node is monitored by one-hop neighbour nodes. In addition to one-hop neighbour monitors, 2-hop neighbours can exchange data using intrusion detection (ID) messages [12]. The main contribution of DEMEM is to introduce these ID messages to help detection, which they term evidence-driven message exchange. Evidence is defined as critical information (specific to a routing protocol) used to validate the correctness of the routing protocol messages, for instance hop count and node sequence number in AODV. The proposed specification-based system uses the following constraints of OLSR to detect intrusions:

1: neighbours in Hello messages must be reciprocal.
2: MPRs must reach all 2-hop neighbours.
3: MPR selectors must match corresponding MPRs.
4: Fidelity of forwarded TC messages must be maintained.

*G.An IDS Architecture with Stationary Secure Database [5]*

Stationary Secure Database (SSD) is a distributed architecture consisting of IDS agents [5]. For local detection and collaboration with other agents in need, all

nodes have IDS agents. IDS agents have five components: local audit trail; local intrusion database (LID); secure communication module; anomaly detection modules (ADMs); and misuse detection modules (MDMs). The local audit trail gathers and stores local audit data – network packets and system audit data

## V. Detection of Misbehaving Nodes

### *A .Watchdog and Pathrater [13]*

It is important in detecting misbehaving nodes. Node that does not carry out what they are assigned to do by mitigating their effects [13]. The watchdog's listens to nodes in promiscuous node to detect misbehaving nodes. The watchdog mechanism of the node monitors the next node to verify that it forwards the packet properly whenever a node forwards a packet. It store sent packets in a buffer. The packets are removed from the buffer after the packets are forwarded by next node. The watchdog increments the failure count of the node implicated when the packets remain in the buffer longer than some timeout period. A notification is sent to the source node if the failure count of a node exceeds a threshold value; the node is identified as a misbehaving node. It is stated that watchdog can also detect replay attacks to some extent.

### *B. Nodes Bearing Grudges [14]*

All the nodes are responsible detecting misbehaving nodes and monitoring the behaviour of its next hop neighbours. There is trust architecture and an FSM in each node with four main components: the monitor, the reputation system, the path manager, and the trust manager. The monitor (neighbourhood watch) keeps a copy of recently sent packets. It can compare them with the packets forwarded by the next hop node and can detect routing and forwarding misbehaviours as deviations from normal expected behaviour. The types of misbehaviour that can be detected by this system are stated to be: no forwarding, unusual traffic attraction, route salvaging and lack of error messages, unusually frequent route updates, and silent route change.

### *C. LiPaD: Lightweight Packet Drop Detection for Ad hoc Networks*

In this approach every node counts the packets that it receives and forwards and periodically reports these counts to a coordinator node. Promiscuous monitoring is not used since it depends on the link layer characteristics and the link layer encryption approach [15]. That's why every node is responsible for monitoring its packets in LiPaD. The algorithm executed in each node is very simple, which is good for resource-constrained nodes

### *D.Intrusion Detection and Response for MANET*

Intermediate nodes may misbehave by dropping or modifying the packets. Some of the techniques may propose to detect misbehaviours A node listens to all nodes in its transmission range, not just the packets forwarded by one of its next nodes. It detects dropping and modification attacks which exceed the value in the threshold table for the particular attack class. However, a node moving out of range of the monitoring node before it forwards packets can be assumed to be carrying out a dropping attack. This issue will be ad-dressed in future by the authors. Also, this approach cannot detect misrouting attacks, since it does not know the next hop of a packet that it monitors.

## VI. Conclusion

The security in MANETs is more important because the use of mobile ad hoc networks has increased. Many MANET IDSs have been proposed, with different intrusion detection techniques, architectures, and response mechanisms. With the nature of MANETs almost the intrusion detection is structured should be distributed and cooperative. A statistical anomaly detection approach should be used. The number of new attacks is likely to increase quickly and those attacks should be detected before they can do any harm to the systems or data. As a consequence intrusion detection for MANETs remains a complex and challenging topic for security researchers.

## References


[1] Heady R, Luger G, Maccabe A, Servilla M (1990) The architecture of a net-work level intrusion detection system. Technical Report, Computer Science Department, University of New Mexico.

[2] Lundin E, Jonsson E. (2002) Survey of Intrusion Detection Research. Technical report 02-04, Dept. of Computer Engineering, Chalmers University of Technology

[3] Uppuluri P, Sekar R (2001) Experiences with Specification-based Intrusion Detection. In Proc of the 4th Int Symp on Recent Adv in Intrusion Detect LNCS 2212: 172-189

[4] Zhang Y, Lee W (2000), Intrusion Detection in Wireless Ad Hoc Networks. In Proc of the 6th Int Conf on Mobil Comput and Netw (MobiCom): 275-283.

[5] Zhang Y, Lee W (2000), Intrusion Detection in Wireless Ad Hoc Networks. In Proc of the 6th Int Conf on Mobil Comput and Netw (MobiCom): 275-283.

[6] Anantvalee T, Wu J (2006) A Survey on Intrusion Detection in Mobile Ad Hoc Networks. Wirel/Mobil Netw Secur, Springer: 170-196

[7] Zhang Y, Lee W (2003) Intrusion Detection Techniques for Mobile Wireless Networks. Wirel Netw : 545-556.

[8] Huang Y, Fan W et al (2003) Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies. In Proc of 23rd IEEE Int Conf on Distrib Comput Syst (ICDCS):478-487.

[9] Sun B, Wu K et al (2006) Zone-Based Intrusion Detection System for Mobile Ad Hoc Networks. Int J of Ad Hoc and Sens Wirel Netw 2:3

[10] Kachirski O, Guha R (2003) Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks. In Proc of the 36th IEEE Int Conf on Syst Sci (HICSS)

[11] Tseng C-Y, Balasubramayan P et al (2003) A Specification-Based Intrusion Detection System for AODV. In Proc of the ACM Workshop on Secur in Ad Hoc and Sens Netw (SASN)

[12] Tseng CH, Wang SH (2006) DEMEM: Distributed Evidence Driven Message Exchange Intrusion Detection Model for MANET. In Proc of the 9th Int Symp on Recent Adv in Intrusion Detect LNCS 4219:249-271.

[13] Marti S, Giuli TJ et al (2000) Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks. In Proc of 6th ACM Int Conf on Mobil Comput and Netw (Mo-biCom):255-265

[14] Buchegger S, Le Boudec J (2002) Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Network. In Proc of 10th Euromicro Workshop on Parallel, Distrib and Netw-based Process: 403-410

[15] Anjum F, Talpade R (2004) LiPaD: Lightweight Packet Drop Detection for Ad hoc Networks. In Proc of IEEE Veh Technol Conf (VTC) 2:1233-1237