Attacker Identification in Mobile Ad hoc Networks

S. S. Manvi
Electronics and Communication Engineering Department
REVA Institute of Technology and Management
Bangalore-560064

M. S. Kakkasageri
Electronics and Communication Engineering Department
Basaveshwar Engineering College
Bagalkot-587102

ABSTRACT
A Mobile Ad-hoc network (MANET) is a multi-hop wireless network where nodes communicate with each other without any pre-deployed infrastructure. An attack is an attempt to bypass the security controls on a computer. The attack may alter, release, or deny data. Intrusion Detection System is a process of monitoring activities in a system, which can be a computer or network system. The mechanism by which this is achieved is called an intrusion detection system. Once an IDS determines that an unusual activity occurs, it then generates an alarm to alert the security administrator. This paper proposes an artificial neural network (ANN) method to find misuse detection in MANETs. Proposed method detects the attacks, corresponding to known pattern at the mobile nodes. At each mobile node whether the known attack is present or not is detected by comparing it with known patterns. These patterns are trained to ANN. Back propagation algorithm is used to train the network. To test the operative effectiveness of the proposed system, the proposed detection method is analyzed in terms of mean square error, number of iterations, computation path time taken to reach required accuracy, and change in learning rate parameter for various network scenarios.

Keywords: **Mobile ad hoc network, Intrusion detection system, Artificial neural network, Back propagation algorithm.**

1. INTRODUCTION
A mobile ad hoc network (MANET) is a dynamic self-configurable wireless network, which has no fixed infrastructure or central administration. These characteristics make MANETs suitable for mission-critical applications, such as disaster recovery, crowd control, search and rescue and automated battlefield communications [1]. Nodes can move arbitrarily, network topology can change frequently and unpredictably, and the bandwidth and battery power are limited. The security issue is becoming a major concern and bottleneck in the applications of MANETs. Therefore, selections of intrusion detection methods are especially important for MANET applications. Regardless of the application, there are certain critical features that can determine the efficiency and effectiveness of an ad-hoc network like autonomous terminal, distributed operations, multihop routing, dynamic network topology, light weight terminals, etc.
Intrusion Detection System (IDS) collects activity information and then analyzes it to determine whether there are any activities or attacks that violate the security rules. An attack is an attempt to bypass the security controls on a computer. The attack may alter, release, or deny data. The success of an attack depends on the vulnerability of the system and the effectiveness of existing countermeasures. Examples of attacks include actions such as stealing data from storage media and devices, obtaining illegitimate privileges, inserting data falsely, modifying information, analyzing network traffic, obtaining illegitimate access to systems through social engineering, or disrupting network operation using malicious software. Some of the attacks are as follows: sleep deprivation, location disclosure, and eavesdropping.
IDS can be classified based on audit data as either host-based or network-based. A network-based IDS captures and analysis packets from traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified into three categories as follows: 1) anomaly detection systems, 2) misuse detection systems 3) specification-based detection systems.
An Artificial Neural Network (ANN) is an information-processing paradigm that is inspired by the way biological nervous system, such as the brain, which processes information. The key element of this paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems.
ANN possesses knowledge, which is contained in the values of the connections weights. Modifying the knowledge stored in the network as a function of experience implies a learning rule for changing the values of the weights. Information is stored in the weight matrix of a neural network. Learning is the determination of the weights. An ANN is configured for specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems involves adjustments to the synaptic connections that exist between the neurons. ANN possesses some advantages like adaptive learning, self-organization, real time operation, and fault tolerance via redundant information coding. ANNs are also applied to solve communication network problems such as resource allocation, routing, security and network management [3].

2. RELATED WORKS
An overview of existing IDS for MANETs is conducted based on reviewing features, security issues and requirements of MANETs [2] [3]. A comparison study is conducted to compare existing intrusion detection methods based on inputs, outputs, processes, advantages and disadvantages. A Survey on Intrusion Detection in MANETs is done in [4]. There is classification of architectures for IDS that have been introduced for MANETs. Current IDSs corresponding to those architectures are also reviewed and compared. The network infrastructures that

MANETs can be configured to be either at or multi-layer, depending on the applications [5].

In the Stand-alone Intrusion Detection Systems architecture, an intrusion detection system is run on each node independently to determine intrusions. Every decision made is based only on information collected at its own node, since there is no cooperation among nodes in the network [6]. Since the nature of MANETs is distributed and requires cooperation of other nodes the intrusion detection and response system in MANETs should also be both distributed and cooperative. Every node participates in intrusion detection and response by having an IDS agent running on them [7].

Hierarchical IDS architectures extend the distributed and cooperative IDS architectures and have been proposed for multi-layered network infrastructures where the network is divided into clusters. Cluster heads of each cluster usually have more functionality than other members in the clusters, for example it is responsible locally for its node as well as globally for its cluster, e.g. monitoring network packets and initiating a global response when network intrusion is detected [8]. A concept of mobile agents has been used in several techniques for intrusion detection systems in MANETs [9]. Due to its ability to move through the large network, each mobile agent is assigned to perform only one specific task, and then one or more mobile agents are distributed into each node in the network. This allows the distribution of the intrusion detection tasks.

Intrusion detection, as a complementary mechanism to intrusion prevention, is necessary to secure MANETs [10]. The study attacks on realistic networks to see what effect they have on communications are proposed in [11]. Multi-objective Mobile Network Anomaly Intrusion builds upon that concept by framing the problem as a multi-objective problem attempting to balance efficiency and effectiveness of the detection [12].

Security issues pertaining to ad-hoc networks attempts to analyze threats faced by the ad hoc network environment and provide a classification of the various security mechanisms [13]. MANETs have unique characteristics and constraints that make traditional approaches to security inadequate are explained in [14]. An efficient mobility profile of ad hoc node for mobility-pattern-based anomaly detection in MANET, in which the mobility pattern of a specific node is characterized by a multi-leaf tree structure [15]. Second-level nodes stands for the possible starting points and leaf nodes stand for the destination node of each possible path.

A method for determining conditions under which critical nodes should be monitored is described in [16]. A novel algorithm for tracing DoS Attackers in MANETs is explained in [17]. In this algorithm, when a node forwards a packet, the node writes its zone ID into the packet with a probability. After receiving these packets, the victim can reconstruct the path between the attacker and itself. Selection in IDS over MANET is investigated in [18]. A Wireless Intrusion Detection System for Secure Clustering and Routing in Ad Hoc Networks presents an integrated secure routing system based on IDS and SUCV (Statistically Unique and Cryptographically Verifiable) identifiers [19]. This IDS solution is based on the detection of behavior anomalies on behalf of neighbor hosts, with passive reactions, aiming to create a cluster whose route paths will include only safe nodes, eventually.

Cyber security and the evolution of IDSs are discussed in [20]. Some of the challenges in designing efficient intrusion detection systems, which could provide high accuracy, low false alarm rate and reduced number of features are explained. A General Cooperative Intrusion Detection Architecture for MANETs presents a cooperative, distributed intrusion detection architecture that addresses these challenges while facilitating accurate detection of MANET-specific and conventional attacks [21]. Parallel analysis for lightweight network incident detection using nonlinear adaptive systems, AID (anomaly intrusion detection) and MID (misuse intrusion detection) systems run in parallel is explained in [22].

We observed from the literature that most of the earlier works are not focusing on misuse detection using ANN. Hence we propose an artificial neural network method to find Misuse detection in mobile ad-hoc network

Remainder of the paper is structured as follows. Section 3 describes the proposed work. Section 4 presents simulation and simulation results. Finally, conclusions are given in section 5.

3. Proposed Work

This section explains the proposed ANN based misused detection in MANETs. Detect the attacks corresponding to the known patterns at the nodes. Train the known patterns to the ANN. Back propagation algorithm is used to train the patterns to the ANN. The Back propagation algorithm used consists of one hidden layer. The numbers of nodes are the input layer neurons. The output layer neurons are same as input neurons. Number of nodes in each hidden layer should be greater than input neurons and less than twice of input neurons. This approach depends on the problem complexity.

3.1 Network environment

We consider a MANET comprising of several nodes that are randomly distributed across a given geographical area as given in figure 1. Each node has a unique identifier and two nodes are neighbors and have a link between them if they are in the transmission range of each other. Every node knows the set of neighbor nodes.

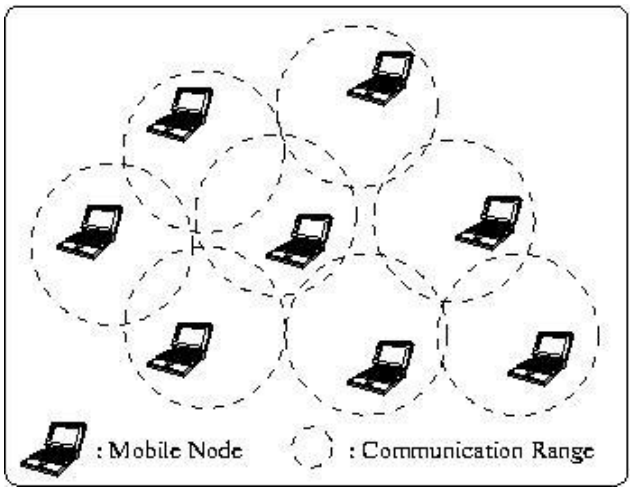

Figure 1. Network environment

3.2 ANN based learning

Figure 2 illustrates the proposed ANN based model for learning in MANETs. It comprises of learning from available known patterns. The resultant node weights are fed to ANN after detecting the attacks if any.

Input: It consists of the number of nodes in MANET and a bias (always equals to 1, so that output of the network should not go into the saturation). For some of the nodes known patterns are fixed.

Misuse detection: Compares the patterns if any with the known patterns, corresponding attack is detected. At the output resultant weights are fed to the ANN.

Training Set: The training set given to the network is nothing but the known patterns. These patterns are assigned some weights in between -1 to +1. For no pattern the weight is assigned zero.

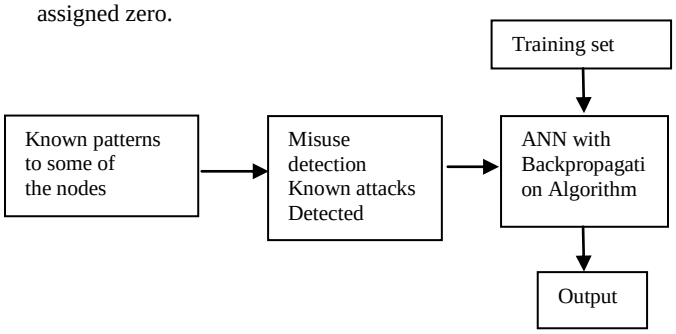

Figure 2. Proposed ANN based Model

Artificial Neural Network: ANN consists of Input layer, output layer and number of hidden layers. ANN with one hidden layer is as shown in figure 3.

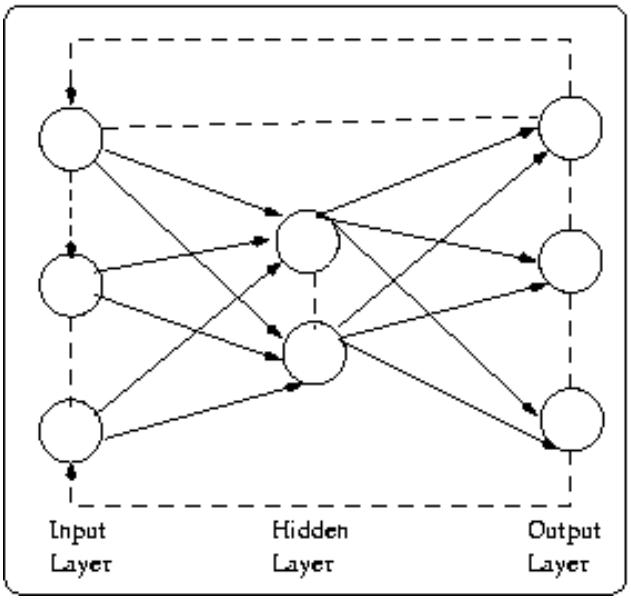

Figure 3. Neural network with one hidden layer

Input Layer: The input layer neurons consist of number of nodes in an Ad-hoc network and bias (always equals to 1, so that output of the network should not go into the saturation).
Hidden layer: The number of hidden layers may be one or greater than one and the number of nodes in each hidden layer should be greater than input neurons and less than twice of input neurons. This approach depends on the problem complexity. ANN with one hidden layer is considered in our approach.
Output layer: The output layer neuron is same as input neurons.
Output: It is the Mean squared error obtained by neural network, which are corrected by using back propagation algorithm to reach the accuracy.

4. SIMULATION

The proposed scheme has been simulated in various network scenarios using "C" programming language. A discrete event simulation is done to test operation effectiveness of the scheme. In this section we describe the simulation model and the simulation procedure. In this section, we describe the simulation model, simulation procedure and performance parameters.

4.1 Simulation model

Using random placement of the nodes within the area given by '*W X H'* square units generates MANET of 'N' nodes. The transmission range of each node is denoted as 'R' units. Each node maintains the information such its id no, location, range, neighbor nodes, intrusion detection type, pattern recognition type. Weight vector changes in back propagation are proportional to the negative gradient of the error. The magnitude change depends on the appropriate choice of learning rate, which is an independent parameter. The learning rate parameter is taken as *'η'*. In random-based mobility models, the mobile nodes move randomly and freely without restrictions. To be more specific, the destination, speed and direction are all chosen randomly and independently of other nodes. The mobility of each node is denoted *'M'* unit per second.
The number of layers in neural network is taken as *'L'*. The number of input neurons equals the number of mobile nodes which are taken as *'inodes'*. The number of output neurons equals the number of input neurons which are taken as *'knodes'*. The number of hidden layer nodes is taken as *'jnodes'*.

4.2 Simulation procedure

To illustrate some results of the simulation following parameters are considered. N=2-15, W=5-24, H=10-48, 3≤ R ≤10, 1≤ M ≤10, L=2, inodes=2-15, jnodes=3-29, knodes=2-15, η=0.1, 0.5 increases instep with Δ=0.01 & 0.05. The simulation procedure is as given below:

Begin

- Generate an ad-hoc network with given number of nodes and initialize weight between –1 to +1 to the nodes.
- Input the patterns with weight into some of nodes randomly.
- Compute the difference between weights and determine the patterns corresponding to attack.
- Find the number of nodes in input layer, hidden layer, and output layer depending on nodes given for MANET.
- Initializing random weights between layers, compute the change in weights defined by delta rule of back propagation algorithm.
- Compute the mean squared error at each iteration.
- Find number of iteration and time taken for the network until the stopping criterion is met.

End

The following performance metrics are used for evaluating the proposed scheme.

- *Mean squared error:* It is the averaged sum of error squares at each iteration.
- *Iteration:* It is one complete cycle consisting of forward pass and backward pass.
- *Path computation Time:* It is the total time taken for iterations to reach the MSE to get required accuracy, which is the percentage value of MSE.

4.3 Result analysis

We observe from the figures 4 and 5, that as the number of nodes attacked increases the iterations required to reach MSE ≤ 10%(0.1) increases for any value of η. This is because as the number of attacked nodes increase in a given area, hence the

MSE increases gradually. As the number of nodes attacked increases, number of iterations also increases.

From figures 6 and 7 it is observed that, as the number of nodes increases the computation time taken to reach MSE ≤ 10% (0.1) decreases for any value of η.

From figure 8 we observe that MSE decreases as the number of iterations increases for different values of η. It is also observed that it takes large number of iterations for η=0.1 with Δ=0.01 and less number of iterations for η=0.5 with Δ=0.05 to reach MSE ≤ 10 %(0.1).

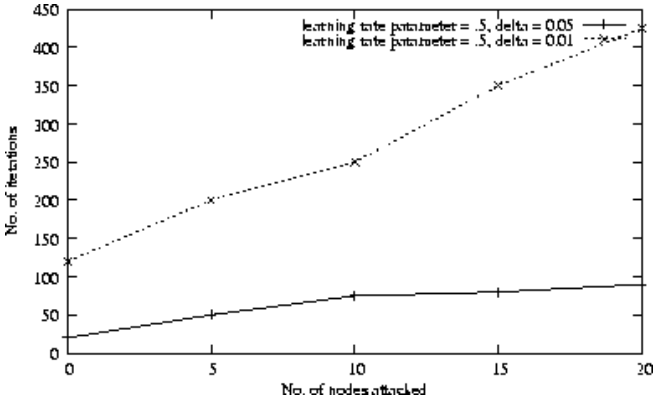

Figure 4. Number of Iterations Vs. Number of nodes attacked (for 10% accuracy)

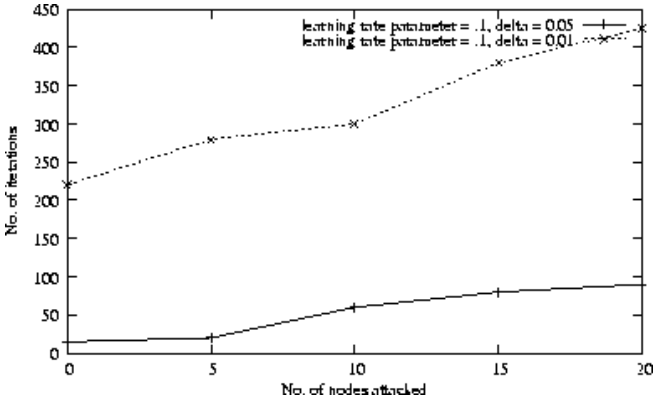

Figure 5. Number of Iterations Vs. Number of nodes attacked (for 10% accuracy)

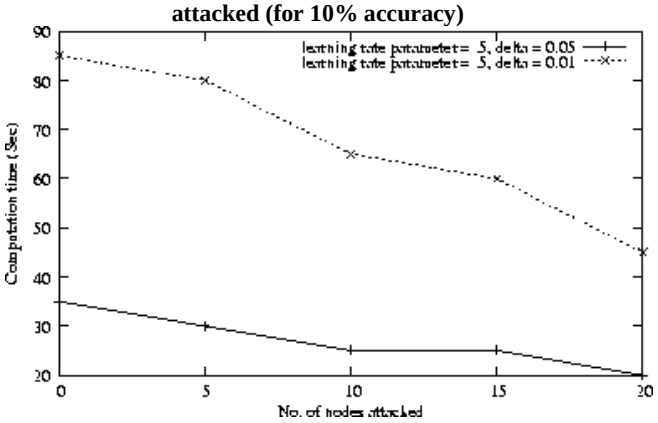

Figure 6. Computation time Vs. No. of nodes attacked (for 10% accuracy)

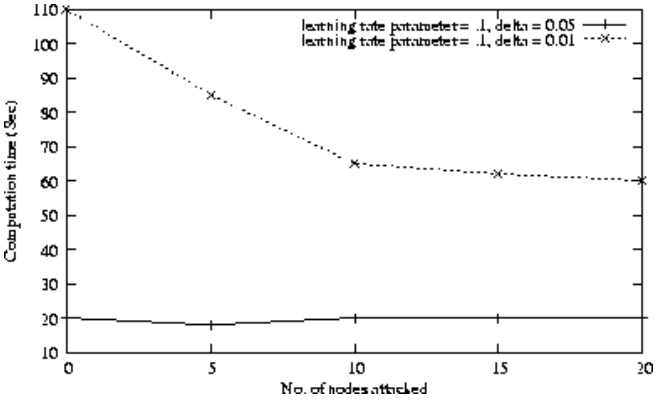

Figure 7. Computation time Vs. No. of nodes attacked (for 10% accuracy)

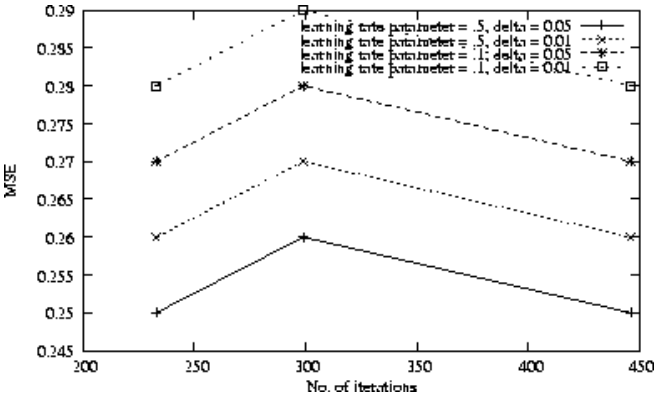

Figure 8. Mean Squared Error versus Number of iterations (for 10% accuracy)

5. CONCLUSIONS

Misuse Detection in Mobile Ad-hoc Network using Artificial Neural Network Based Approach is presented in this paper. It mainly uses back propagation algorithm to train the neural network. Training is done to the neural network by adjusting the synaptic weights. The performance of the proposed scheme is analyzed in terms of mean square error, number of iterations, time taken to reach required accuracy, and change in learning rate parameter. ANN based approach can be applied to the dynamic networks (Wherever the automatic learning capability is critically needed) like MANETs for Authentication, misbehavior, routing, etc.

Compared to traditional method of intrusion detection, neural network based learning is more complicated. As the number of nodes increases the complexity in weight adjustment increases. In future, considering more number of mobile nodes may extend the work. To reduce the complexity of the proposed system advanced algorithms like self-organizing maps can be used for detecting.

6. REFERENCES

[1] Jun-Zhao Sun, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing". www.mediateam.oulu.fi/publications/pdf/92.pdf

[2] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol.9, No. 5, 2003.

[3] Christos Stergiou and Dimitrios Siganos, "Neural Networks",http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html

[4] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol.9, No. 5, 2003.

[5] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches", Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 112, April 2002.

[6] O. Kachirski and R. Guha, \E®ective "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.

[7] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03), pp. 135-147, October 2003

[8] A.Agah, S. K. Das, K. Basu, and M. Asadi, "Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach", Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications (NCA'04), pp. 343-346, 2004.

[9] S. Zhong, L. Li, Y. G. Liu and Y. Yang, "On Designing Incentive-Compatible Routing and Forwarding Protocols in Wireless Ad-hoc Networks: An Integrated Approach Using Game Theoretical and Cryptographic Techniques", Proceedings of the 11th Annual International Conference on Mobile Computing and Networking (MobiCom'05), pp.117-131, 2005.

[10] H. Deng, W. Li, and Dharma P. Agrawal,"Routing Security in Ad Hoc Networks," IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol.40, No. 10, October 2002

[11] C.-Y. T. et al., "A specification-based intrusion detection system for AODV," in Proc. Of ACM Workshop on Security of ad hoc and sensor networks, 2003.

[12] Sarafijanovic, S. and Boudec, J., "An Artificial Immune System Approach with Secondary Response for Misbehavior Detection in Mobile Ad-Hoc Networks". TechReport IC/2003/65, EPFL-DI-ICA, Lausanne, Switzerland, November 2003

[13] Panagiotis Papadimitratos and Zygmunt J. Haas "Secure Routing for Mobile Adhoc Networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

[14] J. S. Balasubramaniyan et al., "An Architecture for Intrusion Detection using Autonomous Agents," Proceedings of the Fourteenth Annual Computer Security Applications Conference, 1998.

[15] O. Kachirski and R. Guha, "Effective Intrusion Detection using Multiple Sensors in Wireless Ad hoc Networks", In Proc. 36th Annual Hawaii Int'l. Conf. on System Sciences (HICSS'03), pp.57.1, 2003.

[16] Y. Zhang and W. Lee. "Intrusion detection in wireless ad hoc networks". In Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 275–283. ACM Press, 2000.

[17] A.Helmy, "Contact-extended zone-based transactions routing for energy-constrained wireless ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 54, no. 1, pp. 307–319,2005.

[18] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions", IEEE Wireless Communications. 11 (1), pp. 38-47. 2004

[19] Yongguang Zhang, Wenke Lee and Yi-An Huang. "Intrusion Detection Techniques for Mobile Wireless Networks". Wireless Networks, Volume 9 Issue 5, September 2003.

[20] Yuehui Chen and Ajith Abraham and Ju Yang, "Feature Deduction and Intrusion Detection Using Flexible Neural Trees", Second IEEE International Symposium on Neural Networks (ISNN 2005), Lecture Notes in Computer Science Vol. 3498, J. Wang, X. Liao and Zhang Yi (Eds.) Springer Verlag, Germany, pp. 439 - 446, 2005.

[21] Yi-an Huang and Wenke Lee. "A Cooperative Intrusion Detection System for Ad Hoc Networks." Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03), October 2003.

[22] David Wagner and Drew, "Intrusion detection via Statistic Analysis", IEEE Symposium on Security And Privacy, 2001