Intrusion Detection Techniques in MANETs and WMNs

Bishal Pradhan[1], Samarjeet Borah[2]

Department of Computer Science & Engineering, Sikkim Manipal Institute of Technology
Majitar, East Sikkim, India, PIN-737136
Department of Computer Science & Engineering, Sikkim Manipal Institute of Technology
Majitar, East Sikkim, India, PIN-737136

ABSTRACT

Intrusion Detection plays a very important role as it marks the first line of defence [14]. In multi-hop wireless network, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks. So, the already existing intrusion detection technique in traditional networks doesn’t serve the purpose. Hence, a specialized intrusion detection schemes must be designed for MANETs and WMNs, which not only identify and classifies every network activities and as either normal or abnormal, but also be able to detect the malicious among the abnormal activities. Various intrusion detection mechanisms has been proposed or adopted for the purpose. This paper surveys the IDS schemes proposed for or deployed in MANETs and WMNs.

Keywords

Intrusion, Intrusion Detection, Intrusion Detection System (IDS), Mobile Ad-hoc Network (MANET), Wireless Mesh Network (WMN), Anomaly, Misuse, Response.

1. INTRODUCTION

Wireless networks are more vulnerable then wired networks to wide variety of attack, because of its openness as wireless radio medium is shared and accessible openly through the air. In a wired network, an attacker needs to physically be connected the network. In a wireless network, an attacker can listen to or consume or transmit packets on a radio link at from anywhere (possibly may not be visible). Thus, the openness makes wireless networks more attractive as targets as well as harder to defend. Mobile Wireless Ad Hoc Networks (MANETs) and Wireless Mesh Networks (WMNs) are the most recent advances in the wireless network technology which operates on multi-hop communication protocols with distributive, dynamic, ad-hoc and mobility as additional features. [14] The mobility afforded by wireless nodes in WMNs and MANETs is great for users but certainly increases security implications. In WMNs mesh routers which are either static or with minimal mobility, form the backbone for mesh clients, but the mesh clients are mobile, and are free to move and join any part of the network. In MANET every node is mobile and hence presents even more challenges for security. In infrastructure based network mobile node may be authenticated with an authentication server that is always accessible regardless of the user’s location. However, in a MANET and WMNs, nodes may be connected to and disconnected from other nodes any point of time of time. Therefore, a centralized authentication facility would not work as it may not always be reached by a mobile node’s location. Authentication of mobile node in MANETs and WMNs is one of the prime requirements for secure communication.

In order to safeguard the MANETs and WMNs from possible intrusion from attackers; a decentralized, cooperative, adaptive and efficient intrusion detection scheme is needed which incorporated all the aspects of the WMNs as well as MANETs. So, the traditional wired-based IDS scheme does not serve the security cause of MANTEs and WMNs. Therefore, a new scheme must be designed, either by upgrading the existing IDS with those additional features or by designing entirely new detection scheme.

2. BACKGROUND

The pre-requisite of the survey are as follows:

A. *Intrusion*

Intrusion is an act of gaining unauthorized access to a computer, information in transmission, and network resources by an intruder.

B. *Intrusion Detection*

Intrusion detection is the process of detection of any actions that attempt to compromise the confidentiality, integrity or availability of a resource.

C. *Intrusion Detection System (IDS)*

An IDS is a device or software application that monitors network and/or system activities for malicious activities or protocol violations and alert system administrators about possible attacks, ideally in time to stop the attack or mitigate the damage.

D. *IDS Architectures*

IDWG (Intrusion Detection Working Group) [12] recommends a general IDS architecture which considers the following four functional modules:

- E–box: Are sensor elements that monitor the target system, by acquiring network event information.
- D–box: Stores information from E blocks for subsequent processing by A and R boxes.
- A–box: Processing modules for analysing events and detecting potential intrusive behaviour on the target system.
- R–box: If any intrusion is detected this module is responsible for raising an alarm to inform the system administrator.

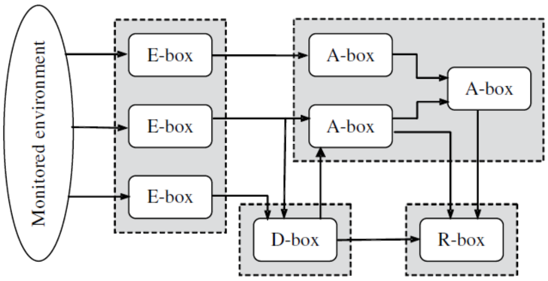

Fig. 1: General IDWG architecture for IDS [12]

Based on the network infrastructures, the MANET and WMN can be configured to either flat or multi-layer.

The optimal IDS architecture may depend on the network infrastructure itself. [14] There are four types of IDS architectures identified as follows:

- Standalone IDS: Each node is equipped with IDS mechanism to determine intrusions independently. The nodes do not cooperate with others in the network and hence does not exchange intrusion information among them. This architecture is more suitable for flat network.
- Distributed and Collaborative IDS: It works by cooperative mechanism to detect the truly malicious activities and distribute the alert to other nodes in the network. So it requires every node to participate in intrusion detection and response by having an IDS agent running on them. The IDS agent is responsible for collecting local events and data to identify possible intrusions, detecting the intrusion and generate an alert to other nodes in case of intrusion.
- Hierarchical IDS: It 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. Each of the clusters has cluster heads which are responsible for detection and alerting the member nodes in case of the intrusion, to the respective cluster.
- Mobile Agent for IDS: It uses mobile agents to collect activities in the network of nodes or its neighbour nodes. The information collected is then analysed by the IDS node for intrusion. This architecture allows the distribution of the intrusion detection tasks.

E. *Functions of IDS*

IDS essentially consist of three functionalities:

- Firstly, IDS must collect data by monitoring some type of networking events.
- Secondly, an analysis engine that processes the collected data. It is equipped with intelligence to detect unusual or malicious signs from the collected data.
- The third functional part is a response, which is typically an alert to system administrators or the network itself. A system administrator is responsible for follow-up investigation of an event after receiving an alert.

F. *IDS Approaches*

On the basis of monitoring events, [6, 10, 14] IDS can be classified into two types: *Host-based IDS* are installed on hosts and monitor their internal events, usually at the operating system level. These internal events are the type recorded in the hosts audit trails and system logs. In contrast, *Network-based IDS* monitor packets in the network. This is usually done by setting the network interface on a host to promiscuous mode (so all network traffic is captured, regardless of packet addresses). Alternatively, there is specialized protocol analysers designed to capture and decode packets at full link speed.

G. *IDS Models*

Currently there are two basic models [2, 8, 11, 12, 14] designed to perform analysis. *Misuse detection model* requires a database of signature of attacks. It works by matching the signature of the event with that of its database. If a matching signature is found, that attack is detected, everything else is assumed to be normal. This model is accurate in detecting known attack. But, it fails to detect the new attack which leads to high rate of false negative. So, signature must be developed, distributed and updated whenever new attacked is discovered.

Anomaly detection model, on the other hand works by comparing behaviour of each nodes with respect to some normal profile [12]. The normal behaviour of nodes contributes towards characterization as normal profile. Anomaly detection tries to works by characterize behaviour of a node, if the behaviour deviates towards normal profile then it normal behaviour and else is assumed to be anomalous, although may not necessarily be malicious. This model is the capable of detecting new attacks without prior experience. However, the main difficulty is characterization of normal profile because normal behaviour can have large deviations and there is no full proof rules saying which statistical metric to be considered for characterizing an accurate normal profile. Secondly, it is not necessary that an anomalous behaviour is always malicious. Only a small fraction of anomalous activities may turn out to be malicious. Thus, anomaly detection model often produces high rate of false negatives. Thirdly, even though if anomaly is detected it cannot not identify a specific attack, unlike a signature. Although they works entirely opposite, they can be used together to realize the advantages of both approaches.

H. *IDS Response* [14]

Detection of an intrusion must generate some type of response which may be used to alert system administrator or the other nodes in the network. There can be two types of response: passive or active.

A passive response logs the intrusion information and raises an alert to system administrators. It does not attempt to stop the intrusion. It is up to the system administrator as it is believed that human judgment is required to formulate the most appropriate course of action.

In active responses, as the intrusion is detected, it attempts to limit the damage of an attack or stop an attack in progress, this is called active response. With this scheme, damage can be mitigated by protecting the valuable assets or the specific target of the attack. Active response could also be helpful in tracking the source of the attack, which might be difficult if the attack is being carried out through intermediaries. But there is a risk in trying active responses as in the event of false positives, normal traffic is mistakenly identified as malicious.

I. *MANET*

A Mobile Ad-hoc Network or Mobile Wireless Ad-hoc Network is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Unlike WMN, since all the nodes in MANET are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology, routing, and packet transmission functionality must be incorporated into each mobile nodes. MANETs and WMNs are closely related, but there are some differences too.

J. *Wireless Mesh Network (WMN)*

A wireless mesh network (WMN) [9] is a communications network made up of dynamically self-organized and self-configured radio nodes organized in a mesh topology consisting of mesh clients, mesh routers and gateways. The mesh clients are the mobile end systems, such as laptops, cell phones and other wireless mobile devices which tend to change their locations over a period of time. On the other hand, the mesh routers are static parts of the WMNs which form the backbone infrastructure and are communicating wirelessly with each other and also forwarding traffic to and from the clients and gateways.

3. UNIQUE CHALLENGES OF MANETS AND WMNS

Intrusion detection is a prime requirement in wired as well as wireless networks. Deployment of IDS in wired network is well understood and relatively straightforward because the network environment is pretty much static as traffic is relayed by stationary routers. So there are natural points of traffic concentration which are logical candidates for IDS scheme. Whereas, wireless networks such as WMNs and MANETs present additional difficulties for intrusion detection due to their openness, dynamism, easy accessibility, mobility, decentralized natures. MANETs have no fixed infrastructure and are usually called infrastructure less network. All nodes are mobile and the network topology is purely dynamic. WMNs on the other hand is no different than MANETs, it just relaxes the requirement of no fixed infrastructure, and usually is a network of fixed and mobile nodes interconnected by wireless links. As in MANETs, mesh nodes can be simultaneously mobile end user devices and fixed or semi-fixed routers. These fixed nodes constitute a backbone infrastructure. Therefore, WMNs are referred to as Infrastructure based wireless network.

A principal characteristic of MANET and WMN is multi-hop routing, where packets traverse the network by opportunistic relaying from node to node [2,3,11,14].

A. Wireless Medium

The wireless medium allows any node to join the network in any part. So, an intruder easily enters the network. In wired networks, traffic is forced to travel along links, and there are natural points of traffic concentration which are convenient locations for intrusion detection. This is not valid in a multi-hop wireless network like WMNs and MANETs, even though there might be a backbone of fixed wireless routers in WMNs. Here, the traffic through each of the access points must be monitored. In practice, this is difficult because access points typically do not have SPAN ports that mirror the traffic. Also wireless traffic cannot be promiscuously monitored by eavesdropping on the radio medium is not ideal. On the other hand, Nodes in a wireless mesh network may have relatively short radio ranges, hence; sensors cannot see all the traffic. Deploying multiple sensors around the entire network for a comprehensive view of traffic is costly.

B. Mobility

One of the main difficulties of multi-hop wireless network is the mobility afforded to nodes. Mobile nodes might travel to hostile environment and will be an easy prey for intruder. Therefore, nodes in a WMNs and MANETs are more vulnerable to compromise and cannot be entirely trusted even if their identity is authenticated.

C. Dynamic Network Topology

This feature is very helpful in self-organization of network dynamically. It means there are no natural fixed points of traffic concentration which would be good choices for monitoring. A possible approach is to run IDS on certain hosts to monitor their local neighbourhoods. However, a node cannot be expected to monitor the same area for a long time due to its mobility. A node may be unable to obtain a large sample of data for accurate intrusion detection.

4. INTRUSION DETECTION SCHEMES FOR MANETS

Since, MANET affords openness, dynamism, mobility, easy accessibility and co-operation among nodes; the intrusion detection scheme must incorporate these aspects of MANETs. So far, many IDSs have been proposed for MANETs, which are fully explained in [1]. Most of them are either applied at network layer as secure routing protocol or on higher layers which somehow uses the routing mechanisms to monitor the nodes in the network. Some of these are:

A. WATCHERS

Watching for Anomalies in Transit Conservation: a Heuristic for Ensuring Router Security [1], is one of the earliest IDS scheme proposed for MANET, and used in distributed environment with link state routing protocol. The WATCHERS, works by analysing network traffic for anomalous and misbehaving nodes. Every node keeps the information of all the other nodes. Therefore, it requires more memory for keeping those records. It is a cooperative anomaly detection mechanism, implemented on every node, in which each node monitors their neighbours independently. If a node detects its neighbour misbehaving or found to be anomalous then it raises an alarm to notify other nodes. However, if a group of nodes are compromised, they can raise an alarm against an innocent node leading to false positive.

B. *Watchdogs and Pathraters* [8, 14]

It uses Dynamic Source Routing (DSR) routing protocol to detect network layer misbehaviours. Watchdog monitors the next hop's forwarding behaviour, while Pathrater analyses the results of the Watchdog, and then select most reliable path for packet delivery. The scheme is limited to source routing, and cannot detect packet dropped below the threshold value.

C. TIARA

Trust Management Intrusion Tolerance Accountability and Reconstitution Architecture [8, 14] detect path failure, and each message is encrypted with digital signature, which increases its cost.

D. CONFIDANT

Collaborative Object Notification Framework for Insider Defence using Autonomous Network Transactions [10, 11, 14] monitors and rates the reputation of its neighbours, and raises an alarm in case of intrusion. However, it can mostly detect only intrusions such as packets dropping.

E. CORE

Similar to CONIDENT is based on monitoring system and reputation system [5]. In this technique each node receives reports from other nodes. The difference between CORE and CONFIDANT is that CORE only allows positive reports to pass through, but CONFIDANT allows negative reports. This means that CORE prevents false reports.

F. *MOBIDS* [8, 14]

Mobile Intrusion Detection System is proposed for distributed environment, in which many nodes monitors the network and sets positive values for cooperating nodes while negative value for non-cooperating nodes. The rating of nodes is broadcast to all the neighbours. However, it cannot differentiate between the real noncooperation (malicious node) and noncooperation due to some hardware failure, low battery power.

G. AODVSTAT [8, 14]

It is based on AODV routing protocol. Sensors sense the radio channels, having two modes of operations. In standalone mode, sensor senses the attack only in its neighbours. In distributed mode, sensors periodically exchange information with the neighbours. It is a signature based approach, and how to update the attack signature files at all sensors in MANET has not been addressed.

The author of [2] has proposed a distributed intrusion detection system for ad hoc wireless networks based on mobile agent technology. Where an agent travels across network to be executed on a certain host to collect information and returns back to the originator. All the decisions, including network traversing, are left to an agent. These mobile agents are employed at several usage levels and process their response in cluster heads (special nodes that are elected using a distributed algorithm within a cluster).

The author of [3] has discussed an agent based anomaly detection techniques where the Home agents present in each node collects the data from its own system to observe the local anomalies. The mobile agent monitors the neighbouring nodes and collects the information from neighbouring home agents to determine the correlation among the observed anomalous patterns.

Apart from the above schemes various IDS schemes has been proposed. Here are some of them in brief. RESANE works by using trust model and calculate reputations to motivate cooperation in nodes. SCAN works in distributed environment and monitors all its neighbours independently for routing and packet forwarding misbehaviour, however it is limited to AODV routing protocol. In [8, 19], the authors proposed distributed IDS for mobile nodes. In [10], a rule based IDS is proposed, however, it cannot detect unknown attacks. Bansal and Baker [6] proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks), which is the enhanced version of DSR protocol. OCEAN also uses a monitoring system and a reputation system. OCEAN divides routing misbehaviour into two groups: misleading and selfish. If a node takes part in routes finding but does not forward a packet, it is therefore a misleading node and misleads other nodes. But if a node does not participate in routes finding, it is considered as a selfish node.

However, there are some efforts made to modify some routing protocols and enable them to detect some form of intrusion in MANETs. There are different proposal of modified version of AODV routing protocol to detect intrusions. Such as SEAODV (Security Extended AODV) is an on-demand routing protocol as same as AODV with security extension that verifies if route to the destination is secure by verifying the neighbour nodes consent. It uses Public key Infrastructure to generate GTK (Group Transient Key) for authentication of source of rout request and route reply, and PTK (Pair-wise Transient Key) for authentication of neighbour nodes. Another version of AODV called SAODV (Secure AODV) works by implementing public key cryptography for authentication of source of route request and route reply, and hash function to secure hope count. But this eradicates the adaptive feature of the AODV protocol. To enforce adaptive behaviour in multi-hop ad-hoc wireless network, an adaptive secure routing protocol A-SAODV has been proposed, which uses dual signature to authorize intermediate nodes to reply for a route request. Other routing protocol such as DSR, DSDV etc has also been calibrated for secure routing. In addition, some new ad-hoc routing protocol such as TORA, ARIADNE, ARAN has been proposed to address the issue of Intrusion in the MANET.

5. INTRUSION DETECTION SCHEMES FOR WMNS

Most of the research in intrusion detection pertains to MANETs [8] because wireless mesh networks are a relatively recent development. Till now, [2] there are no IDSs exclusively designed for WMN. However, all of the intrusion detection schemes for MANETs are relevant to WMNs with some modification.

Nodes in a WMN relay data in a cooperative manner as the same way as that of MANETs does [2]. Therefore, intrusion detection in the MANETs has direct relevance to intrusion detection in WMNs. However, the WMN has significant different characteristics. Therefore, proposing or designing any IDS, needs to consider the following unique characteristics of WMN.

- WMN consists of fixed backbone mesh routers and gateways infrastructure, which is not power constraint.
- Consist of also mobile nodes in ad-hoc mode.
- WMNs enable integration amongst other wireless networks such as WLANs, WMANs.
- Normally, traffic is from gateway toward the nodes through static multiple hops.

Keeping in view these differences, there is a need an IDS system which is specially designed or proposed exclusively for WMN [8].The IDS for WMN must consider its two levels, the end user mesh nodes and mesh routers. There are various IDS schemes proposed for WMNs which are either not yet implemented or under implementation phase.

Ferreira, Oliveira, Carrijo, Bhargava [4] has propose a hybrid IDS that uses a wavelet-based mechanism for anomaly detection in the wireless radio network, and a neural network-based mechanism to classify the intrusion. The wavelet part is strong in detecting anomaly and neural-network part is strong in pattern recognition. The neural network algorithm can always be trained on detected anomalies resulting in decrease in false positive. The idea is to combine the best of both.

Zhang, Abdesselam, Pin-Han, Xiaodong [9] has proposed a reputation-based anomaly detection scheme, called RADAR, for WMNs. The reputation is used for evaluating behaviour of each node by abstracting and examining appropriate observations, such as data packets. But it requires a secure and dependable reputation management mechanism to define, quantify and distribute the trust values of each node. The detection engine then employs a sequence-based and a frequency-based anomaly detectors to capture the behaviour of each node drifts in terms of reputation by examining their temporal and spatial properties respectively which may ultimately give higher degree of accuracy and lower false positive rate. It is implemented with DSR routing protocol to detect routing misbehaviour.

Wang, Wong, Stanley and Basu, [10] has proposed a Cross-layer Based Anomaly Detection in Wireless Mesh Network. It consists of a Data Collection Module, a Profile Training Module, an Anomaly Detection Module, and an Alert Generation Module. These four modules run on each mesh nodes and collaboratively accomplish the goal of detecting anomalous behaviours in WMN backbone. The Data Collection Module collects data samples from physical layer, data link layer, and network layer. Part of the data collection is conducted in a given safe environment which is for profile training purpose and construct the normal profile. In this phase, raw data sets are processed and loaded into profile training module in which machine learning algorithms are applied for pattern learning. Those patterns are saved as profile for future intrusion detection. Three different machine learning algorithms: Bayesian network, Decision tree, and Support Vector Machine (SVM) have been used for pattern matching purpose. The Anomaly Detection Module analyses the traced data for its normality or anomaly. Any observed behaviour that deviates significantly from the profile is considered as an anomaly. Alert will be triggered through the Alert Generation Module. Consequently, further detection or intrusion response action may be called to verify the malicious behaviour.

The author of [13] proposed a hierarchical proxy based IDS scheme which uses two new concepts of proxy and central console as well as implements multi-level hierarchical group topology to provide additional security in the system.

6. ANALYSIS OF THE SURVEY

Out of various schemes surveyed, it is very important to note down the important points and analyse how these schemes performs under different scenario. Here are some of the points that stand out after the survey:

- Almost all the IDS scheme works by cooperation among neighbour nodes and also distributive and mobility is taken care.
- Some of the schemes detects anomalous node, whereas some are capable of detecting misbehaving node.
- Some scheme requires cooperatively identifying each other nodes and each one rates others to let other know the behaviour of the node. But other issues such as node failure, hardware malfunctioning, network congestion may contribute to false positive.
- Scheme such as TORA, CONFIDANT, AODVSTAT works with the use of trust model.
- Some schemes such as SEAODV, SAODV, A-SAODV, TORA, ARIADNE etc are implemented as routing protocol.

The following table summarizes the analysis for the various schemes surveyed:

TABLE I: COMPARATIVE ANALYSIS ON VARIOUS IDS SCHEMES FOR MANET AND WMN

Parameters → **Schemes**	**Cooperation**	**Agent**	**Distributed**	**Authentication**	**Mobility**	**Anomaly detection**	**Misuse detection**	**Routing protocol used**
WATCHERS	Yes	No	Yes	No	Yes	Yes	No	LSR
Watchdogs and Pathraters	Yes	No	yes	No	Yes	Yes	No	DSR
TIARA	Yes	Yes	Yes	Yes, using Digital signature	Yes	Yes	No	Any
CONFIDANT	Yes	No	Yes	No	Yes	No	Yes	DSR
CORE	Yes	No	Yes	No	Yes	No	Yes	DSR
SAODV	Yes	No	Yes	Yes using public key cryptosystem	Yes	Yes	No	Self
SEAODV	Yes	No	Yes	Yes using public key cryptosystem	Yes	Yes	No	Self
A-SAODV	Yes	No	Yes	Yes using public key cryptosystem, and dual signature	Yes	Yes	No	Self
ARIADNE	Yes	No	Yes	Yes using symmetric cryptosystem	Yes	Yes	No	Self
TORA	Yes	No	Yes	Yes	Yes	Yes	No	Self
MobIDS	Yes	Yes, mobile	Yes	No	Yes	Yes	No	Any
AOVSTAT	Yes	Yes	Yes	Yes	Yes	No	Yes	AODV
RADAR	Yes	No	Yes	No	Yes	Yes	No	DSR

7. CONCLUSION

This survey paper basically covers the study of security issues and challenges of MANETs and WMNs and study and analysis of various Intrusion Detection Schemes proposed for them.

This survey can be summarized as:

- Not all abnormal activities in the network are intrusions; hence detection of intrusion requires an intelligent and well informed system.
- The IDS scheme proposals are mostly for MANETs.
- Different approach has been applied to tackle different type of techniques. Most of them either uses routing protocol or has been proposed as new routing protocol.
- Since WMN is a relatively recent development, there is less work done in this field. But those of MANETs are not directly relevant to WMNs.
- There is an urgent need of efficient IDS for WMNs, as this technology is declared as next generation broadband technology.

8. REFERENCES

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

[2] Oleg Kachirski, Ratan Guha, “Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks”, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS’03) IEEE, 2006.

[3] R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai, “Agent Based Efficient Anomaly Intrusion Detection System in

Adhoc networks", IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.

[4] Ed' Wilson Tavares Ferreira, Ruy de Oliveira, Gilberto Arantes Carrijo, Bharat Bhargava, "Intrusion Detection in Wireless Mesh Networks Using a Hybrid Approach", 29th IEEE International Conference on Distributed Computing Systems Workshops, 2009.

[5] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Communication and Multimedia Security Conference (CMS'02), September 2002.

[6] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Research Report cs.NI/0307012, Stanford University, 2003.

[7] Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi, "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes", World Academy of Science, Engineering and Technology, 44, 2008.

[8] Shafiullah Khan, Kok-Keong Loo, Zia Ud Din, "Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks", The International Arab Journal of Information Technology, Vol. 7, October 2010.

[9] Zonghua Zhang, Farid Na¨ıt-Abdesselam, Pin-Han Ho, Xiaodong Lin, "RADAR: a ReputAtion-based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks", WCNC 2008 proceedings, 2008

[10] Xia Wang, Johnny S. Wong, Fred Stanley and Samik Basu, "Cross-layer Based Anomaly Detection in Wireless Mesh Networks", Ninth Annual International Symposium on Applications and the Internet, 2009.

[11] Xuemei You, "Research on the Intrusion Detection System in Wireless Mesh Networks", Second International Conference on Computer Modeling and Simulation, 2010

[12] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges", computers & security 28 (2009) Elsevier, October 2008, Pp18–28

[13] Yatao Yang, Ping Zeng, Xinghua Yang, Yina Huang, "Efficient Intrusion Detection System Model in Wireless Mesh Network", Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.

[14] Chen M., Kuo S., Li P., andZhu M., "Intrusion Detection in Wireless Mesh Network". CRC Press, 2007.

[15] H. Yang, et al., "Security in mobile ad hoc networks: challenges and solutions", IEEE Wireless Communications, vol. 11, Feb. 2004.