Proceedings of the 2007 IEEE International Conference on Telecommunications and
Malaysia International Conference on Communications, 14-17 May 2007, Penang, Malaysia

Distributed Hierarchical IDS for MANET over AODV+

Bahareh Pahlevanzadeh and Azman Samsudin
School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia.
baha@cs.usm.my, azman@cs.usm.my

***Abstract*—In this paper, we introduce background knowledge of wireless ad hoc network in *mobile ad hoc networks (MANET)* as well as *intrusion detection systems (IDS)* and *mobile agents*. This research study surveys, studies and compares the existing intrusion detection based on mobile agent for mobile ad hoc networks. Based on our best knowledge from previous researches we design *distributed hierarchical IDS* inclusive of network-based and host-based intrusion detection system with due consideration to their characteristics on *ad hoc on-demand distance vector routing protocol (AODV+)*. In addition, distributed hierarchical IDS model consists of two layers, cluster member layer and cluster head layer. Designing distributed hierarchical IDS is the main part of our methodology, where we try to show some improvement for ideal and accurate IDS for wireless ad hoc network. We propose some enhancement based on the characteristics and measure the efficiency of IDS in term of accuracy and detection rate and CPU usage.**

***Index*—Ad Hoc On-demand Distance Vector (AODV+), Distributed Hierarchical IDS, Mobile Ad Hoc Network (MANET), Mobile Agent and Network Simulator (NS2).**

I. Introduction

Wireless local area network (WLAN) was introduced around 1980, and just in few past years, wireless ad hoc networks have received significant attention because of their unique facilities [1]. Wireless ad hoc network applications are becoming more popular where wired networking is not available or wiring not economically feasible. With improvement of wireless ad hoc network applications and mobile devices, security becomes one of the main problems, which ad hoc networks confront nowadays. Just like any other network, ad hoc networks experience common security vulnerabilities that cause attacks such as denial of service attack, intruding, spoofing, eavesdropping and signal jamming. Furthermore, preservation of security, reliability, intentional jamming and latency are considerable in a wireless ad hoc network [2]. So there are some motivations to improve security in ad hoc networks (by using some intrusion prevention and detection techniques) that caused us to carry out this research study.

In general, a wireless ad hoc network divides into two types: Mobile Ad Hoc Network (MANET) and Wireless Sensor Network (WSN). In this study we focus more on MANET due to their mobility and their minimal resource requirement. MANET has unique characteristics like mobility, scalability, self-organizing, dynamic network topology, decentralized network control, low-power and resource-limited operation etc. These characteristics make MANET more vulnerable to several types of attacks and physical security threats than fixed wired networks. These properties introduce several problems relating to security of ad hoc network, which is a complex task. Therefore, securing wireless ad hoc networks is a highly challenging issue.

The main problem of this research is how to design a good and ideal intrusion detection system (IDS) that could cover the effective IDS requirements especially accuracy to explore the development of security in a MANET. Although an autonomous, stand-alone MANET is useful in many cases, a MANET connected to the Internet is much more desirable. This interconnection is achieved by using an extended routing protocol called AODV+ [3]. So the main scope of our work is new design and implement of efficient distribution of mobile agents with specific IDS tasks according to their functionality over a MANET that has connection to the Internet by AODV+, and study the effect of the proposed IDS.

II. Intrusion Detection System

A. Intrusion Detection System Definition

IDS can be defined as the guard system that automatically detects malicious activities within a host or a network, and consequently generates an alarm to alert the security apparatus at a location if intrusions are considered to be illegal on that host or network.

B. Intrusion Detection System Classification

There are several ways to categorize an IDS. In many simple IDS implementation, several categories are combined in a single device. Particularly, we described two main IDS classification. First category is based on the technique of intrusion detection and analysis strategy, which have two main types and one hybrid model. These three broad categories of IDS can be used on host-based and network-based IDS systems.

1) Anomaly-Based Detection
2) Signature-Based Detection (Misuse Detection)
3) Specification-Based Detection (Hybrid Detection)

Second category is based on data collection mechanism and monitoring activity, either on single-host or on multiple-host within network:

1) Network-based IDS (NIDS)

2) Host-based IDS (HIDS)

Generally, NIDS uses Signature-based detection and HIDS uses Anomaly-based detection. Each approach has its strengths and weaknesses; each is complementary to the other. A successful IDS will employ both technologies (HIDS and NIDS). In Table I, we compare NIDS and HIDS in case of their strengths and weaknesses to demonstrate how the two can work together to provide additional effective intrusion detection and protection.

C. Intrusion Detection System Requirements

Some papers [4]-[16] suggested IDS, which is one of the best solutions instead of intrusion protection against intruders (especially internal intruders) on MANET. The traditional way (firewall and cryptography) are design for known attacks and also each of these techniques comes with overhead and complexity. Unlike firewall that is the first line of defense and monitors border nodes to detect the external attacks, IDS appears just after an intrusion has happened and a node or network has been compromised. On the other hand intrusion detection monitors internal attacks as well as external attacks; that is why IDS is called as the second line of defense.

So far a few researches have been done in IDS for traditional fixed wired networks. However, applying the research of wired networks to wireless networks is not easy tasks. The efficiency of IDS solution that were designed for fixed wired networks are also limited for wireless ad hoc networks because of some special properties of wireless ad hoc networks. To overcome the problem we need to develop a systematic approach for designing the realistic IDS for MANET. Based on these aims the specialized MANET IDS is expected to support several of the following requirements [5]:

- An IDS should not introduce any weakness and overhead in the MANET.
- An IDS addition of detection should have a proper response.
- An IDS should itself be fault-tolerant and resistant to attacks, especially denial-of-service attacks.
- An IDS should use as little system resources as possible to detect and prevent intrusions.
- High accuracy of the IDS.

III. Related Work

In this section, we present a survey on the work that has been done on security of MANET in the area of IDS based on its architectures; and then we study the security of MANET based on mobile agent.

A. Security of MANET based on IDS Architecture

According to the system architecture, IDS for MANET security can be classified as Stand-alone, Distributed and Cooperative and Hierarchical IDS [6]-[9]. For better comparison, the details of these architectures are elaborated in Table II.

B. Security of MANET based on Mobile Agent

Mobile agents are intelligent and autonomous agent that can move through heterogeneous network and interact with nodes. For mobile agents to be useful for intrusion detection (whereas mobile agent platform is general-purpose software that enables organization to implement many different applications), it is necessary that many host and network devices are installed with a mobile agent platform. Contrast this with many expensive IDS schemes that assume every host is installed with a host-based IDS. This new approach (using mobile Agent for IDS in MANET) is not unusual to install a mobile agent in every host especially which has some features that are very useful in MANET [2], [4], [5], [10]-[12].

The followings are the main mobile agent's features that

TABLE I
EVALUATION OF NIDS AND HIDS AGAINST THEIR STRENGTHS AND WEAKNESSES

NIDS	HIDS
• Broad in scope	• Narrow in scope, monitor specific system activates
• Better for detecting attacks from outside and detect attacks that HIDS miss them	• Better for detecting attacks from inside and detect attacks that NIDS miss them
• Examines packet headers & entire packet	• Does not see packet headers
• Near real-time response	• Responds after a suspicious log entry
• Host independent	• Host dependent
• Bandwidth dependent	• Bandwidth independent
• No over load	• Over load
• Slow down the networks that have IDS clients installed	• Slow down the hosts that have IDS clients installed
• Detects network attacks, as payload is analyzed	• Detects local attacks before they hit the network
• Not suitable for encrypted and switches network	• Well-suited for encrypted and switches environment
• Does not perform normally detection of complex attacks	• Powerful tool for analyzing a possible attack because of relevant information in database
• High false positive rate	• Low false positive rate
• Lower cost of ownership	• Require no additional hardware

demonstrate straight relevance to the special challenging requirements found in MANET [13]:

- Conserving bandwidth
- Improving load balancing in the network
- Reducing the total tasks completion time
- Having robust and fault-tolerant behavior
- Working on a heterogeneous network
- Light-weight

These qualities make mobile agents a choice for security framework in MANET. Table III shows the details of some other researches on IDS, which is based on mobile agent.

IV. Infrastructure of Proposed Distributed Hierarchical IDS

Our proposed solution is using distributed hierarchical IDS for MANET. We apply HIDS for mobile devices and NIDS for Fixed devices. A successful IDS employs both technologies (HIDS and NIDS) to provide additional effective intrusion detection due to hierarchical architecture. For better visualization from our IDS architecture, we divide the IDS design for MANET with AODV+ routing protocol to two parts. The first part, which is when we have communication between wireless nodes and wired nodes (i.e. mixed network) and the second part, is when we have communication between wireless nodes.

A. IDS for Mixed Network

For this part, we apply NIDSes on gateways (which act as base station in mixed network) to capture all the live traffic of mixed network to develop an accurate IDS. Whenever suspicious features occur between wireless and wired nodes, NIDSes will detect them. As we know, the gateway and router are the best location to add IDS on network, because they can monitor and capture live packet traffic on the network. By referring to Table I we found NIDS has less overhead and it presents better accuracy because it is broad in scope and it can detect the attacks from outside.

B. IDS for Wireless Nodes

When we only have communication between wireless nodes, we apply the distributed hierarchical IDS model, which uses several mobile agents. The distributed hierarchical IDS model consists of two layers, cluster member layer and cluster head layer. A group of nodes that are close to each other is defined as a cluster [12]. We can define a node with the highest connectivity, processing power, energy remaining or bandwidth capabilities to be a cluster head, which has bi-directional links to all its members within the cluster. Fig. 1 shows the infrastructure overview of proposed distributed hierarchical IDS using mobile agents.

For the sake of modularity, the task of data collection, transmission and intrusion detection and response have been divided among different agents. The descriptions of the agents are as follow:

1) Mobile Data Collection Agent (MDCA): We distribute HIDS sensors that act as host monitoring on cluster member layer and we call them Mobile Data Collection Agent (MDCA). Each MDCA monitors and collects normal and abnormal features of each mobile node.

TABLE II
DIFFERENT PROPOSED IDS ARCHITECURES

PROPOSED SYSTEM	BY	METHODOLOGY	ARCHITECTURE	HIGHLIGHTS
Watchdog & Pathrate	Marti, Giuli & Lai (2000)	Each node runs a Sub-IDS that detect attack independently over DSR protocol	Stand-alone IDS	• Mitigate the effects of compromised nodes => Improve throughput(+) • Detect misbehave nodes at the forwarding level addition of link level (+) • Detect Byzantine Nodes but does not report to other nodes (-)
Distributed & Cooperative IDS	Zhang & Lee (2002)	Distributed Anomaly Detection	Distributed & Cooperative IDS	• Strong evidence => Detect locally and independently • Weak evidence =>Detect globally and cooperatively by voting • Anomaly detection => poor performance => high false alarm => more overhead (-) • Insecure and in efficient (-)
Real-time Intrusion Detection Ad hoc network (RIDAN)	Stamouli, Argyroud & Tewari (2003)	Misuse Detection and Specification-based Detection	Hierarchical	• Utilize TFSM to detect real time attacks (+) • Minimize the effectiveness of attacks (+) • Has less error compare with other researches (+) • Is not complete secure system (-)

(+) = Advantage, (-) = Disadvantage, TFSM= timed finite state machine, DSR= dynamic source routing.

TABLE III
DIFFERENT PROPOSED IDS BASED ON MOBILE AGENT

PROPOSED SYSTEM	BY	METHODOLOGY	ARCHITECTURE	HIGHLIGHTS
IDS Based on a Static Stationary Database (SSD)	Smith (2001)	• Mobile agent-based Anomaly , Misuse & Hybrid detection • Independently decision-making	Two parts: • Mobile IDS agent • Stationary secure data	• Mobile agents do intrusion detection by using five parts: ADM, MDM and etc. • The use of SSD limits communication between IDS agents • SSD stored in high physical security area ,but still this is in risk of attack (-) • Periodically up to date with non-mobile database(-)
Local Intrusion Detection System (LIDS)	Albers et al. (2002)	• Mobile Agent-based Distributed Anomaly detection • Independently decision making	Two key elements: • Several data collecting agents: o LIDS agent o Mobile agent o MIB agent • A common communication framework	• Use SNMP data located in MIB to process data, transmit SNMP requests to remote hosts to overcome the unreliability of UDP, by using mobile agent (+) • Cost of local information collection is negligible by running SNMP agent on each node (+)
Distributed IDS Using Mobile Agent	Kachirski & Guha (2002)	• Mobile Agent-based Anomaly detection • Independently & Cooperatively	• Multiple sensor types for specific function: • Network monitoring • Host monitoring • Decision making • Action	• Multiple sensors used to implement a bandwidth-conscious scheme • Distributed IDS make better network performance (+)
A Cooperative IDS Framework	Huang & Lee (2003)	• Cluster -based Anomaly detection • Independently & Cooperatively	• Special kind of clustering algorithm • Finite State Machine of the cluster-formation protocols	• Cluster-based improves the efficiency of IDS in terms of memory usage & network overhead (+) • Need to prevent a compromised node be elected as cluster head (-) • Not mention false alarm rate (-)

2) Transmission Agent (TA): After all information packets collected from cluster member layer, the information is then stored in Trace file by MDCA. We need to pass this information to the detection engine on the cluster head layer to be used in Intrusion Detection Agent. This task is done by Transmission Agent (TA).

3) Intrusion Detection Agent (IDA): We apply Intrusion Detection Agent (IDA) on each cluster head, which include a Decision Making Agent (DMA) and Cluster Response Agent (CRA). In fact, in this design we use modified independent decision-making because we have clustering algorithm with cluster head over the network. The modified independent decision-making is conducted when collected information using MDCA and TA has been sent to the particular node, which is cluster head. Then cluster head using anomaly detection engine independently analyses and make decision on the entire information inclusive normal and abnormal situation (intrusion). This is a novelty of our proposed IDS in comparison with the previous researches, which cause the low CPU usage. An IDA is not only able to detect an intrusion, but also can identify the possible attacker and send alarm to all cluster members. Whenever the intrusion is detected, the IDA can determine that the cluster is under attack and using CRA, a response can be initiated to prevent or minimize damage to the cluster. This response can initiate alarm to other cluster members.

4) Network Response Agent (NRA): Each cluster head acts as IDA for its cluster. After each cluster head independently detect and response to intrusion by IDA, NRA will be initialized and initiates extra response to all cluster member of another cluster and even fixed devices.

V. SIMULATION OF PROPOSED IDS

Network Simulator Version 2 (NS2) is used as the suitable test bed for this project [14]. The reason of choosing NS2 as the simulator is partly because of NS2 is an open source application where the code can be modified and extended as well as the range of features it provides. As Table IV shows, the simulated network consists of 2 hosts, 2 routers, 2 gateway and 15 mobile nodes. The topology is a flat rectangular area with 800 meter length and 500 meter width. The duration of simulation is 900 seconds. Five of the 15 mobile nodes use constant bit rate (CBR) traffic sources and they are distributed randomly within the mobile ad hoc network.

We must consider for mixed simulation (wired-communication-wireless), we need to use base-station (gateway) and hierarchical routing in order to rout packets

TABLE IV
COMMON PARAMETERS IN SIMULATION

NETWORK PARAMETER	VALUE
Topology Size	800m x 500m
Number of Mobile Nodes	15
Number of sources	5
Number of gateway	2
Traffic Type	CBR
Packet Rate	1,2,4 packets/s
Packet Size	512 ,600,1000 byte
Simulation Time	900
Transmission range	250 m
Pause Time	5s
Maximum Speed	0.1~ 10 m/s

m = meter, CBR= constant bit rate, s=second.

between wireless and wired domains. In this scenario we divide the task of gateway recovery and routing between 2 prepared gateways and 2 hosts. We define two clusters namely, cluster A and cluster B. Cluster A consists of 8 mobile nodes, in which 3 of them are consider as sources.

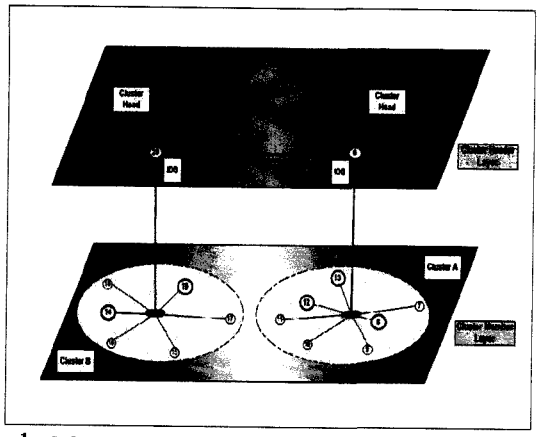

Fig. 1. Infrastructure Overview of Proposed Distributed Hierarchical IDS

In a portion of simulation time traffic flooding attack (a kind of Denial of Service attack) are presented by one of the sources. Cluster B also consist of 7 mobile nodes, in which 2 of them are consider as sources. In a portion of simulation time, the attack is presented by one of the sources. We choose starting time of sending data packets uniformly within the first 10 seconds of the simulation till one second before the end of the simulation. We apply the AODV+ routing protocol in reactive mode of gateway recovery. Screenshot of the simulation scenario using NAM window is shown in Fig. 2 The two hexagonal nodes are the gateways and the four square nodes are the two host and the two routers.

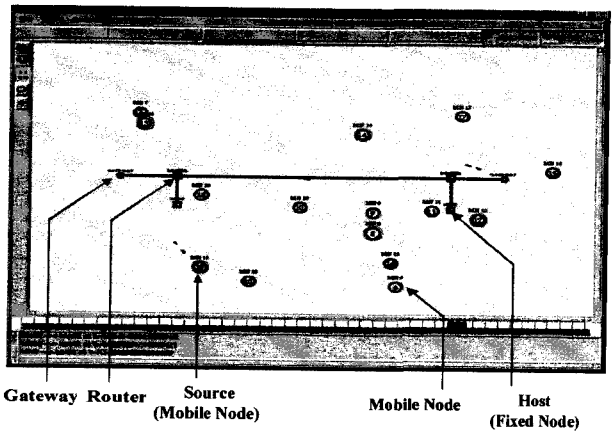

Fig. 2. A Screenshot of the Simulation Scenario

VI. TEST AND RESULTS

A. Test

We test our distributed hierarchical IDS based on two criteria: CPU usage and detection rate accuracy (based on number of attacks). For better understanding, we need to explain the testing part based on NS2 scenario in cluster A (same scenario for cluster B) and show the results in Fig. 3. The test parameters are based on the topology of our simulated network, which are presented in Table IV. We must consider these parameters are just sample values and they can be flexible.

We run our simulated MANET topology through AODV+ routing protocol, in where the source nodes generating normal packets using CBR generator (with 0.5 interval time or send rate of 2 packets/s and packet size 512 byte). Then one of the source that performs as an attacker (node Number 8 in cluster A and 14 in cluster B) tries to send abnormal packets to its target. We generate traffic flooding attack, which is a kind of Denial-of-Service (DoS) attack using CBR generator (with 0.25 interval time or send rate of 4 packets/s and packet size1000 bytes and 600 bytes). Again sources will continue to send normal packet to all cluster members and fixed hosts.

It should be noted that we generate different packet size with different interval time to distinguish between normal and abnormal packets. For instance, during the DoS attack, the flood is also CBR over UDP, but for better viewing of DoS traffic flooding attack and its force on high usage of network resources, we choose high send rate and big packet size compare with the normal packet size (512 byte) and normal send rate (2 packets/s).

For mixed network, NIDS on each node capture all the traffic and can easily detect abnormal packets. In the wireless nodes, which we applied distributed hierarchical IDS (also by applying different agents and with their cooperation), we can detect the attacks and identify the attacker.

B. Results

Based on the detection results, we can find number and duration of attacks. In addition, we can identify the attacker. Detection rate in simulation environment for our designed IDS is 100% and the number of attacks does not affect the accuracy of IDS. In addition accuracy, there is other measurement to evaluate the performance of distributed hierarchical IDS. This measurement is CPU usage. As we know for the sake of modularity, the task of IDS is divided among different agents.

When IDS is running, each agent uses some amount of CPU resource.

We compared our distributed hierarchical IDS (when we have modified independent decision-making by cluster head) with previous researches (which applied independent and collaborated decision making per node) in case of CPU usage.

We found the total CPU usage for IDS is due to several factors such as cluster head formation, running MDCA, TA, IDS and NRA. Total CPU usage of distributed hierarchical IDS (4.65%) is reduced in comparison with the distributed and cooperative IDS (6.00%). Fig. 3 shows, even under a high number of attacks, the CPU usage of distributed hierarchical IDS is still less than distributed IDS. Considering the significant performance from CPU usage based on number of attack, it is clear that overall, distributed hierarchical IDS is a far better approach than the distributed IDS for MANET.

VII. Analysis

A distributed hierarchical IDS, combining MDCA, TA,

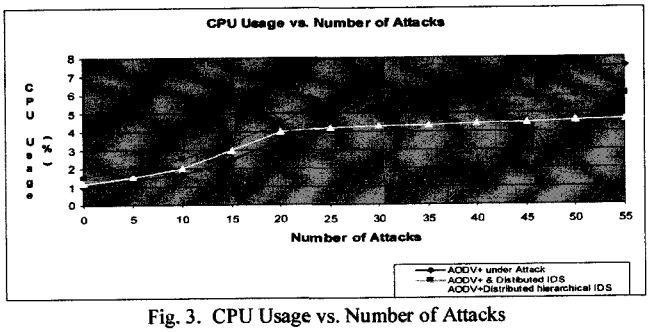

Fig. 3. CPU Usage vs. Number of Attacks

DMA, CRA and NRA, for MANET based on AODV+ routing protocol is the proposed in this research. The system not only has a higher overall detection rate and as a result high accuracy (100%), but also lessened the CPU usage (4.65%). Our experiment results showed that, even when we have the highest number of attacks, the level of detection and as a result the accuracy of our proposed IDS is stable at 100% , while reduces CPU utilization by 1.35%.

This accuracy is the result of anomaly detection and response, which is more powerful in compare with misuse detection. Some important factors for resource constrained equipment are overhead and CPU usage. The distributed hierarchical IDS has low CPU usage, which is the result of mobile agent and cluster-based intrusion detection.

VIII. Conclusion

The main objective of this research was to design and implement of efficient distributed hierarchical IDS using mobile agent over a MANET that has connection to the Internet by AODV+, and study the effect of the proposed IDS in case of accuracy and CPU usage. The outcome of the research should be the first IDS framework designed for AODV+ routing protocol.

In conclusion, the result demonstrates some improvement for ideal and accurate IDS based on mobile agent, clustering and distributed hierarchical IDS for wireless mobile ad hoc network. The result shows that we are successful in proposing some enhancement in case of efficiency of IDS in term of accuracy and CPU usage and confidently we exhibit the development of security in wireless mobile ad hoc networks.

References

[1] P. Brutch, and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks," *Applications and the Internet Workshops*, 2003, pp. 368–373.

[2] The National Institute of Standards and Technology.ANTDwebmaster.May,2001 . Mobile ad hoc network. Available: http://w3.antd.nist.gov

[3] A. Hamidian, "A Study of Internet Connectivity for Mobile Ad Hoc Networks in NS 2" , Master's thesis, Lund Institute of Technology, Sweden, January 2003, Available: http://www.telecom.lth.se/Personal/alexh/rapport.pdf

[4] O. Kachirski, and R. Guha, "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks". Proceedings of *the IEEE Workshop on Knowledge Media Networking*,2002, pp.153–158.

[5] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," Proceedings of *IEEE Personal Communications.* Vol. 11, 2004, pp. 48–60.

[6] Marti, S., Giuli, T., and Lai, K. 2000. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. Proceedings of *the Sixth Annual International Conference on Mobile Communication and Networking,* Boston, Massachussetts. 2(3). Page(s): 123–129.

[7] Y. Zhang, and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," Proceedings of *the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000)*, 2000.

[8] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *ACM/ Kluwer Wireless Networks Journal*, vol. 9, 2003, pp. 545–556.

[9] L. Stamouli, P.G. Argyroudis, and H. Tewari, "Real-time Intrusion Detection for Ad hoc Networks," Proceedings of *sixth IEEE International Symposium Computers and Communications,* June 2005, *pp.374 –380.*

[10] A. Smith, "An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks," *5th Nat'l, Colloq. for Info. Sys. Sec. Education*, 2001.

[11] P. Albers, O. Camp, Percher, J. Bernard , Ludovic and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," *1st Int'l. Wksp. Wireless Info. Sys.*,Ciudad Real, Spain, pp. 3–6, 2002.

[12] Y. Huang, and W. Lee, A Cooperative Intrusion Detection System For Ad hoc Networks. *In Proceedings of the 3th international conference on Distributed Computing systems,* vol 6, *2004*, pp. *1155–1168.*

[13] A. Hijazi, and N. Nasser, "Wireless Using mobile agents for intrusion detection in wireless ad hoc networks," Published *Second IFIP International Conference on March 2005*, pp. 362–366.

[14] S. McCanne, and S. Floyd, "*The Network Simulator - ns-2*", Available: http://www.isi.edu/nsnam/ns/ .

[15] B. Sun, H., Chenand, and L. Li, "An intrusion detection system for AODV," ICECCS 2005. Proceedings of 10th *IEEE International Conference on Engineering of Complex Computer Systems*, 2005, pp. 358–365.

[16] G. Vigna, S. Gwalani, K. Srinivasan, E.M. Belding-Royer, and R.A. Kemmerer, "An intrusion detection tool for AODV-based ad hoc wireless networks," *Computer Security Applications Conference*, 2004, 20th Annual 6-10 Dec., pp. 16–27.