International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 1– No.3, February 2012 – www.ijais.org

Survey of Intrusion Detection and Prevention System in MANETs based on Data Gathering Techniques

Monika Darji
LJ Institute of Computer Application
Ahmedabad, Gujarat
India

Bhushan Trivedi
GLS Institute of Computer Technology,
Ahmedabad, Gujarat
India

ABSTRACT
Intrusion Detection and Prevention System is a must for mobile ad networks as the security mechanisms like encryption, authentication and firewall systems are not able to completely secure the nodes and their communication.

In this paper, we aim to study the various intrusion detection and prevention systems that were proposed for Mobile Adhoc Networks (MANETs) and compare the recent techniques Intrusion Detection based on their architecture and data gathering techniques.

General Terms
Intrusion Detection and Prevention techniques, clustering, MANET, Reputation, Leader election.

Keywords
Intrusion Detection and Prevention System, MANET, Data gathering techniques.

1. INTRODUCTION
MANETs being an emerging technological field is an active area of research and has found usage in a variety of scenarios like emergency operations, disaster relief, military service and task forces. Providing security to the nodes and their data communication in such scenarios is critical.

Mobile Ad hoc NETwork (MANET) [1] is a set of mobile devices like laptops, PDAs, smart phones which communicate with each other over wireless links without a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network using single hop or multi hop communication.

The characteristics of MANET like dynamic topology, lack of fixed infrastructure, vulnerability of nodes and communication channel, lack of traffic concentration points, limited power, computational capacity, memory, and bandwidth make the task of achieving a secure and reliable communication more difficult. Attacks like sleep deprivation, jamming transmission channel with garbage packets, Black hole, Grey hole, Wormhole and DoS. The selfish nodes may not participate in routing and forwarding packets leading to loss of packets.

Hence there is an indispensable requirement for second line of defense which is provided by Intrusion Detection and Prevention System.

This paper is a survey of different Intrusion Detection System proposed for MANETS based on their architecture and data gathering techniques..

2. INTRUSION DETECTION AND PREVENTION
Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices[14]. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

IDPS are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies.

Intrusion Detection System can be classified as Network based which does packet analysis on the boundaries of a network and Host based which identifies intrusion on host machine. As the sophistication of attacks are increasing many folds, IDPSs uses multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection. The primary classes of detection methodologies are [15]:

Signature-based (Misuse detection model): It compares known threat signatures to observed events for identifying intrusion. This is very effective at detecting known threats and exhibits low false positive rates but largely ineffective at detecting unknown threats and many variants on known threats. Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.

Anomaly-based detection: It compares definitions of what activity is considered normal against observed events to identify significant deviations (anomalous behavior). This method uses profiles that are developed by monitoring the characteristics of typical activity over a period of time. The IDPS then compares the characteristics of current activity to thresholds related to the profile. Anomaly-based detection methods can be very effective at detecting previously unknown threats but may generate many false positives as a slight deviation in user activity may cause an alarm.

Specification-based detection: It defines a set of constraints that describe the correct operation of a program or protocol. It checks the execution of the program with respect to defined constraints. This technique provides a capability of detecting previously unknown attacks with low false positive rate.

As the nature and expectations from an Intrusion Detection System in MANET it very different from other wired and wireless networks, many Intrusion Detection System architectures have been proposed to suit the characteristics of MANETS, some of which are discussed in the next section.

3. IDPS FOR MANET

Wireless mobile network configuration depends on its application. The IDS architecture for a wireless mobile network should be designed based on the network infrastructure itself which can be a flat or multi-layered where nodes may be separated into different clusters each having a cluster head to allow communication process.

At any point of time audit data available to a node for making decision on intrusive activity is only the communication happening within its radio range so Intrusion Detection System should be able to use this information and correlate it with data from other nodes.

There are many IDS architectures proposed over the years out of which some important ones are being discussed as they are the base for recent research in intrusion detection

3.1 Distributed and Cooperative Intrusion Detection System

Zhang and Lee [6] proposed a distributed and cooperative architecture for statistical anomaly detection where individual IDS agent are placed on each node which monitors system activities, user activities and communication activities within radio range; detects intrusion and initiates a response. Neighboring IDS agents cooperatively participate in global intrusion detection actions if local IDS is not able to make decision alone. Seeing the vulnerabilities in routing protocols, MAC protocols and wireless applications and services, the model uses cross-layer integration approach to achieve better results in terms of higher true positives and lower false positive rates.

As this architecture is based on statistical anomaly detection, large amount of data that needs to be passed over wireless links to update the database of anomaly rules which is a problem in low bandwidth wireless networks and if enough rules are not available, probability of false positives increase. Also for accurate anomaly detection, it needs to obtain enough audit data to establish the normal patterns of users which is difficult in MANETs. IDS agent running on every node increases resource consumption which is scarce in energy and bandwidth constrained MANETs.

3.2 CONFIDANT

Buchegger and LeBoudec [7] proposed an extension to DSR protocol called CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc Networks).It is related to Watchdog and Pathrater which monitors transmission of surrounding nodes[16]. Each node observes the behaviors of neighbor nodes within its radio range and learns from them. This system also solves the problem of Watchdog and Pathrater such that misbehavior nodes are punished by not including them in routing and not helping them on forwarding packets. Moreover, when a node encounters a misbehaving node, it will send a warning message to other nodes in the network, based on trusted relationship. It uses a Bayesian Approach to assign trust rating. To cooperatively detect misbehaving nodes, it allows nodes in the network to send alarm messages to each other, which can be misused by malicious nodes by sending false alarms which may lead to false positives.

3.3 Distributed Intrusion Detection System Using Multiple Sensors

Kachriski and Guha [8] proposed an intrusion detection system for ad hoc networks based on mobile agents, where selected nodes are facilitated with sensors to collect and merge audit data implementing a cooperative detection algorithm which reduces resource consumption. The selection of these nodes is based on their connectivity index and the outcome of a distributed voting algorithm. Two different methods of decision making for mobile agents are proposed: independent and collaborative. The use of collaborative approach is better as independent approach may lead to single point of failure. Use of mobile agents gives better flexibility as they transport their execution and state information between different sensor hosts of the network, and finally return to the originator host with the result.

3.4 Local Intrusion Detection System (LIDS)

Albers [9] has proposed a distributed and collaborative architecture of intrusion detection system by using mobile agents. On every node, local intrusion detection system (LIDS) is implemented for monitoring the local activities and for cooperating with other LIDS and exchanging security data and intrusion alerts. LIDS agents use either the anomaly or misuse detection. Once a local intrusion is detected, the LIDS initiates a response and informs other nodes in the network. Upon receiving an alert, the LIDS protects itself against intrusion by use of a suitable defense mechanism. To distribute the intrusion detection tasks, mobile agents are used and as a result, the amount of exchanged data is tremendously reduced. Each mobile agent can be assigned a specific task which is achieved in an autonomous and asynchronous fashion without any help from its LIDS.

3.5 Dynamic Hierarchical Intrusion Detection Architecture

Dynamic intrusion detection hierarchy that is potentially scalable to large networks was proposed by Sterne [10]. The nodes are organized in a hierarchy with the top level nodes as Cluster Heads.Every node in the network monitors, logs, analyze, and send alerts, and responds to the alerts send by other nodes. The cluster heads have the additional tasks of (i) data filtering and data fusion, ii) detection of intrusions and (iii) security management.

3.6 Zone-Based Intrusion Detection System (ZBIDS)

Sun [11] have presented the architecture of a zone-based intrusion detection system (ZBIDS) that uses both local and collaborative detection technique. The local detection module consists of a general intrusion detection agent model and a Markov chain-based anomaly detection algorithm. The collaborative detection module works on the ZBIDS agents and uses an aggregation algorithm on the gateway nodes in the clustered ad hoc network. The formation and maintenance of zones requires each node to know its own physical location and to map its location to a zone map, which requires prior design setup.

4. COMPARISION OF IDS FOR MANETS

For comparative study of three systems have been undertaken as they are more recent and try to cater to the problems faced by intrusion detection systems for mobile ad-hoc networks.

4.1 An Intrusion Detection Architecture for Clustered Wireless Ad Hoc network

The architecture proposed by Jaydip Sen [13] adopts a clustered semi-centralized approach in which local intrusion detection data is integrated, reduced and incrementally aggregated and send to cluster head for network wide global intrusion detection. Ad hoc network is divided into clusters which are managed by cluster head and inter-cluster communication takes place through gateway nodes by use of mobile agents. Cluster head is chosen on the basis of election algorithm invoked periodically. To ensure load balancing and fault tolerance, cluster head is chosen randomly. Every node maintains a database of known attack for signature based detection and anomaly detection, upper and lower threshold are defined. Use of mobile agents increases flexibility.

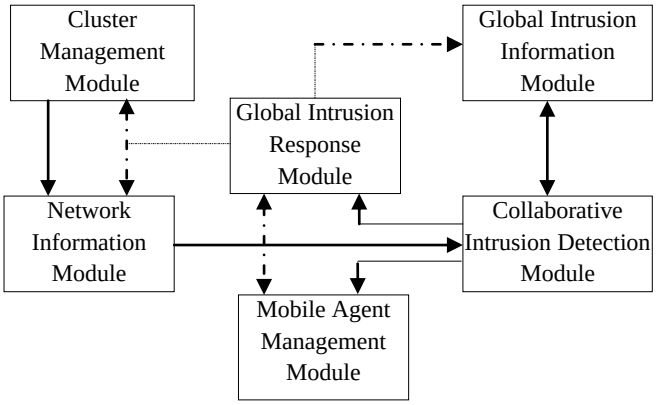

Figure 1: CHM Architecture [13]

The system consists of two major modules; cluster head module (CHM) runs only on cluster head while cluster member module (CMM) runs on all nodes.CHM architecture is shown below in figure 1, the solid arrows represent query message and dotted arrow represent response[13]

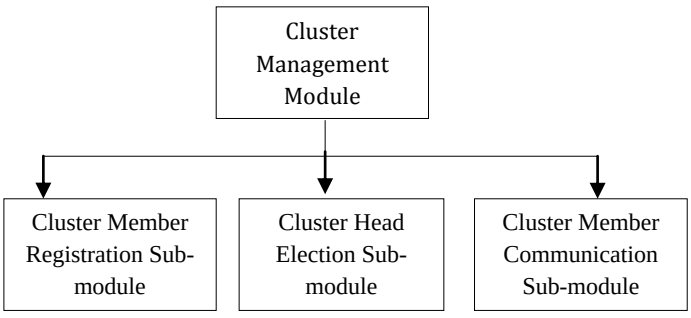

Figure 2: Cluster Management Module

Network Information Module keeps information regarding cluster head nodes of neighbor clusters. Mobile Agent Management module manages creation, dispatch and deletion of mobile agents for cooperative intrusion detection. The Global Intrusion Information Module is divided into two sub-modules as shown in figure3.

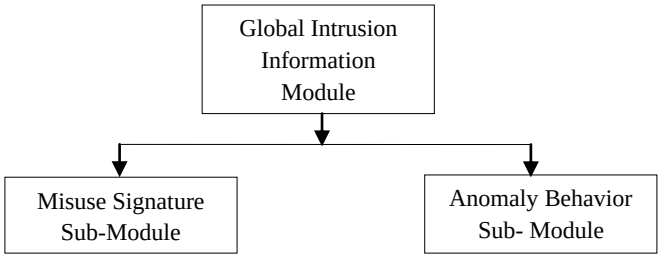

Figure 3: Global Intrusion Information Module

Collaborative Intrusion Detection Module consists of three sub-modules as shown in figure 4.

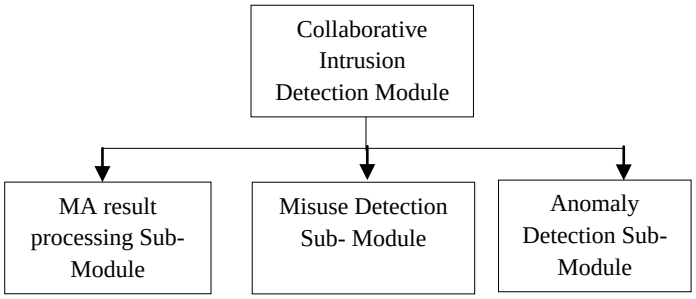

Figure 4: Collaborative Intrusion Detection Module

Global Intrusion Response Module consists of three sub-modules as shown in figure 5.

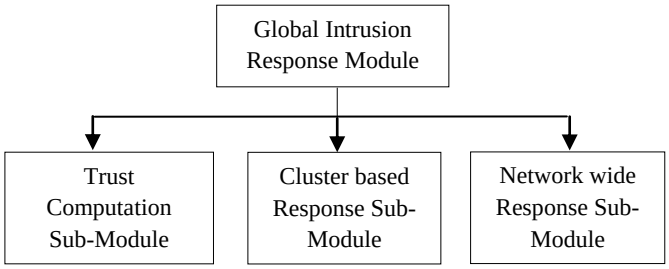

Figure 5: Global Intrusion Response Module

Cluster Member Module runs on all nodes including cluster head nodes. It maintains the data collected locally by cluster-members about intrusion detection and response. It is divided into six sub-modules as shown in figure 6.

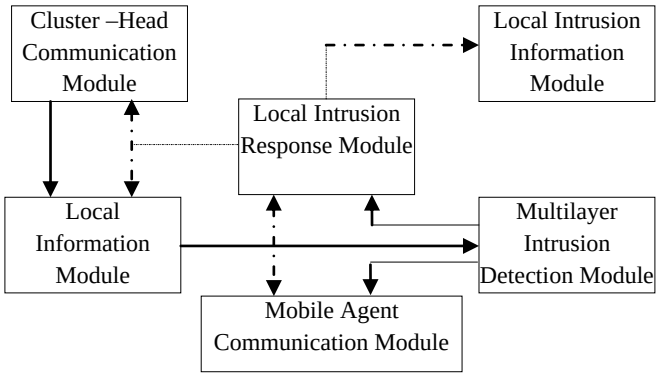

Figure 6: CMM Architecture [13]

Cluster –Head Communication Module communicates with cluster head to send information about local intrusion and request it to dispatch mobile agents for cooperative intrusion detection.

The Local Information Module invokes election algorithm and voting for dynamically electing cluster head depending on trust level and connectivity index.

The Mobile Agent Communication Module manages execution and result collection from mobile agents. The Local Intrusion Information Module maintains a database called intrusion interpreter base which includes process of learning. The Multilayer Intrusion Detection module makes intrusion detection possible at each layer. The Local Intrusion Response Module at each node compares trust value of each node in its cluster and invokes appropriate intrusion response actions like isolating the offending node from network. This IDS focuses on detecting traffic related attacks like power, storage and CPU exhaustion, network bandwidth exhaustion attacks like flooding and deprivation attacks, routing-disruption attacks such as blackhole and grayhole.

4.2 Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET

This is based on Vickrey, Clarke, and Groves (VCG) model [14] to ensure truth-telling to be the dominant strategy for any node.

Leaders are elected in a manner to ensure optimum resource utilization. To address the selfish behavior, incentives are designed in the form of reputation to encourage nodes to honestly participate in the election scheme. Two schemes are proposed Cluster Independent Leader Election (CILE) and Cluster Dependent Leader Election (CDLE). The former assumes given clusters of nodes, whereas the latter does not require any pre-clustering.

Higher effective lifetime of nodes is achieved by balancing resource consumption VCG model performs well during leader election by producing higher percentage of alive nodes
It also shows normal nodes will carry out more duty of intrusion detection and will exhaust their battery power if more shellfish nodes are present and so IDS will run on fewer nodes and may cause security breach. Reputation System Model is used to (1) Motivate nodes to behave normally and (2) punish the misbehaving nodes. Figure below shows the reputation model with following components.

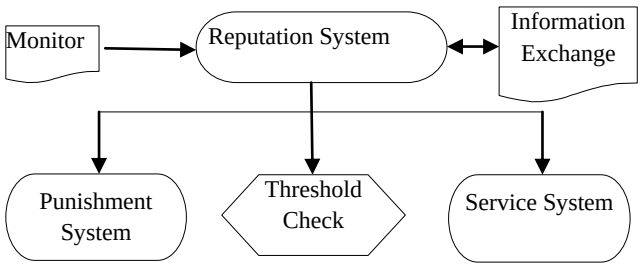

Figure 7: Reputation system model [14]

Monitor: Used to monitor the behavior of elected leader. The randomly selected set of nodes called checkers mirror a small portion of the computation done by the leader so the checkers can tell whether the leader is actually carrying out its duty.

Information Exchange: It includes two types of information sharing: (1) The exchange of reputation with other nodes in other clusters (2) To reduce the false positive rate, the checkers will exchange information about the behavior of the leader to make decision about the leader's behavior.

Reputation System: It is defined in the form of a table that contains the ID of other nodes and their respective reputation R. The node that has the highest reputation can be considered as the most trusted node and is given priority in the cluster's services.

Threshold Check: It has two main purposes: (1) To verify whether nodes' reputation is greater than a predefined threshold. If the result is true then nodes' services are offered according to nodes' reputation. (2) To verify whether a leader's behavior exceeds a predefined misbehaving threshold. According to the result, the punishment system is called.

Service System: To motivate the nodes to participate in every election round, the amount of detection service provided to each node is based on the node's reputation. Packets of highly reputed nodes should always be forwarded and packets of node with an unacceptably low reputation will have less priority.
Punishment System: To improve the performance and reduce the false-positive rate of checkers in catching and punishing a misbehaving leader, cooperative game-theoretical model is used to efficiently catch and punish misbehaving with low false positive rate.

4.3 Mobile agents-based intrusion detection system for mobile ad hoc networks

IDS proposed by Yinan Li [15] is divided into clusters by using suitable algorithm and a detection unit based on agent runs on the cluster head. Cluster head identifies intrusive activity by local data gathering and characteristics comparison and then isolates malicious nodes. If a cluster head is unable to gather sufficient evidence to declare a node malicious, it can trigger joint decision with other cluster heads to determine intrusive activity of a node by using partial voting. Partial voting instead of collective voting effectively reduces energy consumption of nodes. The IDS working is shown in figure 7.

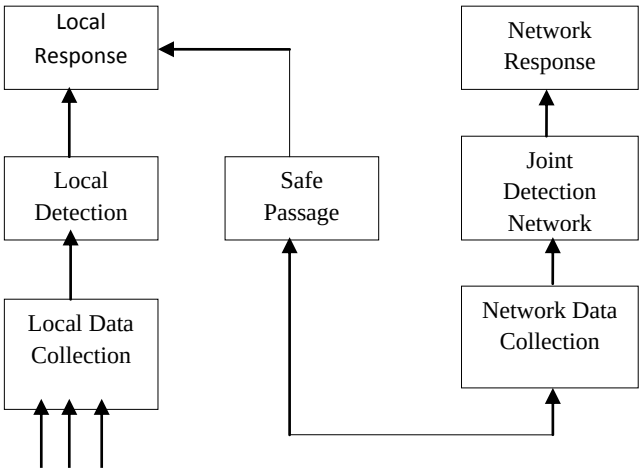

Figure 8: Intrusion Detection Process [15]

An agent is activated on cluster head node to gather data from all other nodes in the cluster to analyze the behavior of the nodes; if intrusion is detected, it will notify other nodes in the cluster by broadcasting. If agent is unable to make decision, it will select a natural number of hop as radius and send joint decision request to all cluster head nodes in range of its hop radius.

Cluster head nodes after analyzing the anomalous data, will determine whether intrusion has occurred or not. Agent will make decision based on the decision of majority of cluster head nodes inform all the nodes. If cluster head node itself is compromised, agent will notify this to all other cluster heads and exclude it from routing elect a new cluster head by clustering algorithm. The main drawbacks are Intrusion detection technique being used that there are some issues pertaining to security of mobile agents.

From the above study it is apparent that one of the major parameter for intrusion detection is the data gathering technique for analysis along with the detection style. A comparison is presented below in Table 1:

Table 1: Comparison of Intrusion Detection Systems

Ref. No.	Architecture	IDS type	Data gathering Technique	Comment
13	Clustered semi-centralized layered architecture using mobile agents	Signature and threshold based	Monitoring based and feedback among intermediate cluster head	Accuracy will be effected in case of varying noise levels, interference and varying signal propagation characteristics and may result into high false positive
14	Clustered And Cluster Independent	Signature based	Trust and reputation based	Resource utilization is optimized. Punishment and incentive system reduces false positive rate
15	Clustered using mobile agents	Signature based	Local data gathering and partial voting. Probing based using agents	Reduces energy consumption. Joint decision involving cluster heads reduces false positive rate

5. CONCLUSION AND FUTURE DIRECTION

After analyzing the architectures of IDS for MANETs we come to a conclusion that IDS architecture that involves cross layer design using autonomous mobile agent based architecture which is distributed and cooperative can efficiently detect the abnormalities and is more suitable for mobile ad hoc networks. Apart from architectural issues, data gathering techniques like monitoring based, trust or reputation based, feedback and probing based determines the false positive rates.The future scope of work also includes combining monitoring based, trust based and probing based techniques in various attack scenarios to develop intrusion detection techniques using mobile agents which will reduce the false positives and improve detection and prevention effectiveness.

6. ACKNOWLEDGEMENTS

I am indebted to my PhD guide Dr. Bhushan Trivedi for giving me an insight on intrusion detection systems.

7. REFERENCES

[1] .S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008.

[2] George Aggelou, Mobile Ad Hoc Networks, McGraw-Hill, 2004.

[3] E. Ahmed, K. Samad, W. Mahmood, "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks," AusCERT2006 R&D Stream Program, Information Technology Security Conference, May 2006.

[4] Zhou Chunyue, L.Y., (2006) "A Pattern Matching Based Network Intrusion Detection System", IEEE, 9th International Conference on Control, Automation, Robotics and Vision 2006, 5-8 Dec, ICARCV '06, Singapore.

[5] Lu Huijuan, Chen Jianguo and Wei Wei, (2008) "Two Stratum Bayesian Network Based Anomaly Detection Model for Intrusion Detection System", International Symposium on Electronic Commerce and Security, pp.482-487.

[6] Y. Zhang, W. Lee, "Intrusion Detection in wireless ad -hoc networks", Proc. of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM'2000), pp. 275-283, Aug 6-11.

[7] S. Buchegger, J.L. Boudec, "Performance analysis of the CONFIDANT protocol: cooperation of nodes- fairness in dynamic ad-hoc networks," Proc. of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), June 2002, pp. 226-236.

[8] O. Kachirski, R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks", Proc. of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE, 2002.

[9] P. Albers, O. Camp, J-M. Percher, B. Jouga, M. Ludovic, and R.Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches", Proc. of the First International Workshop on Wireless Information Systems (WIS-2002), April 2002, pp.1-12.

[10] D.Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R.Talpade,C.Ko, R. Balupari, C-Y. Tseng, T. Bowen, K. Levitt, J. Rowe, "A General Cooperative Intrusion Detection Architecture for MANETs", In Proc. of the 3rd IEEE International Workshop on Information Assurance, pp. 57-70, 2005.

[11] B. Sun, K. Wu, U.W. Pooch. "Zone-based Intrusion Detection for Mobile Ad Hoc Networks. Ad Hoc and Sensor Wireless Networks", zVol 2, No. 3, 2006.

[12] 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.

[13] Jaydip Sen, "An Intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks", Second International Conference on Computational Intelligence, Communication Systems and Networks, 2010.

[14] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on Dependable and Secure Computing, vol. 99, no. 1, 2008.

[15] Yinan Li , Zhihong Qian," Mobile agents-based intrusion detection system for mobile ad hoc networks" 2010 International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering

[16] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, pp. 255-265, Aug. 2000.