BEHAVIORAL INTRUSION DETECTION IN MOBILE AD HOC NETWORKS

S.Mamatha[1] and Dr. A. Damodaram[2]

[1]Associate professor, Dept of Computer science and Engineering,
Bhoj Reddy Engineering College for Women
msathineni@yahoo.co.in

[2]Professor, Dept of Computer Science and Engineering,
J.N.T.University, Hyderabad,
damodarama@rediffmail.com

ABSTRACT

Mobile ad hoc networks due to their ease and speed in setting up are currently used in emergency, military and other areas. Due to their frequent use in applications where the integrity of data and communication is necessary it is very important to provide security for the MANETS. The wireless ad hoc networks have different characteristics when compared to wired networks, so the intrusion detection techniques employed for wired networks can no longer be effective for an ad hoc network when applied directly. Hence the existing Intrusion detection system have to be modified to work effectively in the new network environment .In this paper we give an introduction to MANETS and different intrusion detection techniques. We then propose IDS that uses a quantitative method of anomaly definition based on transmission characteristics and transmission behavior of the nodes

KEYWORDS

Mobile Ad hoc networks, Intrusion Detection, security, anomaly definition.

1. INTRODUCTION

A mobile ad hoc network is a temporary infrastructure less wireless network in which the nodes move arbitrarily. In a MANET mobile nodes which are in the radio range of each other can directly communicate using wireless links whereas those nodes that are far away depend on other nodes to pass on messages. These Ad hoc networks can be individual separate network or a secondary network which may be connected to a wired local area network or even to an internet. In spite of its ease in being able to deploy the wireless ad hoc networks, they have intrinsic vulnerabilities that make them prone to malicious attacks. One of the major issues related to ad hoc networks is providing secure communication among mobile nodes.

The environment of the mobile ad hoc network generates a set of challenges in their security design. These include highly dynamic topology, open decentralized peer-to-peer architecture, a shared wireless medium. Because of the dynamic topology the attackers can easily reach the network and exploit or possibly disable the mobile ad hoc network. Attacks on MANETS can be in the form of an active attack or passive attack targeted at various layers of the OSI model [1]. They can be classified under the various OSI layers as shown in the table.

Table1 : Security issues in MANETS

Layer	Security Issues
Application layer	Detecting and preventing viruses, malicious codes, worms and application abuses
Transport layer	Confidentiality and authentication of end-to-end communication through data encryption.
Network layer	Protection of the forwarding protocols and providing security to ad hoc routing..
Link layer	Protection of the wireless MAC protocol and provision of link-layer support.
Physical layer	Preventing signal jamming denial-of-service attacks

Similar to the wired networks, the first level of defense to overcome the various attacks in MANETS that are listed in the table can be provided through cryptography and authentication [2][3].and many solutions for the security issues at different layers have been proposed in [4],[5],[6] However, the implementation of these mechanisms is not always possible due to the limitation that some nodes may be present some may move out. Though intrusion prevention measures are inserted into the network, there are still some weak links that can be broken. So it is essential to employ another level of defense through the application of intrusion identification and response system. These systems alert the network about the possibility of an intrusion and then take direct preventive measures to protect the network. The studies made on the security of MANETS show that despite the security at various layers, intrusion detection is still needed[7],[8],[9].So the main challenge is to build an intrusion detection and response system while maintaining the preferred network performance.

2. INTRUSION DETECTION

Intrusion detection can be described as a technique to recognize “any set of actions which attempt to compromise the confidentiality, integrity or availability of a resource”. The techniques used to detect intrusion into a network are by observation of actions, security tags or audit data. In the context of mobile ad hoc network we need to identify any malicious nodes either from outside or from the node inside the network which have turned bad. Malicious nodes can easily interrupt or partition the network using various types of attacks.

Intrusion detection in wireless ad hoc networks is very important as the intrusion preventive measures like encryption and authentication can reduce intrusions but not eliminate them. These measures cannot defend against compromised nodes and the fact that such nodes already carry private keys makes the network more vulnerable. The dynamic nature of the ad hoc network assumes that trust between nodes in the network is almost absent.

There are basically two modules employed in current Intrusion detection system: anomaly detection and misuse detection.

2.1 Anomaly detection

In these systems, a baseline profile of normal system activity is created. Any activity of the system that deviates from the baseline is treated as a possible intrusion. Any standard anomaly detection system takes in audit data for analysis, the audit data is changed based on the comparison with the profile of a user. Initially the system dynamically generates the users profile and subsequently updates it based on user's usage. If any comparison between the audit data and the users profile result in a deviation crossing a threshold set, an alarm is raised declaring intrusion. Such systems are well suitable to detect anonymous or any new attacks that are not encountered earlier.

An example anomaly detection system is as shown in the figure[10].

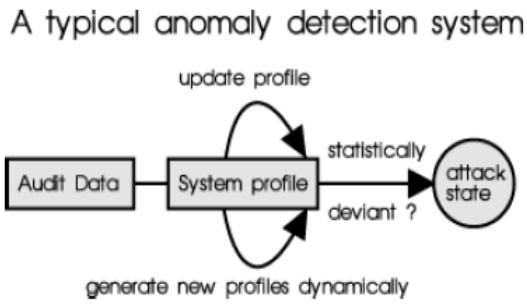

Fig 1: Example of Anomaly detection system

Problems with this approach are:

1. Abnormal activities that are not intrusive are marked as intrusive (false positives).
2. Malicious activities that behave in a normal manner are not detected (false negatives).

2.2 Misuse Detection system

In Such systems, assessment is made based on the signature of an intrusive process and the traces it leaves in the observed system. Legal behavior is defined and observed behavior compared against it to recognize intrusions. These systems try to identify any indication of intrusive activity without the knowledge of background traffic.

A misuse detection system uses audit data for analysis and compares it to large databases of attack signatures. The attack signatures are usually referred as rules with respect to timing information and are also specified as known attack patterns. On comparison between audit data and known attack patterns, if any match results an alarm of intrusion is declared.

An example misuse detection system is as shown in the figure[10].

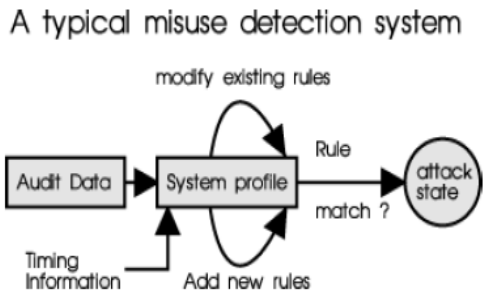

Fig 2: Example Misuse detection system

3. OBJECTIVE OF PROPOSED SYSTEM

There are different IDS which detect, report and average anomaly-data in network using clusters. They have distributed solution involving more than one level of central entity. The presence of central entities makes it a central point of failure and the cluster may become nonfunctional if an attacker targets the cluster head. So we require a non-centralized solution. There are even some of the non-centralized solutions like the one proposed by M.Alam, T.Li et al[11] which do not cater to mobile nodes or MANETS.

Our challenge is to find dynamic, distributed and quantitative intrusion detection solution for MANETS which involve mobile nodes in a non-cluster based environment. we try to show how to identify nodes displaying malicious behavior. How to identify a compromised node that has started as legal node but has been compromised after some time. How the proposed IDS is distributive, scalable and configurable.

4. PROPOSED TECHNIQUE

The first step in attaining secure ad hoc network consists of identification of nodes in the network that displays unexpected behavior. Identifying the malicious nodes consists of two steps:

1. Recognition of nodes classified as malicious.
2. Determine whether the classification is correct.

4.1 Recognition

Nodes that have deviation from normal behavior in data exchange patterns are defined as malicious nodes. From the method proposed by Alam et. al.,[11] we try to make each node calculate and maintain DTQ(Data Transmission Quality) for each of its neighbors. Where DTQ is calculated as

$$DTQ = K \times \frac{D \times STB()}{E \times P()}$$

STB ()- The stability of model behavior,
P () – probability of successful transmissions,
E- total energy spent to transmit data burst,
D- total packets transmitted successfully,

K- a constant

$$\frac{\sum_{j=0}^{\frac{N}{M}} \frac{d_j}{u_j}}{\left(\frac{N}{\sum_{i=0}(\frac{d_i}{u_i})}\right)^{\alpha}}$$

The stability factor, STB () is defined as:

Where d_i represents the successfully transmitted bytes and u_i represent those bytes that are attempted to be transmitted while sending the past ith data messages. α is a constant greater than 1. When DTQ value falls below a threshold the neighbor is signaled as a malicious node.
The process of identifying malicious node is shown in the flowchart below.

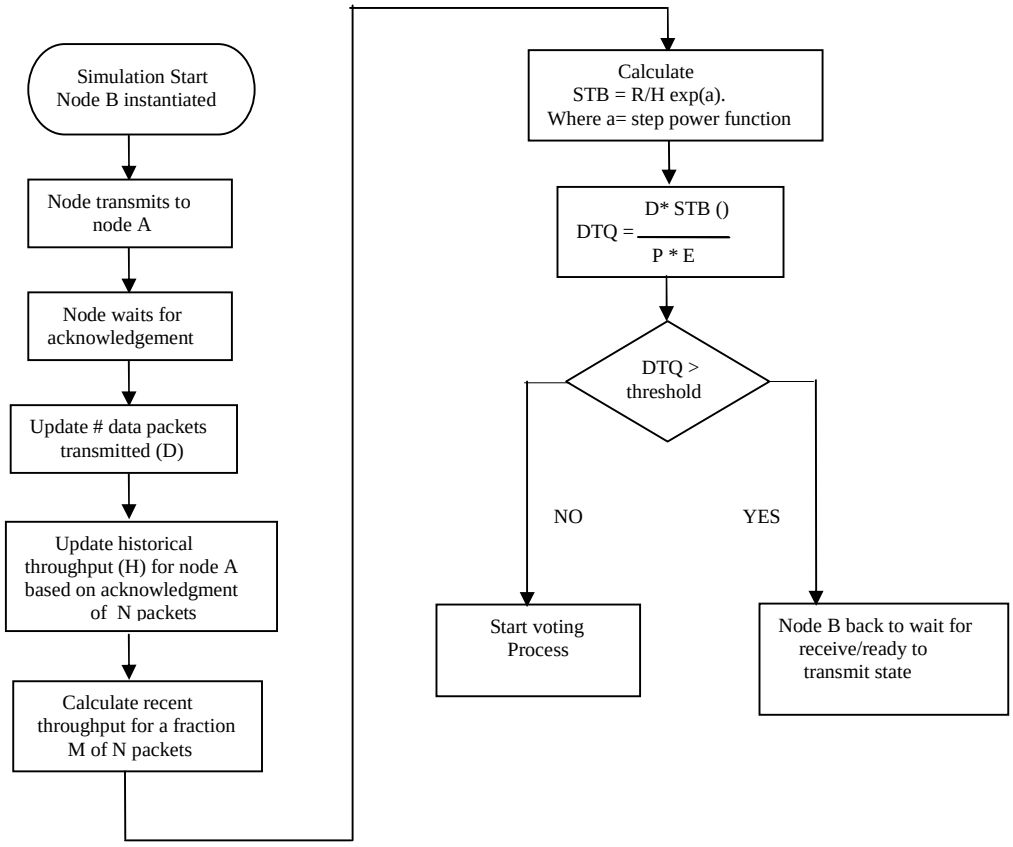

Fig 3 : Identification of malicious nodes

4.2 Confirmation

The next step in the identification of malicious nodes is to confirm whether a reading made by one node is correct or not. It is determined based on the approach where each node in the network is sent a request to admit/deny the decision. Nodes in the network on receiving the request can vote for or veto by referring to its own DTQ readings for node in the question. If more votes have been received approving a malicious behavior, the node is added to black-list which make all nodes to refrain from further communication with this node.

The voting process for an example where node A has detected that node B's DTQ has fallen below the threshold is as shown in the flowchart

After the voting process the node may be blacklisted or exonerate. Once anode is blacklisted a message with this information is sent immediately to all the nodes in the network. As soon as the node is blacklisted, no further communication with such nodes is entertained. If the node is found clear all nodes treat it as usual.

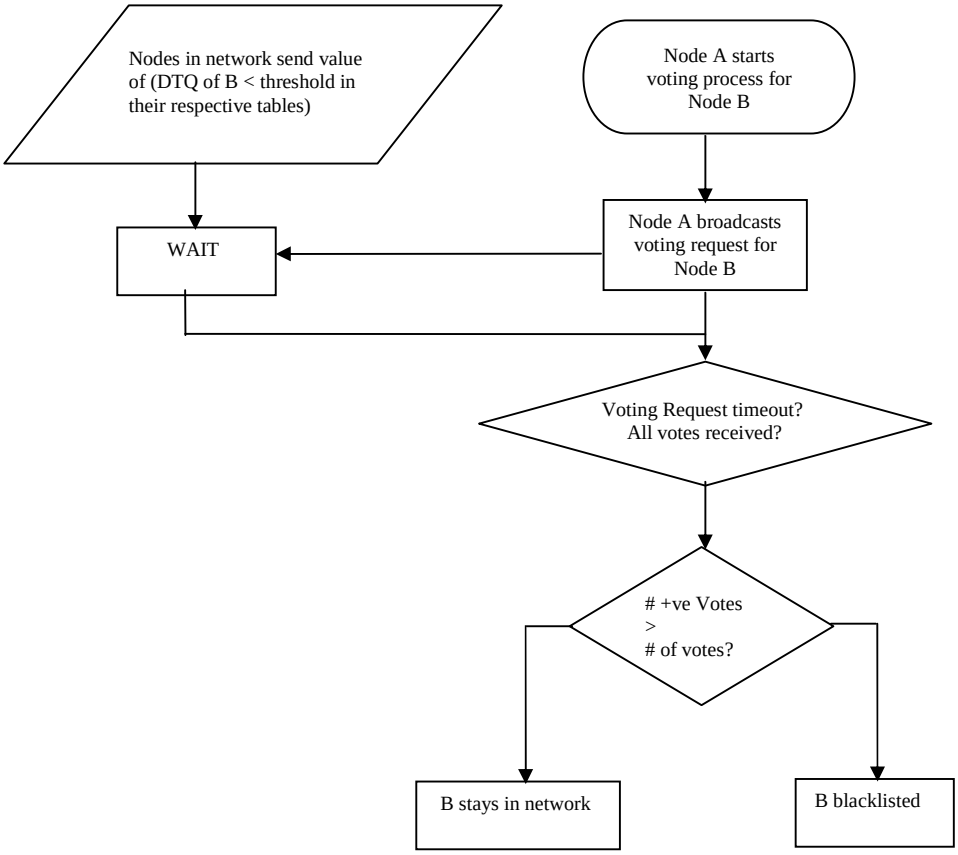

Fig 4: Voting Process

5. SIMULATIONS

We have used NS2 Simulator to show the simulation of AODV protocol to detect malicious nodes for varying speeds and accelerations.

The settings used for varying mobility features are

Number of nodes = 10
Simulation run time = 400 seconds
Mobility update Interval =1 second
Malicious node count = 4
Malicious node Id = nodes 4,7,8,9
Acknowledgement timeout = 30 s
Initial speed = 5 m/s

Varying Speed

The graph is used to display the count of nodes which are identified by a function of time. All malicious nodes are successfully detected. There is a possibility of false positives as noticed. The identified false positives are explicated by exploring the sent/received/acknowledged message counts of various nodes obtained from the output files. The false positives can occur due to various reasons like node not receiving messages for an unlimited period from a particular node, vote-replies lost and so on.

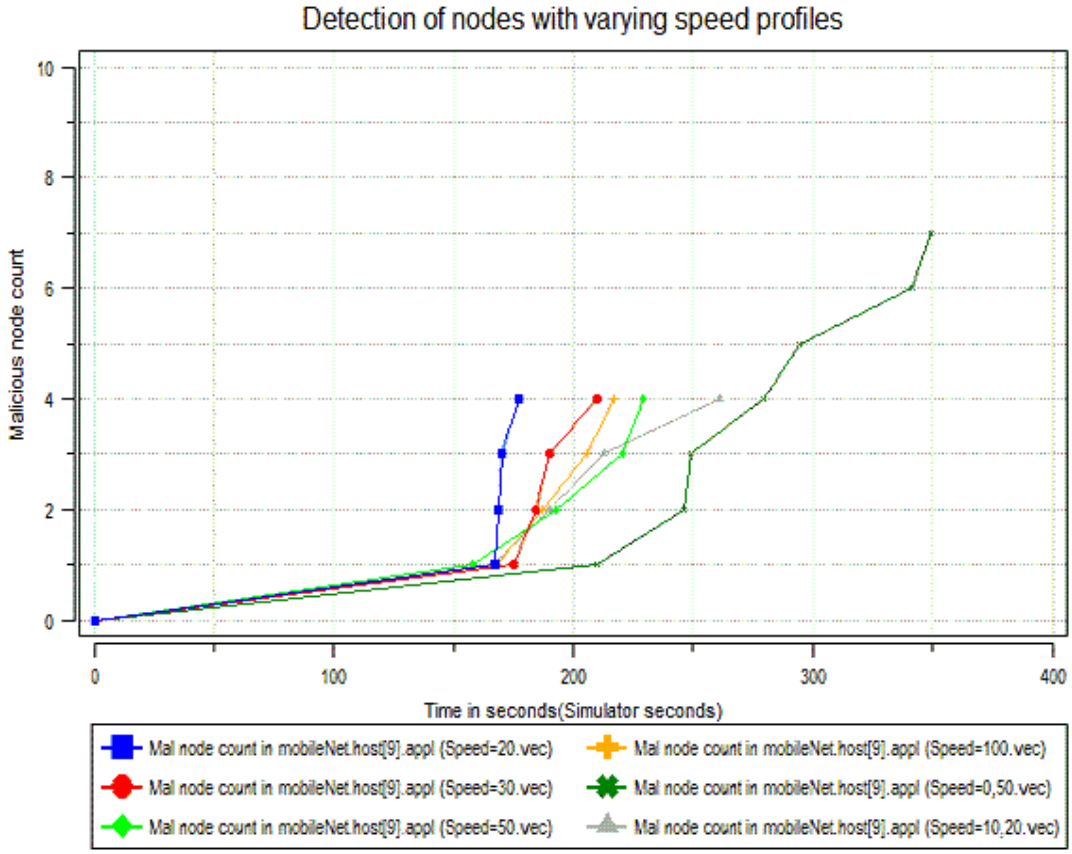

Fig 5 : Intrusion Detection with varying speeds

Varying Acceleration

Acceleration always enhances the pace at which nodes travel. The change in the acceleration is applied once every mobility interval update seconds. All the malicious nodes are always detected. It is observed that as acceleration increases, the percentage of false positives increases as shown in the graph below. This is because as the acceleration increases, the velocity of the nodes increases sporadically.

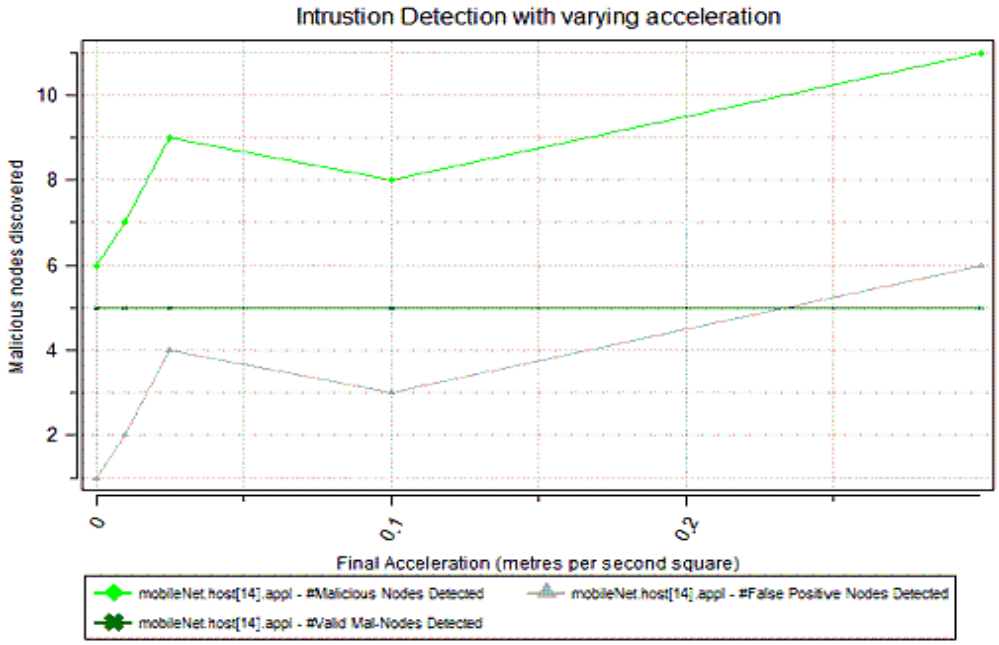

Fig 6: Node Detection with varying acceleration

Varying the number of malicious nodes

We evaluate the behavior of our IDS based on the number of malicious nodes introduced and nodes employed as a whole are changed. The tests are conducted by using a varying count of malicious nodes, carrying out 20 to 90 percent of the network. The graph starts with 20 percent performance and proceeds to90 percent performance. All malicious nodes are successfully detected. With the settings used, no false positive identifications happened, even though the simulation ran for a considerable time after the malicious nodes were identified.

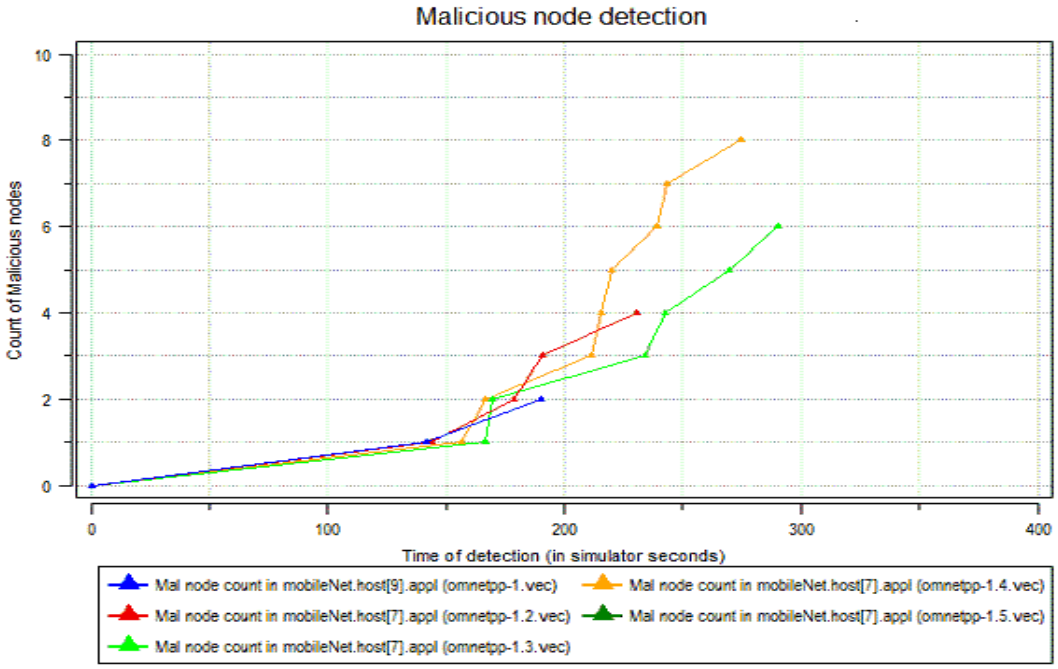

Fig 7: Node Detection with varying number of malicious nodes

6. CONCLUSION

We proposed an intrusion detection method based on behavioral attributes to identify the suspicious or compromised nodes in a MANET with mobile nodes. Here the abnormality of normal behavior is defined quantitatively by observing data exchange activity. We tried to identify the malicious nodes and also confirm whether the reading made by a node is correct or not. A MANET where there are mobile nodes, the forwarding of data to the correct recipient can be done only through a routing protocol. We have used AODV, an Adhoc On-demand Distance Vector reactive routing protocol, to achieve our function. Our proposed system is scalable because it can be enhanced to test with different mobility models and also test the IDS with different attack models.

The future work is to measure all the data with various simulation runs to detect malicious nodes in different types of attacks like selective forwarding, flooding attack, worm-hole attack, sink-hole attack, black hole attack etc.

REFERENCES

[1] H yang, H.Y Luo,F ye,S.W Lu and L.zhang. Security in mobile ad hoc networks: Challenges and Solutions. IEEE Wireless Communication, pages 38-47, vol 11, Feb 2004

[2] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu lu and lixia Zhang. Self-securing ad hoc wireless Networks. IEEE symposium on computers and communications, February2002

[3] Lidong Zhou and Zygmunt J.Hasas. Securing Ad Hoc Networks. IEEE Transactions On Dependable And Secure Computing Volume: 3, Issue: 4, Pages: 386-399February 2006.

[4] Stephan Bohacek, Katia Obrazka and Jaoa P Hespanha. Saddle policies for secure routing in Communication networks. IEEE Conference on Decision and Control, December 2002.

[5] Panagiotis Papadimitratos and Zygmunt J. Haasl. Secure Routing for Mobile Ad hoc Networks.IEEE Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, January 2002.

[6] Manel Guerrero Zapata and N. Asokan . Secure Routing for Mobile Ad hoc Networks. Proceedings of the 1st ACM workshop on wireless Security, January 2002.

[7] Wensheng Zhang, R.rao, Guohong Cao and George Kesidis. Secure routing in ad hoc networks and a related intrusion detection problem. Proceedings of MILCOM'03, IEEE conference on Military Communications, pages 735-740, 2003. .

[8] Qing Zhang, Ting Yu and peng ning. A framework for identifying compromised nodes in sensor Networks.ACM Transactions on information & system security vol 11, March 2008.

[9] Carl Hartung, James Balasalle and Richard Han. Node compromise in sensor networks: The need for secure systems. University of Colorado Technical Report CU-CS-990-05 December2004.

[10] Hongmei deng, Wei Li and Dharma P.Agrawal. Routing security in wireless Ad hoc Networks. IEEE Conference on Decision and control, Dec2002.

[11] Tao li, Min Song and Mansoor Alam. Compromised sensor node detection: A quantitative approach. IEEE International Conference on Distributed Computing systems, 2008. .

.