www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 12, Dec.2013 Page No. 3422-3430

Efficient Monitoring Of Intrusion Detection In Mobile Ad Hoc Networks Using Monitoring Based Approach

N.Kumar[1] *M.Rameshkumar*[2] *R.Karthikeyan*[3]

ASST.PROFESSOR[1, 2, 3]

Department Of Computer Science and Engineering,

nkvsc.org@gmail.com[1]Maestro.ramesh@gmail.com[2],watrapkarthik@gmail.com[3]

Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai, India·

Abstract: ***A mobile ad hoc network (MANET) is a collection of wireless devices moving in seemingly random directions and communicating with one another without the aid of an established infrastructure. To extend the reachability of a node, the other nodes in the network act as routers. Several intrusion detection techniques (IDTs) proposed for mobile ad hoc networks rely on each node passively monitoring the data forwarding by its next hop. This project presents quantitative evaluations of false positives and their impact on monitoring based intrusion detection for ad hoc networks. Experimental results show that, even for a simple three-node configuration, an actual ad hoc network suffers from high false positives; these results are validated by Markov and probabilistic models. However, this false positive problem cannot be observed by simulating the same network using popular ad hoc network simulators, such as ns-2, OPNET or Glomosim. To remedy this, a probabilistic noise generator model is implemented by using sliding window based monitoring approach. With this revised noise model, the simulated network exhibits the aggregate false positive behavior similar to that of the experimental testbed. Simulations of larger (50-node) ad hoc networks indicate that monitoring-based intrusion detection has very high false positives. These false positives can reduce the network performance or increase the overhead. In a simple monitoring-based system where no secondary and more accurate methods are used, the false positives impact the network performance in two ways: reduced throughput in normal networks without attackers and inability to mitigate the effect of attacks in networks with attackers.***

Keywords: Intrusion detection techniques, reachability of a node, mobile ad hoc networks, data forwarding, Markov and probabilistic models, false positive problem, noise generator model.

1 Introduction

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANET does not depend on pre-existing infrastructure or base stations. Network nodes in MANET are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network.

There are two types of MANET: closed and open. In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be most important in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes, and their behavior is termed selfishness or misbehavior. One of the major sources of energy consumption in mobile nodes of MANET is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

Several techniques have been proposed to detect and alleviate the effects of such selfish nodes in MANET. Two techniques were normally used, namely watchdog and pathrater, to detect and mitigate the effects of the routing misbehavior, respectively. The watchdog technique identifies the misbehaving nodes by overhearing on the wireless medium. The pathrater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. The watchdog technique is based on passive overhearing.

Unfortunately, it can only determine whether or not the next-hop node sends out the data packet. The reception status of the next-hop link's receiver is usually unknown to the observer. Ad hoc networks are ideal in situations where installing an infrastructure is not possible because the infrastructure is too expensive or too vulnerable, the network is too transient, or the infrastructure was destroyed. For example, nodes may be spread over too large an area for one base station and a second base station may be too expensive.

Ad hoc networks maximize total network throughput by using all available nodes for routing and forwarding. Therefore, more number of nodes that participate in packet routing, greater the aggregate bandwidth, shorter the possible routing paths and smaller the possibility of a network partition. However, a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious, or broken. Selfish nodes use the network but do not cooperate, saving battery life for their own communications: they do not intend to directly damage other nodes. Malicious nodes, on the other hand, aim at damaging other nodes by causing network outage by partitioning while saving battery life is not a priority.

1.1 Intrusion Detection Techniques

An intrusion is defined as a set of actions that compromises confidentiality, availability, and integrity of a system. Intrusion detection is a security technology that attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. The system can be a host computer, network equipment, a firewall, a router, a corporate network, or any information system being monitored by intrusion detection system.

An Intrusion Detection System dynamically monitors a system and users' actions in the system to detect intrusions. Because an information system can suffer from various kinds of security vulnerabilities, it is both technically difficult and economically costly to build and maintain a system that is not susceptible to attacks. An Intrusion Detection System, by analyzing the system and users' operations, in search of undesirable and suspicious activities, may effectively monitor and protect against threats. Generally, there are two types of intrusion detection: misuse-based detection and anomaly based detection.

A misuse-based detection technique encodes known attack signatures and system vulnerabilities and stores them in a database. If deployed IDS find a match between current activities and signatures, an alarm is generated. Misuse detection techniques are not effective to detect novel attacks because of the lack of corresponding signatures. An anomaly-based detection technique creates normal profiles of system states or user behaviors and compares them with current activities. If a significant deviation is observed, the IDS raise an alarm. Anomaly detection can detect unknown attacks. However, normal profiles are usually very difficult to build. For example, in a MANET, mobility-induced dynamics make it challenging to distinguish between normalcy and anomaly. It is, therefore, more challenging to distinguish between false alarms and real intrusions. The capability to establish normal profiles is crucial in designing an efficient, anomaly based IDS.

As a promising alternative, specification based detection techniques combine the advantages of misuse detection and anomaly detection by using manually developed specifications to characterize legitimate system behaviors. Specification-based detection approaches are similar to anomaly detection techniques in that both of them detect attacks as deviations from a normal profile. However, specification based detection approaches are based on manually developed specifications, thus avoiding the high rate of false alarms. However, the downside is that the development of detailed specifications can be time-consuming.

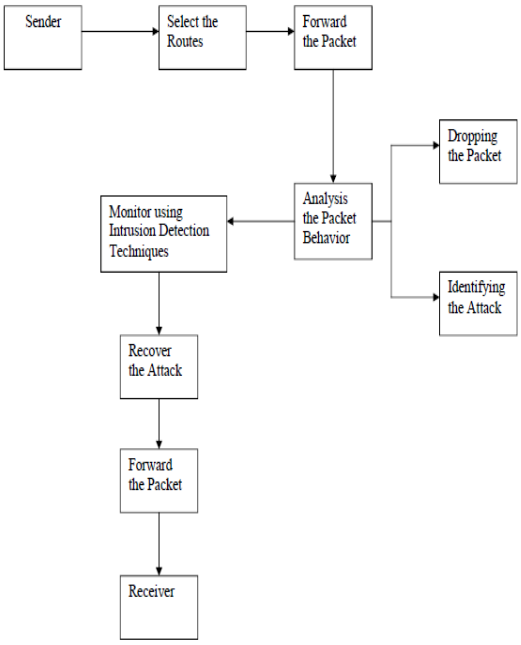
2 System Model

A mobile ad hoc network is a group of mobile nodes without requiring centralized administration or fixed network infrastructure, in which nodes can communicate with other nodes out of their direct transmission ranges through cooperatively forwarding packets for each other. HADOF is a set of mechanisms to defend against routing disruptions in mobile ad hoc networks. Based on the observed behavior and the history record of ach node, HADOF aims to detect and punish malicious nodes, and improve network performance. For each node, the first mechanism is to launch a route traffic observer to monitor the behavior of each valid route in its route cache, and to collect the packet forwarding statistics submitted by the nodes on this route. Since malicious nodes may submit false report, for each node, the next mechanism is to keep a cheating record database for the other nodes. If a node is detected as dishonest, this node will be excluded from the future routes, and its packets will may not be forwarded by other nodes as punishment. The third mechanism is to use friendship to speed up the malicious node detection. The fourth mechanism is to explore route diversity by discovering multiple routes to the destination, which can increase the chance of defeating the malicious nodes who aim to prevent good routes from being discovered.

In addition, an adaptive route rediscovery mechanism is applied to determine when new routes should be rediscovered. Both analysis and extensive simulation confirmed the effectiveness of these mechanisms, which introduce little overhead to the existing routing protocols and can handle various attacks very well. A malicious node may manipulate routing messages, (selectively) drop data packets, and frame up other good nodes, with the objective of dysfunction the network and consuming valuable resources. This existing system use “HADOF” (the acronym of Honesty, Adaptivity, Diversity, Observer, and Friendship) against routing disruptions. Since malicious nodes may submit false report, each node also keeps a cheating record database that indicates if some nodes are dishonest or have been suspected as dishonest. If a node is detected as cheating, then this node will be excluded from future routes. Furthermore, the packets originated from this cheating node will be dropped as punishment. For example, if node B is detected as cheating by node A, A will exclude B from any route originated from A in the future. However, in many situations, if malicious nodes are smart enough, it is hard to find concrete evidence to prove that they are cheating. To address this issue and speed up the malicious node detection, each node can build a list of nodes that it trusts. The next two mechanisms are to explore the route diversity and the dynamic nature of mobile ad hoc networks. Since there may exist more than one route from a source to a destination, the source can try to find multiple routes to the destination, and dynamically determine which route should be used based on the current behavior and the past history of those routes.

DSR is an on-demand source routing protocol for mobile ad hoc networks. On-demand routing means that routes are discovered at the time when a source wishes to send a packet to a destination and no existing route is known by the source. Source routing means that when sending a packet, the source lists in packet header the complete sequence of nodes through which the packet is to traverse. There are two basic operations in DSR: Route Discovery and Route Maintenance. In DSR, when a source S wishes to send packets to a destination D but does not know any routes to D, S initiates a Route Discovery by broadcasting a ROUTE REQUEST packet, specifying the destination D and a unique ID. When a node receives a ROUTE REQUEST not targeting it, it first checks whether this request has been seen before by checking the request's ID. If yes, it discards this packet, otherwise, it appends its own address to this REQUEST and rebroadcasts it. When the REQUEST arrives at D, D then sends a ROUTE REPLY packet back to S, including the list of accumulated addresses (nodes). A source may receive multiple ROUTE REPLIES from the destination, and can cache these routes in its Route Cache. Route Maintenance handles link breaks. If a node detects the next hop is broken when trying to send a packet, it sends a ROUTE ERROR packet back to the source to notifying the link break. The source then removes the route having this broken link from its Route Cache. For subsequent packets to the destination, the source will choose another route in its Route Cache, or will initiate a new Route Discovery when no such route exists.

Figure 1 Architectural Representation



2.1 Attacks and Node Behavior Assumptions

Two types of attacks have been widely used to attack the network layer in ad hoc networks: resource consumption and routing disruption. Resource consumption attacks refer to that the attackers inject extra packets into the network in attempt to consume valuable network resources. Routing disruption attacks, which are the focus of this paper, refer to that attackers attempt to cause legitimate data packets to be routed in dysfunctional ways, and consequently cause packets to be dropped or extra network resources to be consumed. Some examples of routing disruption attacks are: black hole, gray hole, wormhole, rushing attack, and frame-up.

2.2 Disadvantages

1 Nodes using watchdog have to keep receiving packets from their neighbor, the network capacity may be reduced and a lot of energy is wasted.

2 The watchdog cannot distinguish malicious behavior from misbehavior caused by

temporary network malfunction, such as collisions or network congestions.

To overcome these disadvantages a new model presents quantitative evaluations of false positives and their impact on monitoring based intrusion detection for ad hoc networks. This model quantifies false positives and analyzes their impact on the accuracy of monitoring-based intrusion detection. This use a combination of experimental, analytical, and simulation analyses for this purpose. This validate the experimental results by deriving a Markov chain to model monitoring and estimate the average time it takes for a sender to suspect its next hop. The results indicate that monitoring based intrusion detection has very high false positives, which impact its capability to mitigate the effect of attacks in networks with attackers. In monitoring-based intrusion detection, each node monitors the forwarding behavior of its neighboring nodes. In most cases, a node only monitors its next hop in a route. Two types of windows can be used to keep track of monitoring: fixed window or sliding window. One end router (denoted as node 1) sends packets to the other end router (node 3) via the intermediate router (node 2). It use static routes in node 1 and node 2 to ensure that the next hop for packets transmitting from node 1 is node 2 and the next hop for packets transmitting from node 2 is node 3. RTS/CTS handshake is used to reduce frame collisions due to the hidden terminal problem. Node 1 is set to promiscuous mode and monitors (overhears) transmissions from node 2 to node 3. In each experiment, node 1 transmits at a rate of 200 Kbps (fifty 500 byte packets /s) for up to 80 seconds. A single CBR over UDP connection is used. Node 2 transmits every packet it receives from node 1 to node 3. Every node records the ID of each packet it receives, transmits, or overhears. The packet trace from each router is sent to a desktop machine via the Ethernet connection of the routers. After the experiment, then analyzed the packet traces obtained from the three nodes. It removed the traces for the first 500 packets, which were considered to be part of the network warm-up.

With the MAC level ACK mechanism in the 802.11 protocol, node 1 can determine if a packet it transmitted is received successfully by node 2. Therefore it considered only the packets that were successfully received by node 2 in our analysis of false positives. The three-node testbed is small, nodes are stationary, and only one connection between the end nodes with static routes is used to eliminate routing overhead and contention among the test nodes. Since there is only one active connection, there is no interference noise from other node transmissions within the network. If monitoring is not effective in a three-node network, it likely to be even less effective in a larger MANET where there is interference due to transmissions by other nodes which adds to the background noise. This model describes the state of sliding-window-based monitoring using a discrete-time Markov chain. More specifically, it uses the number of not-overheard packets in the monitoring window as the state of the monitoring by node 1. The window slides to the right with each packet received by node 2. Therefore, packet receptions of node 2 are the time steps in the Markov chain. The purpose of the Markov model is to determine analytically the expected time to suspect its next hop by a monitoring node. Given that monitoring is imperfect and environmental noise could increase false positives, it is surprising that none of the published results on monitoring-based intrusion detection techniques analyzed the impact of noise. Also, to the best of our knowledge, there are no extensive evaluations of monitoring techniques using testbeds (with 10 seconds of nodes), and most large network evaluations were done using simulations. This project uses the following performance metrics to evaluate the effectiveness of monitoring:

[1] *Number of nodes suspected*: The total number of nodes suspected by one or more nodes in the network.

[2] *Total false positives*: The total number of times that normal nodes are suspected.

Intrusion Detection Techniques (IDT) can be classified as: signature-based detection, anomaly detection, and specification-based detection. Based on how the data needed for intrusion analysis are gathered, IDT for MANET can be divided into three approaches: monitoring-based, probing-based, or explicit feedback among intermediate nodes in routes. In this monitoring based approach, nodes monitor transmission activities of neighboring nodes and its next hop, it will send an alarm message back to source node. However, monitoring-based intrusion detection is not likely to be accurate for ad hoc networks due to varying noise levels, varying signal propagation characteristics in different directions, and interference due to competing transmissions within the network.

2.3Advantages

1 Misbehaving node can be easily identified.
2 Packet lost is reduced.
3 Network capacity will be increased and energy wastage is avoided.
4 Markov chain model is used to validate the time based calculation effectively.
5 Greater bandwidth and low cost.

3 Process Model

3.1 Network Model

A mobile ad hoc network is a group of mobile nodes without requiring centralized administration or fixed network infrastructure, in which nodes can communicate with other nodes out of their direct transmission ranges through cooperatively forwarding packets for each other. One underlying assumption is that they communicate through wireless connections. Since adhoc networks can be easily and inexpensively set up as needed, and mine site operations. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. Before the mobile ad hoc networks can be successfully deployed, security concerns must be addressed. Generally, this categorizes the nodes into two classes: good and malicious. A good node will try its best to forward packets for others, that is, it is fully cooperative. A malicious node may manipulate routing messages, (selectively) drop data packets, and frame up other good nodes.

3.2 Analyzing the Forwarding Behavior

Nodes send out a ROUTE REQUEST message, all nodes that receive this message forward it to their neighbors and put themselves into the source route unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. It may send that reply along the source router in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible due to asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST messages or gratuitous. After receiving one or several routes, the source picks the best (by default the shortest), stores it, and sends messages along that path.

In case of a link failure, the node that cannot forward the packet to the next node sends an error message toward the source. One end router (denoted as node 1) sends packets to the other end router (node 3) via the intermediate router (node 2). This use static route in node 1 and node 2 to ensure that the next hop for packets transmitting from node 1 is node 2 and the next hop for packets transmitting from node 2 is node 3. RTS/CTS handshake is used to reduce frame collisions due to the hidden terminal problem. Node 1 is set to promiscuous mode and monitors (overhears) transmissions from node 2 to node 3. A single CBR over UDP connection is used. Even though the overall packet delivery ratio is about 98 percent, node 1 suspects node 2 within a short period of time.

3.3 Identifying the Attacks

In MANET, routing misbehavior can severely degrade the performance at the routing layer. Specifically, nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. Network nodes collectively detect and declare the misbehavior of a suspicious node. Each node continuously monitors the behavior of its first-hop neighbors. If a suspicious event is detected, details of the event are passed to the System. Once an attacker is on certain route, it can create a black hole by dropping all the packets passing through it, or create a gray hole by selectively dropping some packets passing through it. If the protocols have the mechanism to track malicious behavior, an attacker can also frame up good nodes. The normal trace route protocol allows the sender to simply send packets with increasing Time-To-Live (TTL) values, and wait for a warning message from the router at which time the packet's TTL value expires. The misbehaving nodes, however, refuse to forward the data packets from the source. This leads to the source being confused.

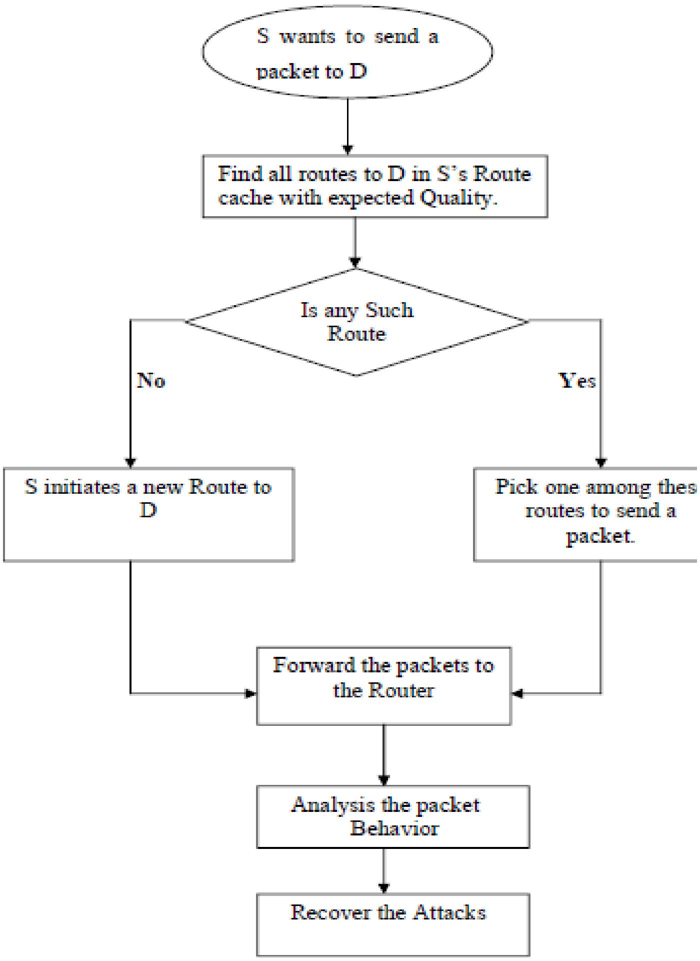
3.4 Monitoring Based Intrusion Detection Techniques

An intrusion is defined as a set of actions that compromises confidentiality, availability, and integrity of a system. Intrusion detection is a security technology that attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. In monitoring-based intrusion detection, each node monitors the forwarding behavior of its neighboring nodes. In most cases, a node only monitors its next hop in a route. Two types of windows can be used to keep track of monitoring: fixed window or sliding window. With fixed window monitoring, packets are numbered. The size of the monitoring window varies from 1 to W. Therefore, with the fixed windows approach, a malicious node can afford to drop packets at a faster rate, at times. The drawback of the sliding windows approach is that it can lead to higher false positives in noisy environments. All of the noise seen by the nodes is generated by external sources in the environment surrounding the nodes. This point out the inadequacy of the evaluations of monitoring-based detection techniques using simulators. Therefore, it is important to understand the impact of noise on monitoring techniques.

3.5 Performance Evaluation

This module evaluates the performance of the simulation. All simulations were run for 1,800 seconds with 200 seconds first used for warm-up; and the attackers, in the simulations with attacks, start dropping packets at 600 seconds. Each configuration was repeated 20 times and the results were averaged; the 95 percent-level confidence intervals are indicated for all data points. The node suspected graph clearly shows that the number of normal nodes suspected and total false positives respectively, as a function of simulation time in both high-density and low density networks with threshold T=10%. The throughput graph shows that network throughput when the 10 malicious nodes drop all received data packets starting at simulation time of 600 seconds. To further understand the throughput behavior, then looked at the total false positives and true positives for different packet drop rates graph. The number of false positives is larger than the number of true positives when drop rate is low (5 to 20 percent) and false positives are close to true positives when for 40 to 100 percent drop rates. It is difficult to differentiate malicious nodes from normal nodes, especially when the drop rate is low.

Figure 2 Data Flow Diagram


S wants to send a packet to D
Find all routes to D in S's Route cache with expected Quality.
Is any Such Route
No
Yes
S initiates a new Route to D
Pick one among thes routes to send a packet.
Forward the packets to the Router
Analysis the packet Behavior
Recover the Attacks

5 Conclusion

Several monitoring-based intrusion detection techniques proposed in literature rely on each node passively monitoring the data forwarding by its next hop to mitigate packet dropping attacks by insider nodes. Though monitoring- based intrusion detection is not likely to be accurate for ad hoc networks due to varying noise levels, varying signal propagation characteristics in different directions, and interference from competing transmissions, there are no specific studies on the impact of noise on false positives and the impact of false positives on network performance. This project presented quantitative evaluations of false positives in monitoring-based intrusion detection for ad hoc networks. This shows even for a simple three node configuration, an actual ad hoc network suffers from high false positives. It validated the experimental results using discrete-time Markov chains and probabilistic analysis. However, this problem of false positives cannot be observed by simulating the same three-node network using popular ad hoc network simulators such as ns-2 with mobility extensions, OPNET or Glomosim, because they do not simulate the noise seen in actual network environments. To remedy this, we developed a parameterized noise model based on GEV distribution function. With the noise model incorporated in the Glomosim simulator, this shows the three-node network simulation reveals the same false positive patterns that the experimental network produced and the analytical models predict. It used the simulator fortified with the GEV noise model to study the impact of monitoring-based intrusion detection on larger ad hoc networks. The results indicate two potential problems with monitoring-based IDT: 1) IDT may reduce performance of a normal network, especially when the network is not dense, and 2) IDT may not improve the network throughput since any mitigation of packet dropping by malicious nodes is offset by suboptimal paths used owing to false positives. The IDT we evaluated is a simple one and depends primarily

on monitoring. A more elaborate IDT may use additional mechanisms such as trust values of nodes and cross-checking other nodes monitoring data before actually suspecting a node. However, even in such techniques, monitoring may be used as the key step to initiate the detection process. This can increase the overhead of intrusion detection and may deter its use. In light of that the results indicate a fundamental problem with monitoring- based IDTs: the key technique used is unreliable, and any detection process based on it is likely to be error prone.

References

[1]. Sorav Bansal and Mary Baker -2003 'Observation-based Cooperation Enforcement in Ad hoc Networks'

[2]. Sonja Buchegger and Jean-Yves Le Boudec-2004 'A Robust Reputation System for Mobile Ad-hoc Networks'

[3]. Sonja Buchegger and Jean-Yves Le Boudec-2002 'Performance Analysis of the CONFIDANT Protocol (Cooperation

of Nodes: Fairness in Dynamic Ad-hoc Networks).

[4]. Imrich Chlamtac, Marco Conti and jeaJennifer J.-N. Liu-2003.‘Mobile ad hoc networking and imperatives and challenges’ Jiangyi Hu.-2005 ‘Cooperation in Mobile Ad Hoc Networks’

[5]. Zhang Yongguang, Lee Wenke. Intrusion detection techniques for mobile wireless networks. *Mobile Networks and Applications*, 2003.

[6]. Argyroudis P G, O’Mahony D. Secure routing for mobile ad hoc networks. *IEEE Communications Surveys* & *Tutorials*,2005, 7(3): 2–21.

[7]. Albers P, Camp O, Percher J M, et al. Security in Ad hoc networks: a general intrusion detection architecture enhancing trust based approaches. *Proc. of the First International Workshop on Wireless Information Systems*,2002.

[8]. Bhargava S, Agrawal D P. Security enhancements in AODV protocol for wireless ad hoc networks. *Vehicular Technology Conference*, 2001, 4: 2143–2147.

[9]. Wang Weichao, Lu Yi, Bhargava Bharat K. On vulnerability and protection of ad hoc on-demand distance vector protocol. *Proc. of 10th IEEE International Conference on Telecommunication*, 2003.

[10]. Subhadrabandhu D, Sarkar S, Anjum F. A framework for misuse detection in ad hoc networks—Part I. *IEEE Journal on Selected Areas in Communications,* 2006, 24(2): 274–289.

[11]. Tseng Chinyang, Henry Songtao, Balasubramanyam Poornima, et al. A specification-based intrusion detection model for OLSR. *RAID, LNCS* 3858, 2006: 330–350.

[12]. Alur R, Dill D L. A theory of timed automata. *Theoretical Computer Science,* 1994, 126:183–235.