Comparative study of Distributed Intrusion Detection in Ad-hoc Networks

Sumitra Menaria
Post graduate Student
Institute of technology,
Nirma University, India

Prof Sharada Valiveti
Associate Professor
Institute of technology,
Nirma University, India

Dr K Kotecha
Director
Institute of technology,
Nirma University, India

ABSTRACT

In recent years ad hoc networks are widely used because of mobility and open architecture nature. But new technology always comes with its own set of problems. Security of ad hoc network is an area of widespread research in recent years. Some unique characteristics of ad hoc network itself are an immense dilemma in the way of security. In this paper we have presented study about characteristics of ad hoc network, how they are problematic in ad hoc network security, attacks in ad hoc network and brief description of some existing intrusion detection system. We have also justified why distributed intrusion detection is better for ad hoc network with comparative study of existing intrusion detections in ad hoc network.

General Terms

Ad hoc networks, Security, IDS, DIDS.

1. INTRODUCTION

Ad hoc networks have turned out to be a very popular research theme. By providing communication in the absence of a predetermined infrastructure they are very attractive for many applications such as tactical and disaster recovery operations and virtual conferences. On the other hand, this flexibility introduces new security risks. Moreover, different characteristics of ad hoc networks make traditional security methods ineffective and incompetent for this new environment. Intrusion detection, which is an essential part of a security system, also presents challenges due to the dynamic nature of ad hoc networks, the absence of central administration, and their highly constrained nodes. The mobility of wireless devices demands more flexible, stronger and efficient defense schemes. Here in this paper we have mentioned details of attacks in ad hoc network, available techniques as well as architecture of different IDS with their comparison.

The paper is focused on the detailed study of vulnerabilities in ad hoc networks which affects intrusion detection, attacks possible on ad hoc networks with a brief overview, intrusion detection grouping and the research achievements in IDS field.

2. VULNERABILITIES OF AD HOC NETWORK

Ad hoc networks have characteristics such as dynamically changing topology, weak physical protection of nodes, the absence of centralized administration, and high dependence on inherent node cooperation. Due to dynamic topology, ad hoc networks do not have a well-defined boundary, and thus, mechanisms such as firewalls are not applicable. Vulnerabilities in ad hoc network described in [1, 2, 3 and 4] are:

1) ***Dynamic topology:*** Due to dynamic topology ad hoc networks require sophisticated routing protocols. A particular difficulty is that misbehaving node can generate wrong routing information which is hard to discover. Mobility of devices is also creates a problem.

2) ***Absence of infrastructure****:* Ad hoc networks do not have any fixed infrastructure which makes traditional security mechanism of cryptography and certification inapplicable.

3) ***Vulnerability of nodes:*** Physical protection of nodes is not possible hence they can more easily be captured and falls under the control of an attacker.

4) ***Vulnerability of channels:*** In wireless network, message eavesdropping and injection of fake messages into the network is easy without having physical access to network components.

3. TYPE OF ATTACKS

For the purpose of intrusion detection, one needs to analyze anomalies due to both the consequence and technique of an attack. Consequence gives evidence about the success of attack and technique helps in identifying attack and some time attacker too.

Attacks in ad hoc network can be categorized according to their consequences into passive attack which not involve disruption of information but they are merely intended to get information and to spy on the communication within the network vs. active attack in which data are altered by attacker which involves overloading of network or preventing nodes from using the networks services effectively anymore [7].

Internal attack which comes from compromised node inside the network vs. external attack in which unauthenticated attackers can replay old routing information or inject false routing information to partition the network or increase the network load [1].

Unbalanced use of transmission channel vs. anomaly in packet forwarding [6] which is explained below:

In unbalanced use of transmission channel one node tries to prevent other nodes in its neighborhood from getting fair share of the transmission channel. This misbehavior can be considered as DoS attacks against the competing neighbors in a contention-based network as competing neighbors are underprivileged of their fair share of the transmission channel. Some of the possible methods for unfair use of the transmission channel are as follows:

- Ignoring the MAC protocol: A misbehaving node can generate RTS/CTS at an unacceptable rate by ignoring the backoff mechanism.
- Jamming the transmission channel with garbage packets.
- Ignoring the bandwidth reservation scheme.
- Malicious flooding.
- Network Partition: A connected network is partitioned into k (k more than 2) sub a network where nodes in different sub networks cannot communicate even through a route between them actually does exist.
- Sleep Deprivation: A node is forced to exhaust its battery power.

Where as in anomalies in packet forwarding following attacks are included:

- Drop packets: A node may disrupt the normal operation of a network by dropping packets. This type of attack can be classified into two types:
    - Black hole attack: A misbehaving node drops all types of packet
    - Gray hole attack: An attacker selectively drops data packets.
- Delay packet transmissions: A node can give preference to transmitting its own or friends' packets by delaying others' packets.
- Wormhole: A tunnel is created between two nodes that can be utilized to secretly transmit packets.
- Packet dropping. A node drops data packets that it is supposed to forward.
- Routing Loop : A loop is introduced in a route path
- Denial - of - Service: A node is prevented from receiving and sending data packets to its destinations.
- Fabricated route messages: Route messages with malicious contents are injected into the network. Specific methods include
    - False Source Route: An incorrect route is advertised into the network thereby setting the route length to be 1 regardless where the destination is.
    - Maximum sequence: Modify the sequence field in control messages to the maximum allowed value.
    - Cache Poisoning: Information stored in routing tables is either modified, deleted or injected with false information.
    - Selfishness: A node is not serving as a relay to other nodes.
    - Rushing: This can be used to improve fabricated route messages.
    - Spoofing: Inject data or control packets with modified source address.

4. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

4.1 Based on data collection mechanisms

An intrusion detection system (IDS) can be classified as network-based or host-based according to the audit data that is used [8, 9].

1) Network Based (NIDS):

Network-based IDS runs on a gateway of a network and captures and examines the network traffic that flows through it. Obviously this approach is not suitable for ad hoc networks since there is no central point that allows monitoring of the whole network. The NIDS are broader in scope, are able to detect attack from outside, examine packet header and entire packet. The problem with NIDS is that it has high false positive rate.

2) Host Based (HIDS):

A host-based IDS relies on capturing local network traffic to the specific host. This data is analyzed and processed locally to the host and is used either to secure the activities of this host, or to notify another participating node for the malicious action of the node that performs the attack. It is better for detecting attack from inside but it responds after suspicious log entry.

4.2 Based on detection techniques

1) Signature or Misuse based IDS:

Misuse detection uses a priori knowledge on intrusions and tries to detect attacks based on specific patterns or signatures of known attacks. Although misuse detection systems are very accurate in revealing known attacks, their basic disadvantage is that attacking mechanisms are under a continuous evolution, which leads to the need for an up-to-date knowledge base [13].

2) Anomaly based IDS:

Anomaly detection has the advantage of being able to discover unknown attacks while it adopts the approach of knowing what is normal. As a result it attempts to track deviations from the normal behaviors that are considered to be anomalies or possible intrusion [14].

3) Specification based IDS:

The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints [21].

5. ARCHITECTURE OF IDS

Based on the network infrastructures, the ad hoc network can be configured to either flat or multi-layer. The optimal IDS architecture for the ad hoc network may depend on the network infrastructure itself.

There are four main architectures on the network, as follows:

1. In the standalone architecture, the IDS runs on each node to determine intrusions independently. There is no cooperation and no data exchanged among the IDSes on the network. This architecture is also more suitable for flat network infrastructure than for multilayered network infrastructure [12].
2. The distributed and collaborative architecture in which every node in the ad hoc network must participate in intrusion detection and response by having an IDS agent running on them. The IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently [5].
3. The hierarchical architecture is an extended version of the distributed and collaborative IDS architecture. This architecture proposes using multi-layered network infrastructures where the network is divided into clusters. The architecture has cluster heads which in some sense, act as control points which are similar to switches, routers, or gate ways in wired networks[17].
4. The mobile agent for IDS architecture uses mobile agents to perform specific task on a nodes behalf the owner of the agents. This architecture allows the distribution of the intrusion detection tasks. There are several advantages using mobile agents [15, 16], for intrusion detection.

6. RESEARCH ACHIEVEMENTS IN DISTRIBUTED IDS

Since the IDS for traditional wired systems are not well suited to Ad hoc network, many researchers have proposed several distributed IDS especially for ad hoc network, out of which some of them will be reviewed in this section.

Yian Huang et al. in 2003 proposed an Cooperative and Distributed algorithm in [5][20]. The model for an IDS agent is structured into six modules.

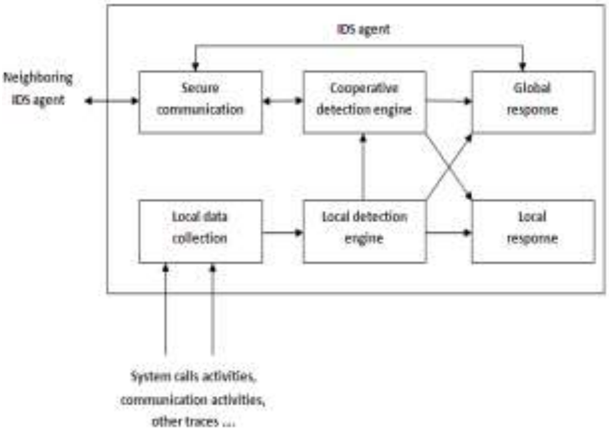


Figure 1. Cooperative and Distributed Model

The local data collection module collects real-time audit data, like system and user activities within its radio range. This collected data are analyzed by the local detection engine module for evidence of anomalies. If an anomaly is detected with strong evidence, the IDS agent can determine independently that the system is under attack and initiate a response through the local response module or the global response module , depending on the type of intrusion, the type of network protocols and applications, and the certainty of the evidence. If an anomaly is detected with insufficient evidence, the IDS agent can request the cooperation of neighboring IDS agents through a cooperative detection engine module, which communicates to other agents through a secure communication module.

Kachirski and Guha in 2002 have given algorithm of distributed with multiple sensors in [17]. It is a multi-sensor intrusion detection system based on mobile agent technology. The system is divided into three main modules, each of which represents a mobile agent with certain functionality: monitoring, decision-making or initiating a response. It divides functional tasks into categories and assigning each task to a different agent, the workload is distributed which is suitable for the characteristics of ad hoc networks. In addition, the hierarchical structure of agents is also developed in this intrusion detection system as shown in figure 2.

- Monitoring agent: Network monitoring and Host monitoring are done by the agents of this class.
  - A host-based monitor agent hosting system-level sensors and user-activity sensors is run on every node to monitor within the node
  - A monitor agent with a network monitoring sensors run only on some selected nodes to monitor at packet-level to capture packets going through the network within its radio ranges.
- Action agent: Every node also hosts this action agent. Since every node hosts a host-based monitoring agent, it can determine if there is any suspicious or unusual activities on the host node based on anomaly detection. When there is strong evidence supporting the anomaly detected, this action agent can initiate a response, such as terminating the process or blocking a user from the network.

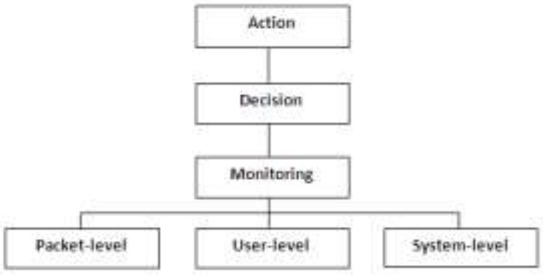


Figure 2: DIDS Using Multiple Sensors

- Decision agent: The decision agent is run only on those nodes only which run network monitoring agents. These nodes collect all packets within its radio range and analyze them to determine whether the network is under attack.

Moreover, if the local detection agent not able to make a decision on its own due to unsatisfactory evidence, it reports to the decision agent for investigate further. This is done by using packet-monitoring results that comes from the locally running network monitoring sensor. If the decision agent concludes that the node is malicious, the action module of the agent running on that node will carry out the response. The network is logically divided into clusters with a single clusterhead for each cluster. This cluster head will monitor the packets within the cluster whose originators are in the same cluster are captured and investigated. This means that the network monitoring agent and the decision agent run on the clusterhead. In this mechanism, the decision agent performs the decision making based on its own collected information from its network-monitoring sensor; thus, other nodes have no influence on its decision. This way, spoofing attacks and false accusations can be prevented.

A.Mitrokotsa et al. in 2006 proposed a distributed model in [10]. The proposed intrusion detection system is composed of multiple local IDSs agents. Each IDS agent (Figure 3) is responsible for detecting possible intrusions locally. The collection of all the independent IDS agents forms the IDS system for the mobile wireless ad hoc network.

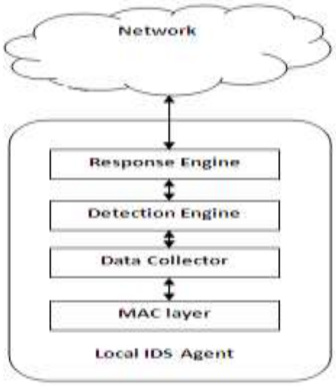


Figure 3: IDS with Multiple Local IDS

Each local IDS agent is composed of the following components:
Data Collector: Responsible for selecting local audit data and activity logs.
Detection Engine: Responsible for detecting local anomalies using local audit data. The local anomaly detection is performed using the eSOM classification algorithm. The procedure that is followed in the local detection engine is the one described below:

- Select labeled audit data and perform the appropriate transformations.
- Compute the classifier using training data and the eSOM algorithm.
- Apply the classifier to test local audit data in order to classify it as Normal or Abnormal.

Response Engine: If an intrusion is detected by the Detection Engine then the Response Engine is activated. The Response Engine is responsible for sending a local and a global alarm in order to notify the nodes of the mobile ad hoc network about the incident of intrusion. Special attention should be paid on the function of the Response Engine in order to avoid possible flooding caused by the notification messages of intrusion. Thus, the broadcasted notification of intrusion is restricted to a few hops away from the node where the anomaly has been detected since the neighboring nodes run the greatest risk of possible intrusion. When the Response Engine is activated, the node fires a fake RTS (Ready to Send) message destined to the suspicious node. If the suspicious node replies to that packet then the node is classified as malicious.

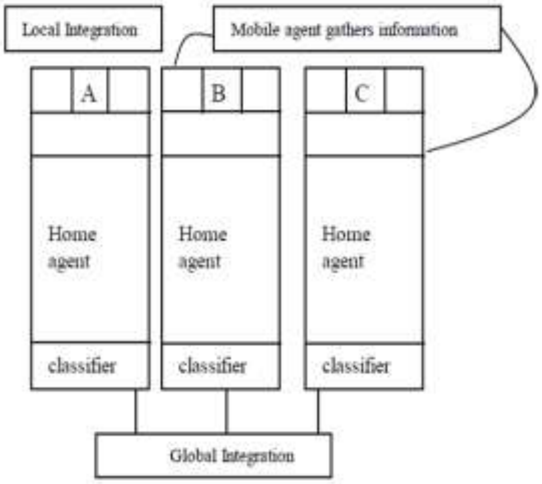


Figure 4: Agent Based cooperative and distributive model

Otherwise, the node fires an AODV ERROR message as the suspicious node is indicated as moved. After the discovery of the adversary the local IDS agent fires an ALERT message notifying its one hop neighbors. Alternatively, the local IDS agent could send ALERT messages to all potentially traffic generators that exist in its routing table, thus achieving a global response to all nodes that are directly influenced by the malicious node.

R.Nakkeeran et al. in 2010 proposed an Agent Based cooperative and distributive model in [15]. This model provides the three different techniques to provide sufficient security solution to current node, Neighboring Node and Global networks. The following section outlines each module’s work in detail.
1) Home agent**:** Home agent is present in each system and it gathers information about its system from application layer to routing layer.

a) ***Current node:*** Home Agent is present in the system and it monitors its own system continuously. If an attacker sends any packet to gather information or broadcast through this system, it calls the classifier construction to find out the attacks. If an attack has been made, it will filter the respective system from the global networks. Percentage of anomaly is calculated as follows :
Percentage = Number of predicted abnormal class
X 100/Total number of traces

b) ***Neighboring node****:* Any system in the network transfer any information to some other system, it broadcast through intermediate system. Before it transfer the message, it send mobile agent to the neighboring node and gather all the information and it return back to the system and it calls classifier rule to find out the attacks. If there is no suspicious activity, then it will forward the message to neighboring node.

c) ***Data collection****:* Data collection module is included for each anomaly detection subsystem to collect the values of features for corresponding layer in a system. Normal profile is created using the data collected during the normal scenario. Attack data is collected during the attack scenario.

d) ***Data preprocess:*** The audit data is collected in a file and it is smoothed so that it can be used for anomaly detection. Data preprocess is a technique to process the information with the test train data. In the entire layer anomaly detection systems, the above mentioned preprocessing technique is used.

2) Cross feature analysis for classifier sub model construction.

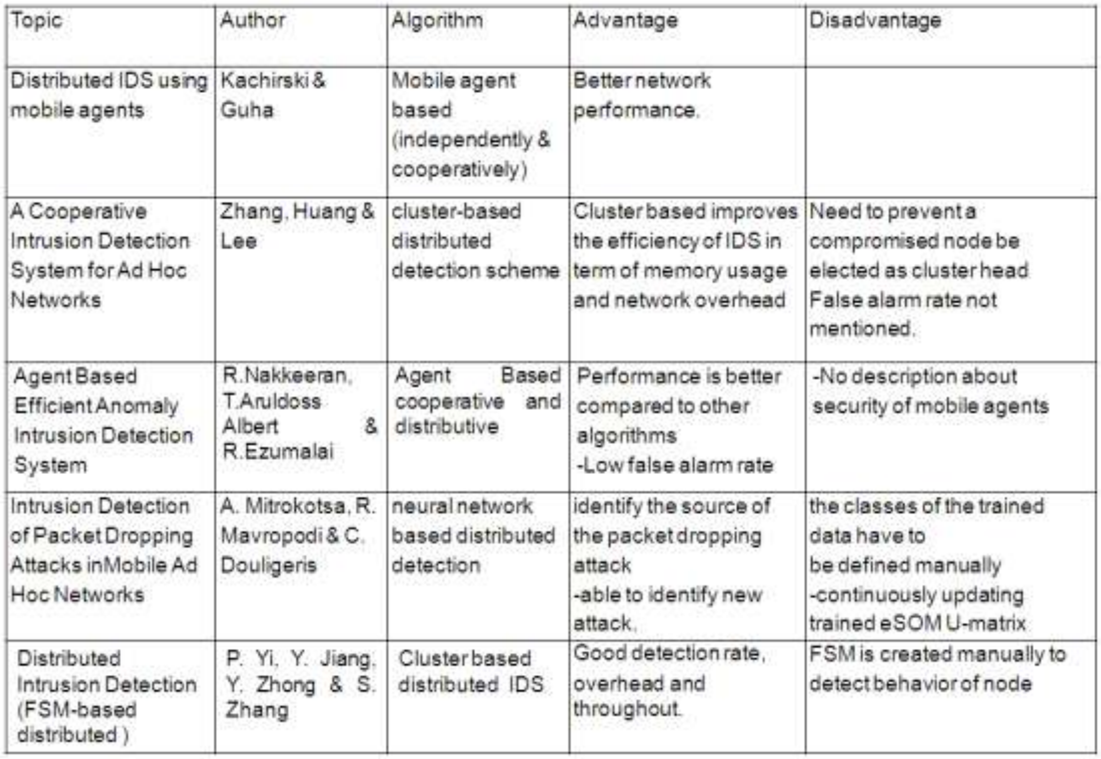
3) Local integration: Local integration module concentrate on self system and it find out the local anomaly attacks. Each and every system under hat wireless networks follows the same methodology to provide a secure global network.

4) Global integration: Global integration module is used to find the intrusion result for entire network. The aim of global integration is to consider the neighbor node(s) result for taking decision towards response module.

Ping Yi et al. in 2005 gave a distributed algorithm based on FSM in [21]. A network monitor is the node which monitors the behavior of nodes within its monitor zone. The monitor in a zone is selected by competition. A monitor employs a finite state machine (FSM) for detecting incorrect behavior in a node. It maintains a FSM for each data flow in each node. According to the author, node checks each ROUTE REQURE, ROUTE REPLY, ROUTE ERROR, DATA and if find any maliciously modified entry then go to alarm as shown in FSM below. There are five different FSM for different packets as discussed above. FSM-based intrusion detection system can detect attacks on the DSR. In the system, firstly we propose an algorithm of selecting monitor for distributed monitoring all nodes in networks.

Secondly, we manually abstract the correct behaviors of the node according as DSR and compose the finite state machine of node behavior. Intrusions, which usually cause node to behavior in an incorrect manner, can be detected without trained date or signature. Meanwhile, our IDS can detect unknown intrusion with fewer false alarms. As a result, we propose a distributed network monitor architecture which traces data flow on each node by means of finite state machine.

Table 1. Comparison of different Distributed IDS



Topic	Author	Algorithm	Advantage	Disadvantage
Distributed IDS using mobile agents	Kachirski & Guha	Mobile agent based (independently & cooperatively)	Better network performance.	
A Cooperative Intrusion Detection System for Ad Hoc Networks	Zhang, Huang & Lee	cluster-based distributed detection scheme	Cluster based improves the efficiency of IDS in term of memory usage and network overhead	Need to prevent a compromised node be elected as cluster head False alarm rate not mentioned.
Agent Based Efficient Anomaly Intrusion Detection System	R.Nakkeeran, T.Aruldoss Albert & R.Ezumalai	Agent Based cooperative and distributive	Performance is better compared to other algorithms -Low false alarm rate	-No description about security of mobile agents
Intrusion Detection of Packet Dropping Attacks inMobile Ad Hoc Networks	A. Mitrokotsa, R. Mavropodi & C. Douligeris	neural network based distributed detection	identify the source of the packet dropping attack -able to identify new attack.	the classes of the trained data have to be defined manually -continuously updating trained eSOM U-matrix
Distributed Intrusion Detection (FSM-based distributed)	P. Yi, Y. Jiang, Y. Zhong & S. Zhang	Cluster based distributed IDS	Good detection rate, overhead and throughout.	FSM is created manually to detect behavior of node

Ricardo Puttini et al. in 2007 has developed a fully distributed algorithm described in [18]. In fully distributed IDS distribution is not restricted to data collection but also applied to execution of the detection algorithm and alert correlation. Each node in the MANET runs a local IDS (LIDS) that cooperates with others LIDS. A mobile agent framework is used to preserve the autonomy of each LIDS while providing a flexible technique for exploring the natural redundancies in

MANET to compensate for the dynamic state of wireless links between high mobility nodes. The proposed solution has been validated by actual implementation, which is described in the paper. Three attacks are presented as illustrative examples of the IDS mechanisms. Attack detection is formally described by specification of data collection, attack signatures associated with such data and alerts generation and correlation.

7. CONCLUSION

Intrusion prevention techniques alone are not enough to secure ad hoc network. Hence a more efficient intrusion detection system is required. Among existing distributed intrusion detection algorithms, anomaly detection systems are more economic due to distributed nature of ad hoc network. To give clear view about DIDS we have presented details about different DIDS. In future we intend to develop new algorithm with machine learning based approach and compare it with existing techniques.

8. REFERENCES

[1] Ali Ghaffari. ”Vulnerability and Security of Mobile Ad hoc Networks”, Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006.

[2] Karan Singh, R. S. Yadav, Ranvijay, ”A REVIEW PAPER ON AD HOC NETWORK SECURITY”,International Journal of Computer Science and Security, Volume (1): Issue (1)

[3] Levente Butty, Jean-Pierre Hubaux,. ”Report on a Working Session on Security in Wireless Ad Hoc Networks”,Mobile Computing and Communications Review,Volume 6, Number 4

[4] Pin Nie, ”Security in Ad hoc Network”,2006.

[5] Yian Huang, Wenke Lee, ”A Cooperative Intrusion Detection System for Ad Hoc Networks”, In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pages 135147, Fairfax, Virginia, 2003. ACM Press.

[6] S.Madhavi,Dr. Tai Hoon Kim, ”AN INTRUSION DETECTION SYSTEM IN MOBILE ADHOC NETWORKS”, International Journal of Security and Its Applications Vol. 2, No.3, July, 2008

[7] Adam Burg,”Ad hoc network specific attacks,” 2003.

[8] Ioanna Stamouli,”Real-time Intrusion Detection for Ad hoc Networks”, in 2003.

[9] Tiranuch Anantvalee,Jie Wu, ”A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” c 2006 Springer.

[10] AikateriniMitrokotsa, Rosa Mavropodi, Christos Douligeris,”Intrusion Detection of Packet Dropping Attacks inMobile Ad Hoc Network” TAyia Napa, Cyprus, July 6-7, 2006.

[11] Himani Bathla, Kanika Lakhani, ”A Novel Method for Intrusion Detection System to Enhance Security in Ad hoc Network”, JOURNAL OF COMPUTING, VOLUME 2, ISSUE 5, MAY 2010, ISSN 2151-9617

[12] Satria Mandala, Md. Asri Ngadi, A.Hanan Abdullah, ”A Survey on MANET Intrusion Detection”, in: International Journal of Computer Science and Security, Volume (2) : Issue (1).

[13] Farooq Anjum,Dhanant Subhadrabandhu and Saswati Sarkar, ”Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols”, in 2003

[14] P C Kishore Raja, Dr.M.Suganthi.M, R.Sunder, ”WIRELESS NODE BEHAVIOR BASED INTRUSION DETECTION USING GENETIC ALGORITHM”,Ubiquitous Computing and Communication Journal,2006.

[15] R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai,”SAgent Based Efficient Anomaly Intrusion Detection System in Adhoc networks”,IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.

[16] Sampathkumar Veeraraghavan, S. Bose, K. Anand and A. Kannan, ”SAn Intelligent Agent Based Approach for Intrusion Detection and Prevention in Adhoc Networks”,IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24, 2007.

[17] O. Kachirski and R. Guha, ”Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks” Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS’03), p. 57.1, January 2003.

[18] Ricardo Puttini,Jean-Marc Percher, ”A Fully Distributed IDS for MANET”, in 2007.

[19] Adrian P. Lauf, Richard A. Peters, and William H. Robinson,”Distributed Intrusion Detection System for Resource-Constrained Devices in Ad Hoc Networks”,in 2008.

[20] Yongguang Zhang,Wenke Lee,Yian Huang, ”Intrusion Detection Techniques for Mobile Wireless Networks”,Appear in ACM WINET Journal in 2003.

[21] Ping Yi, Yichuan Jiang, Yiping Zhong, Shiyong Zhang, ”Distributed Intrusion Detection for Mobile Ad Hoc Networks”,Proceedings of the The 2005 IEEE Symposium on Applications and the Internet Workshops AINT-W05.