Collaborative Anomaly-based Intrusion Detection in Mobile Ad Hoc Networks

By

Paryani Sunil k.

Roll No: 08MCES59

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AHMEDABAD-382481

May, 2011

Collaborative Anomaly-based Intrusion Detection in Mobile Ad Hoc Networks

Major Project

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology in Computer Science and Engineering

By

Paryani Sunil k.

Roll No: 08MCES59

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AHMEDABAD-382481

May, 2011

Declaration

This is to certify that

1. The thesis comprises my original work towards the degree of Master of Technology in Computer Science and Engineering at Nirma University and has not been submitted elsewhere for a degree.

2. Due acknowledgement has been made in the text to all other material used.

Paryani Sunil K.

Certificate

This is to certify that the Major Project entitled "Collaborative Anomaly-based Intrusion Detection in Mobile Ad Hoc Networks" submitted by Paryani Sunil k. (08MCES59), towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering of Nirma University of Science and Technology, Ahmedabad is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project part-II, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Dr.S.N.Pradhan
Professor and PG-Coordinator,
Department Computer Engineering,
Institute of Technology,
Nirma University, Ahmedabad.

Vijay Ukani
Asso. Professor and Guide,
Department Computer Engineering
Institute of Technology,
Nirma University, Ahmedabad.

Prof.D.J.Patel
Professor and Head,
Department Computer Engineering,
Institute of Technology,
Nirma University, Ahmedabad.

Dr.K.Kotecha
Director,
Institute of Technology,
Nirma University, Ahmedabad.

Abstract

An intrusion detection mechanism that uses collaborative efforts of the nodes in a neighbourhood to detect aberrant behaviour in a mobile ad hoc network. A node showing this kind of behaviour is termed as a malicious node. The technique is designed for detection of malicious nodes in a neighbourhood in which each pair of nodes are within radio range of each other. Such a neighbourhood of nodes is known as a clique. This technique uses message passing between the nodes.The procedure for monitor node election is invoked and is aimed to reduce the computation and communication costs. The monitor node, operating in dual power mode, connects the clusters which help in routing messages from a node to any other node. The monitor node initiates the detection process. The monitor node sends data packets to two other nodes, called target nodes, through the node which has to be tested for malicious behaviour. The monitor node then requests each of these two nodes to return back the data packets that have been sent to them by the node under consideration. The monitor node compares this data with the one it had sent out. Based on this, the monitor determines which of the nodes are secure and which of them are suspicious. Finally, the monitor node, with the help of secure nodes, separates malicious nodes from the suspicious nodes.

This technique is aimed to reduce the computation and communication costs to select a monitor node and reduces the message passing between the nodes to detect a malicious node from the cluster hence there very less traffic and less chances of a collision.

Acknowledgements

Before I get into the things I would like to add a few heartfelt words for the people who were part of this work in numerous ways. People who gave unending support right from the stage the project idea was conceived.

In particular, I wish to thanks and profound gratitude to **Vijay Ukani,** Asso. Professor, Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad for his faith in this project as well as valuable guidance and continual encouragement throughout part one of the Major project. I heartily thankful to him for his time to time suggestions and the clarity of the concepts of the topic that helped me a lot during this study.

Special thanks to **Dr. S.N. Pradhan,** Professor, Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad for fruitful discussions and valuable suggestions during meetings and for their encouragement.

I would like to thanks **Dr.Ketan Kotecha,** Hon'ble Director,Institute of Technology, Nirma University, Ahmedabad for providing basic infrastructure and healthy research environment.

There are times in such projects when the clock beats you time and again you run out of energy and you just want to finish it once and forever. At that time my family members has encouraged me with their warm wishes and constat support.

- Paryani Sunil K.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handhold digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society.[1]

In the ubiquitous computing environment, individual users utilize, at the same time, several electronic platforms through which they can access all the required information whenever and wherever they may be. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method: it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile AdHoc Network is one of the wireless networks that have attracted most concentrations from many researchers.

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension[2]. In the mobile ad hoc network, nodes can directly communicate with all the other

nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network.

1.1 Vulnerabilities of the Mobile Ad Hoc Networks

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. Here I discuss the various vulnerabilities that exist in the mobile ad hoc networks.

1.1.1 Lack of Secure Boundaries

The meaning of this vulnerability is self-evident: there is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network.

Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service.

1.1.2 Threats from Compromised nodes Inside the Network

There is no clear secure boundaries in the mobile ad hoc network, which may cause the occurrences of various link attacks. These link attacks place their emphasis on the links between the nodes, and try to perform some malicious behaviors to make destruction to the links. However, there are some other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This vulnerability can be viewed as the threats that come from the compromised nodes inside the network.
Since mobile nodes are autonomous units that can join or leave the network with freedom, it is hard for the nodes themselves to work out some effective policies to prevent the possible malicious behaviors from all the nodes it communicate with because of the behavioral diversity of different nodes. Furthermore, because of the mobility of the ad hoc network, a compromised node can frequently change its attack target and perform malicious behavior to different node in the network, thus it is very difficult to track the malicious behavior performed by a compromised node especially in a large scale ad hoc network. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised.

The threats from compromised nodes inside the ad hoc network should be paid more attention, and mobile nodes and infrastructure should not easily trust any node in the network even if it behaves well before because it might have been compromised.

1.1.3 Lack of Centralized Management Facility

Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems.The absence of centralized management machinery will cause vulnerability that can influence several aspects of

operations in the mobile ad hoc network.

1.1.4 Restricted Power Supply

Due to the mobility of nodes in the ad hoc network, it is common that the nodes in the ad hoc network will reply on battery as their power supply method. While nodes in the wired network do not need to consider the power supply problem because they can get electric power supply from the outlets, which generally mean that their power supply should be approximately infinite; the nodes in the mobile ad hoc network need to consider the restricted battery power, which will cause several problems.

The problem that may be caused by the restricted power supply is denial-of-service attacks. Since the adversary knows that the target node is battery-restricted, either it can continuously send additional packets to the target and ask it routing those additional packets, or it can induce the target to be trapped in some kind of time-consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests since it has run out of power.

1.1.5 Scalability

Finally, here need to address the scalability problem when the vulnerabilities in the mobile ad hoc network. Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of nodes, or even thousands of nodes.

In other words, these protocols and services need to scale up and down efficiently.[3]

1.2 Security Solutions to the Mobile Ad Hoc Networks

We have discussed several vulnerabilities that potentially make the mobile ad hoc networks insecure in the previous section. However, it is far from our ultimate goal to secure the mobile ad hoc network if we merely know the existing vulnerabilities in it. As a result, we need to find some security solutions to the mobile ad hoc network. In this section, we survey some security schemes that can be useful to protect the mobile ad hoc network from malicious behaviors.

1.2.1 Security Criteria

Before we survey the solutions that can help secure the mobile ad hoc network, we think it necessary to find out how we can judge if a mobile ad hoc network is secure or not, or in other words, what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the security state of the mobile ad hoc network. In the following, we briefly introduce the widely-used criteria to evaluate if the mobile ad hoc network is secure.

1.2.2 Availability

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service.[3]

1.2.3 Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways: A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

1.2.4 Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

1.2.5 Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

1.2.6 Nonrepudiation

Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then

use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

1.2.7 Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

1.2.8 Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

1.2.9 Security Criteria: Summary

We have discussed several main requirements that need to be achieved to ensure the security of the mobile ad hoc network. Moreover, there are some other security criteria that are more specialized and application-oriented, which include location privacy, self-stabilization and Byzantine Robustness, all of which are related to the routing protocol in the mobile ad hoc network. Having dealt with the main security criteria, we then move to the discussion on the main threats that violate the security criteria, which are generally called as attacks.

1.3 Attack Types in Mobile Ad Hoc Networks

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types:

1. External attacks:- in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

2. Internal attacks:- in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

In the two categories shown above, external attacks are similar to the normal attacks in the traditional wired networks in that the adversary is in the proximity but not a trusted node in the network, therefore, this type of attack can be prevented and detected by the security methods such as membership authentication or firewall, which are relatively conventional security solutions.
However, due to the pervasive communication nature and open network media in the mobile ad hoc network, internal attacks are far more dangerous than the internal attacks: because the compromised nodes are originally the benign users of the ad hoc network, they can easily pass the authentication and get protection from the security mechanisms. As a result, the adversaries can make use of them to gain normal access to the services that should only be available to the authorized users in the network, and they can use the legal identity provided by the compromised nodes to conceal their malicious behaviors.
Therefore, we should pay more attention to the internal attacks initiated by the malicious insiders when we consider the security issues in the mobile ad hoc networks.

1.4 Thesis Organization

The remainder of the thesis is organized as follows:

In Chapter [2] will provide you background review and related work that are important for the understanding of the Intrusion Detection System. This chapter introduces different method of Intrusion Detection System.

Then I define the problem definition for the my thesis is given in chapter[3]. The objective of this thesis is to find new simple methods for efficiently selection of the monitor node from the cluster and detection of malicious nodes in a neighbourhood in which each pair of nodes are within radio range of each other.

Chapter [4] The Proposed Algorithm, a new algorithm for performing the Intrusion Detection. The algorithm suggests a new way to reduce the computation and communication costs to select a monitor node and reduces the message passing between the nodes to detect a malicious node from the cluster hence there very less traffic and less chances of a collision. Chapter[5] provides an example of the algorithm with 5 nodes.

chapter[6] will give you brief introduction of simulators and tools available in the market.To understand better to proposed algorithm chapter[7] provides Simulation Methodologies and Performance Evaluation, describes in brief the simulation tool, NCTUns. It also describes the procedure followed, to carry out the simulation. The simulation results along with the performance analysis of the proposed algorithm are presented.

Finally in chapter[7] concluding remarks and scope for future work is presented.

Chapter 2

Literature Survey

The basic preconditions for intrusion detection are that there are intrinsic and observable characteristics of normal behavior that can be collected and analyzed and that it is possible to use those characteristics and behaviors to distinguish normal from abnormal behavior. Most traditional intrusion detection systems take either a network-based or a host-based approach to recognizing and deflecting attacks.

- Network-based IDS listen on the network, to capture and examine individual packets flowing through a network.

- Host-based systems are concerned with what is happening on each individual host.

However, due to some specific features of MANET, neither host-based nor network-based IDS is suitable for MANET. Thus, the IDS for MANET have been proposed to work in a collaborative way and as part of the existent routing protocols.The following are some of the proposed techniques for intrusion detection in MANET found in the literature.

2.1 Watchdog and Path-rater tools for detecting and mitigating routing behavior

Marti et al.[4] presented the watchdog and path-rater tools for detecting and mitigating routing behavior.

Watchdog is an intrusion detection system running on each node in the mobile ad-hoc network. It assumes that the nodes operate in the promiscuous mode, which makes them listen to the transmissions of their one-hop neighbors. Thus by listening to its neighbors, a node can detect whether packets sent to its neighbor for forwarding have been successfully forwarded by its neighbor or not. If the neighbor is found to be behaving maliciously (crosses a threshold of accepted misbehavior), it is considered malicious and its behavior is reported to the path-rater.

Examples of malicious behavior could be dropping a packet or modifying its contents before forwarding. Path-rater is also a component running on each node, which maintains behavior ratings for each node in the network.

These ratings are used as metrics while choosing a path for data transmission. Watchdog has some obvious disadvantages such as watchdog can be deceived by two neighbors colluding together and the other being the need for each node to store the transmitted packets until they are forwarded by its neighbor in the route .

Hasswa et al. [5] also discuss the weaknesses of Pathrater. The major weaknesses, related to the rating scheme include:

1. inflexible binary states
2. behavioral deceit
3. new node anonymity
4. re-entrance of previously
5. encouraging selfishness and greed

Similar to the Pathrater, Routeguard is run by each node in the network.
Each node stores a rating for all the nodes it knows. However, as an improvement to Pathrater, Routeguard assigns ratings to nodes and calculates a path metric in a refined way.
Routeguard introduces a more detail and natural classification system that rates each node in the network into one of the five classes: Fresh, Member, Unstable, Suspect, or Malicious. Each node is treated differently depending on its status and rating.

2.2 IDS Architecture for MANET

Manikopoulus and Ling [6] presented an architecture for mobile ad-hoc network security where an intrusion detection system (IDS) runs on every node.
This IDS collects local data from its host node and neighboring nodes within its communication range, processes raw data and periodically broadcasts to its neighborhood classifying normal or abnormal behavior based on processed data from its host and neighbor nodes. Architecture is given below Figure 2.1.

2.3 Proposed Intrusion Detection Scheme Principle of Misuse Detection

Intrusion detection scheme, which is based on the principle of misuse detection that can accurately match signatures of known attacks is presented in [7] by Nadkarni and Mishra. Partwardan et al.Proposed an intrusion detection scheme based on anomalous behavior of neighboring nodes [8]. Each node monitors particular traffic activity within its radio range.All locally detected intrusions are maintained in an audit log. Once local audit data is collected, it can be processed using some algorithm to detect ongoing attacks from the collected data.

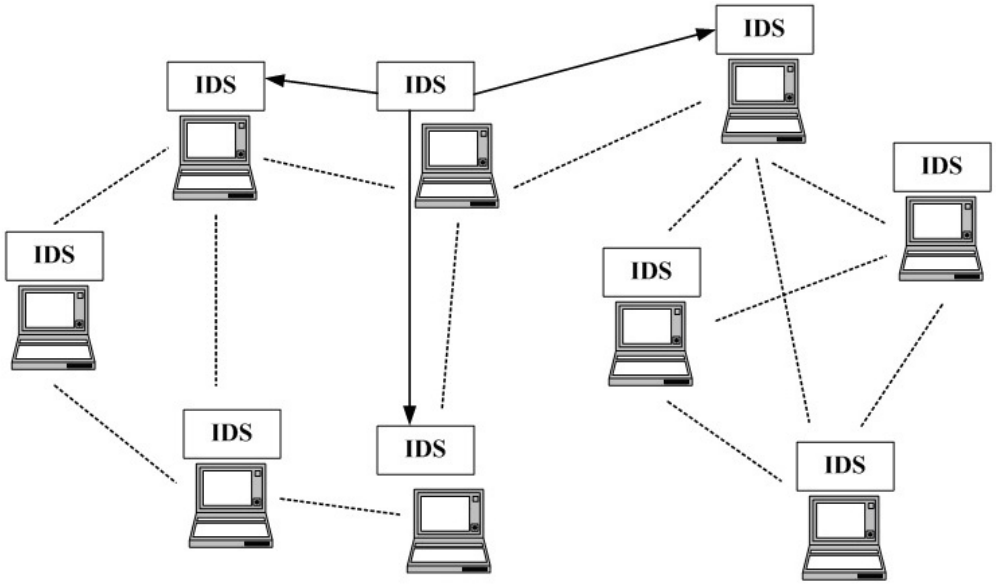

Figure 2.1: An IDS Architecture for MANET

2.4 Proposed Intrusion Detection System Based on Cooperative and Distributed Systems

Zhang and Lee [9] examined the vulnerabilities of a wireless ad-hoc network, the need for an intrusion detection to supplement a secure routing mechanism, and the reason why detection methods available for the wired environment are not applicable directly in a wireless environment. They also proposed an intrusion detection system which is both cooperative and distributed.

Zhang et al. [10] developed an architecture for intrusion detection which is distributed and cooperative. They also presented how anomaly detection could be done by using a classifier which is trained using normal data to predict what is normally the next event given the previous sequence of events. Deviation from the predicted event would mean that there is an intrusion.

Anantvalee and Wu [11]extensively surveyed on various intrusion detection techniques and also gave a comparison among these techniques.

2.5 IDS Architecture for Distributed and Cooperative Systems

Albers et al. [12] gave an IDS architecture with the use of mobile agents, which is both distributed and cooperative it is given below Figure refidssystem.
A Local Intrusion Detection System (LIDS) sits on every node, which detects intrusion locally. However, a LIDS can cooperate with other LIDS for global detection.
Kachirski and Guha [13] also used mobile agents to develop a multisensor intrusion detection system. The system consists of three main agents:

1. Monitoring agent, action agent and decision agent, each taking care of a functionality thereby distributing the workload. Monitoring agents are of two types: the network monitoring agent and the host-based monitoring agent.

2. The action agent sits on every node and takes care of initiating a response after an anomaly is detected.

3. The network is logically divided into clusters, each with a clusterhead. The network monitoring agent and the detection agent are run on the clusterhead.

The network monitoring agent captures and monitors packets passing through the network within its radio range. When the local detection cannot make a decision on its own, it reports to the decision agent, which uses the packet-monitoring results that comes from the packet-monitoring agent to decide whether it is malicious or not.

2.6 Proposed CONFIDANT Protocol for IDS

Buchegger and LeBoudec [14] proposed the CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad-hoc Networks) protocol which makes misbehavior unattractive.

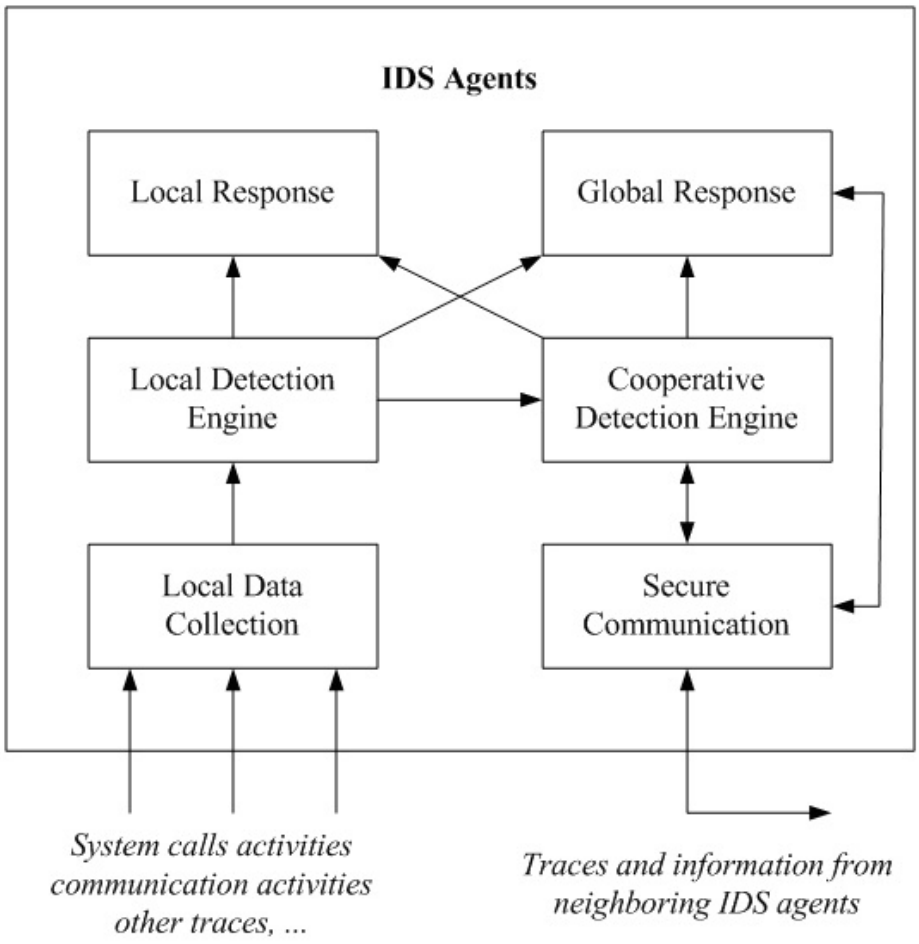

Figure 2.2: A Conceptual model for an IDS System

This protocol is similar to Watchdog and Pathrater. However, apart from monitoring malicious behavior within its radio range as in Watchdog, a node also processes information from trusted nodes to detect a misbehaving node.
When a node concludes from its observations that another node is malicious, it informs the path manager, which removes all paths containing the misbehaving node. Moreover, it also sends ALARM message about this misbehaving node to other trusted nodes.

Michiardi and Molva [15] proposed CORE, a mechanism based on reputation to detect selfish nodes and enforce cooperation among them. CORE can be said to have two components, the monitoring system and the reputation system as in CONFIDANT. For the reputation system, it maintains several tables for each node, one table for each function such as routing discovery or forwarding packets performed by the node and also a table for accumulated values for each node.
Negative rating is given to a node only from direct observation when the node does not cooperate, which eventually results in decreased reputation of the node. However, positive rating is given from both direct observation and positive reports from other nodes, which results in increased reputation. When a request comes from a node, if the overall reputation of the node is negative, it is rejected thus isolating it from the network.

Bansal and Baker [16] proposed OCEAN(Observation-based Cooperation Enforcement in Ad-hoc Networks), an extension to the DSR protocol. It also uses a monitoring system and a reputation system as in the above mechanisms. The difference of OCEAN from the other protocols that use both these systems is that it relies only on its own observations. This prevents unwanted conclusions that may result from false accusations.

2.7 Recent Scenario for IDS

N. Marchang, R. Datta [17]presented two new algorithms for intrusion detection in mobile ad-hoc networks. The algorithms use collaborative effort from a group of nodes for determining the malicious nodes by voting. Messages are passed between the nodes and depending on the messages received, these nodes determine suspected nodes (nodes that are suspected to be malicious). These suspected nodes (votes) are eventually sent to the monitor node (the initiator of the detection algorithm). At the monitor node, the suspected nodes that receive at least a minimum number of votes are finally detected as malicious nodes.

Another algorithm presented by Deepak Kumar Sharma1, Dr. S. K. Saxena, Ajay Kaushik, Vijay Tiwari[18] for intrusion detection. The algorithm uses collaborative efforts from a group of nodes for determining malicious nodes. For analyzing a particular node, the monitor node requests for the data packets from those two nodes that were to receive packets from the node under consideration. If even one of the two messages returned by the nodes matches with the actual data, the node is deemed as secure. Else, the node is marked as suspicious. The monitor node then uses the secure nodes to detect the malicious node(s) from the set of suspicious nodes. This method guarantees that no secure node is falsely accused to be malicious. Thus the algorithm detects the malicious nodes with high accuracy.

2.8 Summary

The algorithms proposed in this are based on anomaly detection as in [17,18]. This is different from misuse detection as proposed in [7,8]. However, our algorithms use collaborative efforts of nodes in the neighborhood to detect a malicious node. This makes them more tolerant to factors such as packet collision. The proposed algorithms also takes care of efficiently selection of monitor node. As in [19], to run our

algorithms, the network is divided into clusters, and the algorithms can be run in each cluster, with the clusterhead as the monitor node. Here, that uses a efficiently select monitor node to reduce the computation and communication costs and collaborative message passing mechanism to detect malicious nodes.

In this thesis we propose an intrusion detection mechanism based on cooperative, anomaly based. The intrusion detection technique reduces the message passing between the nodes to detect a malicious node from the cluster hence there less traffic and less chances of a collision and the procedure for monitor node election is invoked and is aimed to reduce the computation and communication costs.

Chapter 3

Problem Definition

3.1 Motivation

Intrusion Prevention is first line of defense against attacks in MANET. Intrusion Detection and response presents a second line of defense. New vulnerabilities will continue to invent new attack methods so new technology such as MANET, we focus on developing effective detection approaches

3.2 Scope

The monitor node, operating in dual power mode, connects the clusters which help in routing messages from a node to any other node. The monitor node initiates the detection process. The monitor node sends data packets to two other nodes, called target nodes, through the node which has to be tested for malicious behaviour. The monitor node then requests each of these two nodes to return back the data packets that have been sent to them by the node under consideration. The monitor node compares this data with the one it had sent out. Based on this, the monitor determines which of the nodes are secure and which of them are suspicious. Finally, the monitor node, with the help of secure nodes, separates malicious nodes from the suspicious nodes scope of this dissertation.

3.3 Objective

The objective of this thesis is to find new simple methods for efficiently selection of the monitor node from the cluster and detection of malicious nodes in a neighbourhood in which each pair of nodes are within radio range of each other. Such a neighbourhood of nodes is known as a clique. This technique uses message passing between the nodes.The procedure for monitor node election is invoked and is aimed to reduce the computation and communication costs.

Chapter 4

Proposed Algorithm

To present the algorithm we make the assumptions that monitor node is not malicious.

The Algorithm has following steps.

Step 1. Find the neighbors of each node N (i.e., nodes within its transmission range)

Step 2. Compute the running average of the speed for every node till current time T . This gives a measure of mobility and is denoted by M_n , as

$M_n = 1 \div T \sum_{t=1}^{T} \sqrt{(X_t - X_{t1})^2 + (Yt - Y_{t1})^2}$

where (X_t,Y_t) and (X_{t1},Y_{t1}) are the coordinates of the node n at time t and t1, respectively.

Step 3. Compute the cumulative time, P_n, during which a node v acts as a clusterhead. P_n implies how much battery power has been consumed which is assumed more for a clusterhead than an ordinary node.

Step 4. Calculate the combined weight W_n for each node n, where

$W_n = \mathrm{w1}M_n + \mathrm{w2}P_n$

where w1 and w2 are the weighing factors for the corresponding system parameters.

Step 5. Choose that node with the smallest W_n as the Monitor. All the neighbors of the chosen Monitor are no longer allowed to participate in the election procedure.

Step 6: The monitor node, M, sends a pair of messages to the remaining n-1 nodes, asking them to forward the messages to other nodes, say i and j ($i \neq j$), in the set. The nodes, that any particular node needs to forward the messages to, are decided by the monitor node. The monitor node also maintains a look-up table to make sure that there is no node in the cliques, to which not even a single packet has been forwarded.

Step 7: Each of the n-1 modes then forwards the messages to the intended nodes. For eg, the node s may be asked to forward messages Mi and Mj to nodes i and j respectively (A malicious node might not forward the message or might change the intended messages before forwarding them).

Step 8: The monitor node then analysis each of the remaining n-1 nodes, by sending a DATAREQUEST message. Like, if monitor node is to check a node s, it will ask the two nodes, say i and j, to send back the message, Mi and Mj that s had sent them.

Step 9: On receiving a DATA-REQUEST message, the 2 nodes then reply to the monitor with a DATAREPLY message. For eg, the nodes i and j will send back Mi and Mj messages back to monitor node, if node s delivered these messages to them correctly.Else, they would reply with incorrect messages, Mi' and Mj' (supposing these are the messages that node s had sent them, and thus the node s is a malicious node). Also, if either of the node i or j is a malicious one, it may send back wrong message,

or may not send any message at all.

Step 10: Upon inspecting each node, i.e. by taking back messages from all pair of target nodes, the monitor decides which nodes are malicious and which are not.

The following results show how:

1. If while inspecting node s, via target nodes I and j, at least one message from either i or j matches with the original message, then the node s is termed as a secure node.

2. If both the messages returned from the nodes do not match, then the node under consideration is termed as a suspicious node. The monitor, using the steps 6-9, runs another test of each suspected node, by using them as a router to forward messages to at least one of the secure nodes. This way, finally the malicious nodes are tracked down.

3. In step 6, the monitor node sends each node a pair of messages, to be forwarded to two other nodes. These nodes, to which the messages must be forwarded, are decided by the monitor node itself. The monitor node maintains a table so as to keep track of the nodes to which each node sends the data.

Step 11: Repeat the step 1 to 5 after t time to select new monitor node

For the clique in Figure 4.1, the table looks like shown in Table I.

For a clique of 7 nodes,having nodes A, B, C, D, E, F and G, with A being the monitor node, the look-up table will look something like given in Table II.

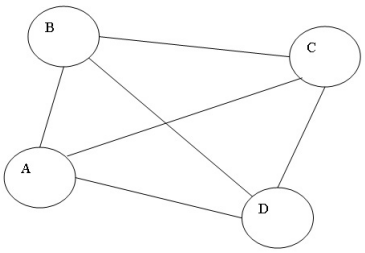

Figure 4.1: Set of node on MANET

Source	Target
B	C,D
C	B,D
D	B,C

Table I: Clique Table for 4 nodes

Source	Target	Unused Nodes
B	C,G	B,D,E,F
C	B,E	D,F
D	B,F	D
E	C,D	-----

Table II: Clique Table for 7 nodes

After the target nodes for B have been decided, the monitor checks out the unused nodes column before assigning target nodes to node C. Also, a target node cannot be the same as the source; hence when assigning targets for node D, even though we have 2 unused nodes, we can only use one of them. The other target node has to be repeated.

In step 8, after completion of step 7, the monitor node analyzes each of the n-1 nodes for malicious activity. For analysis of any node, say s, the monitor requests the two nodes, say i and j that were supposed to get packets from nodes. The participating nodes have no idea that an intrusion detection system is being run, and thus a malicious node cannot escape detection.

In step 9, each pair of nodes that were the target nodes for a particular node send back the data packets they got from that node. A faithful node will send back whatever it got, or tell monitor node whether it received any packet or not. A malicious node will falsely send out wrong information to monitor node. If a node s had sent a malicious node i message Mi, then i would sent back anything other than Mi, say Mi. The monitor node maintains a list of all the messages it had send to various nodes to be forwarded to 2 other nodes. When it receives messages back from any pair of nodes, it compares these with those in its table. A node is termed secure even if one its target node sends back the right message; i.e. the message that monitor node had send to the source node. A suspected node is the one for which monitor node did not receive any correct message. This could probably be due to the fact that the sending node was a malicious one, or both of the target nodes for a node were malicious.

In step 10, the monitor node has a list of suspected nodes, and another list of secure nodes. The monitor node now inspects each suspect node by using secure nodes as target nodes. Since secure nodes will act faithfully, hence they would send back only that information that they receive from each of the suspected nodes. Hence,

after this second run, the monitor will be able to separate secure nodes from malicious nodes.

Chapter 5

Illustrative Example

To have a better understanding of how this algorithm works, we consider a case when there are 6 nodes out of which 2 nodes are malicious, i.e., k=2 and n=6. Figure5.1 illustrates how the messages are passed between various nodes during the process. Node 0 is the monitor node and nodes 1 and 5 are malicious nodes. For the sake of simplicity, we will assume that the monitor node sends a same type of message, RIGHT, represented by solid labeled R, to all the nodes. It also directs each node to relay the message to two other nodes. For this example, we consider the TableI that is maintained by the monitor node.

The nodes 2, 3 and 4 being non-malicious nodes relay RIGHT message to their targets. To maintain readability, these messages are not shown in Figure5.1 On the

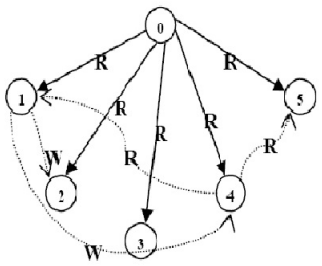

Figure 5.1: Messages passed between nodes during execution

Source node	Target nodes
1	2,4
2	1,3
3	2,5
4	1,5
5	3,4

Table I: Monitor Node Table

other hand, nodes 1 and 5 will surely send out different messages, marked WRONG (depicted by dotted lines labeled W) to their target nodes. The case with node 1 is shown in the Figure5.1 After each node has forwarded the messages sent to it, the monitor node now has to analyze each node, as in step 3. It sends a DATA-REQUEST message asking each pair of target nodes for the data they received from the source node. Like, for node 2, its target nodes 1 and 3 will relay back WRONG and RIGHT messages, respectively, back to the monitor node. This is because the node 1 is malicious and is bound to lie; whereas node 3 is non-malicious and will tell the truth. The monitor marks a node as secure even if one of its targets node data matches with what monitor had sent it. Hence, node 2 will be a secure node. Similarly, node 3 will also be secure. Now, although node 4 is not malicious, but its target nodes are 1 and 5, both being malicious. So, they might collude and send wrong data back to the monitor node. As we can see in Figure5.1 node 4 sends out RIGHT message to nodes, 1 and 5. But the monitor node will receive different messages from both these nodes. Hence, node 4 will be termed suspicious for the time being. Now, nodes 1 and 5 need to be analyzed. We have shown message transfer for node 1 in the Figure5.2 It sends out wrong messages to its target nodes 2 and 4. When these nodes reply

Source node	Target nodes
1	2,3
4	2,3
5	2,3

Table II: New monitor node table

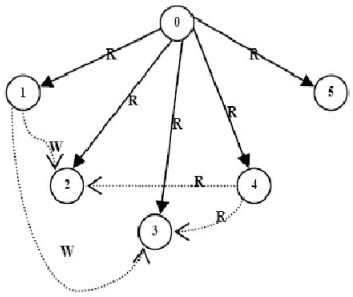

Figure 5.2: Messages passed between nodes 1,4 and 5

to monitor node, they will send the WRONG message, which they received. Hence, node 1 will also be added to the list of suspicious nodes. Similarly, node 5 will also be a suspect node. There are now three suspect nodes- 1, 4, 5 and two secure nodes- 2, 3. Now, the monitor node uses at least one of the secure nodes as target nodes to separate malicious nodes from suspected nodes. It will again maintain a table of following sorts give in Table II:

It follows the same procedure again; from steps 1 to step 4. While inspecting each of these 3 nodes, the monitor takes feedback from nodes 2 and 3. These nodes

being nonmalicious, will give back the same data back to monitor which the source nodes had send. This way, monitor will receive two RIGHT messages for node 4, thus establishing its loyalty. But for nodes 1 and 5, it will receive WRONG messages from both the target nodes. So, finally, 1 and 5 will we nailed down. This mechanism is depicted in Figure5.2

The nodes 1 and 5 are bound to send WRONG messages to other nodes, since they are malicious. But, node 4 will forward the same message as it receives from the monitor node. When the monitor node requests back messages from the target nodes of each of these 3 nodes; the nodes 2 and 3, being secure, will reply truthfully. Hence, the monitor node will receive same messages from nodes 2 and 3 as it had sent out to node 4. So, node 4 will be made secure. But for nodes 1 and 5, the monitor will still receive none of the correct messages, and hence they will be termed malicious.

Chapter 6

Simulators and Tools

6.1 Network Simulators

Network simulation is one of the most predominant evaluation methodologies in the area of computer networks. It is widely used for the development of new communication architectures and network protocols. So-called network simulators allow one to model an arbitrary computer network by specifying both the behavior of the network nodes and the communication channels. For example, in order to investigate the characteristics of a new routing protocol, it is usually implemented in a network simulator.

6.1.1 NS-2

Network Simulator 2 (NS2)[20] is a most popular discrete event simulator for the Wireless Sensor Networks. It is used it the simulation of TCP, routing and multicast protocol for wired and wireless networks. It supports 802.11 and 802.15.4 type of wireless MAC. NS2 uses two languages, C++ and OTcl. For the protocol implementation it uses C++, OTcl is used for simulation configuration. Simulation can be observed by Trace file or NAM file. NS-2 does not have good scalability for large wireless networks.

6.1.2 GloMoSim

Global Mobile Information System Simulator (GloMoSim) is a parallel discrete event based simulator for wireless networks. The simulation is performed by Parsec, a parallel programming language. By this one can simulate upto 10000 nodes. GloMoSim uses layered architecture wherein each layer uses different API these layers are integrated by different APIs and may be developed by different people.

6.1.3 OMNeT++

OMNeT++ is an extensible, modular, component based C++ simulation library and framework developed in C++. It has simple and powerful GUI library. It is useful for simulation of communication networks, queuing networks and performance evaluation. OMNeT++ is a collection of modules which are written in C++. These modules can be interfaced, nested to form a compound model. The interfacing and nesting is achieved by NED language. The outputs of the simulation are in the scalar and vector form. For the analysis of the result, we can use simulation.

6.1.4 TOSSIM

The TinyOS provides a TOSSIM as discrete event simulator/emulator. For wireless sensor networks, programs are written in nesC code. For running nesC code in TOSSIM it requires programming interface i.e. written in Python or C++. Python is a powerful debugger which allows dynamic simulation. Transforming code from one to the other is simple in C++. External programs can connect to TOSSIM by TCP socket for monitoring and actuating.

6.1.5 NCTUns

The NCTUns network simulator and emulator (NCTUns) is a high-fidelity and extensible network simulator capable of simulating various devices and protocols used in

both wired and wireless networks. Its core technology is based on the kernel-reentering simulation methodology invented by Prof. S.Y. Wang at Harvard University in 1999 when Wang was pursuing his Ph.D. degree. Due to this novel methodology, NCTUns provides many unique advantages that cannot be easily achieved by traditional network simulator such as OPNET Modeler and ns-2.

NCTUns removes many limitations and drawbacks in the Harvard network simulator. It uses a distributed architecture to support remote simulations and concurrent simulations. It uses an open-system architecture to enable protocol modules to be easily added to the simulator. In addition, it has a highly-integrated GUI environment for editing a network topology, specifying network traffic, plotting performance curves, configuring the protocol stack used inside a network node, and playing back animations of logged packet transfers.

Chapter 7

Implementation

In this chapter the performance of the algorithm proposed in chapter 4 is evaluated. Before presenting the simulation results, I explain the simulation environment and methodologies used to carry out the tests.

7.1 NCTUns6.0 Simulator

NCTUns6.0 Simulator :- The NCTUns uses a novel kernel-reentering simulation methodology As a result, it provides several unique advantages that cannot be easily achieved by traditional network simulators. NCTUns is a software tool that integrates user-level processes, operating system kernel, and the user-level simulation engine into a cooperative network simulation system. In Appendix-A outlines the procedure for installation of NCTUns6.0.

7.2 Simulation Experiments

The Proposed Algorithm was simulated using the NCTUns6.0 Simulator. Various realistic radio ranges were taken where the nodes move according to the waypoint. Mobility model with a maximum speed of 10 m/s. The routing protocol used was AODV. Message loss was considered by random selection of messages at various steps

of the algorithm except at the first step. The detection process was aborted if packet loss happened at step 1 The malicious nodes were selected n at random and were made to drop or modify all the messages that they were to forward.

In view of my algorithm, they send WRONG messages. The simulation was done for different values of n(number of nodes) and k(number of malicious node). For different percentage of collisions, twenty random runs were performed for each simulation scenario, i.e., for each value of n.

The percentage of collisions is the percentage calculated from the maximum total number of messages that will be received during the execution of the algorithm. It may be noted that if no collision occurs the maximum total number of messages are passed and received successfully. However, when collisions are assumed, some messages may never reach a recipient due to collision.

No	Parameter	value
1	Number of Nodes	5, 20
2	Node movement Space	200 m x 200m
3	Frequency(Mhz)	2400
4	Transmission power(dbm)	6
5	Operation Mode	Ad Hoc Mode
6	Node Mobility	Random Way Point
7	Routing Protocol	AODV
8	Node Speed	10m/s Maximum

Table I: Simulation Parameters

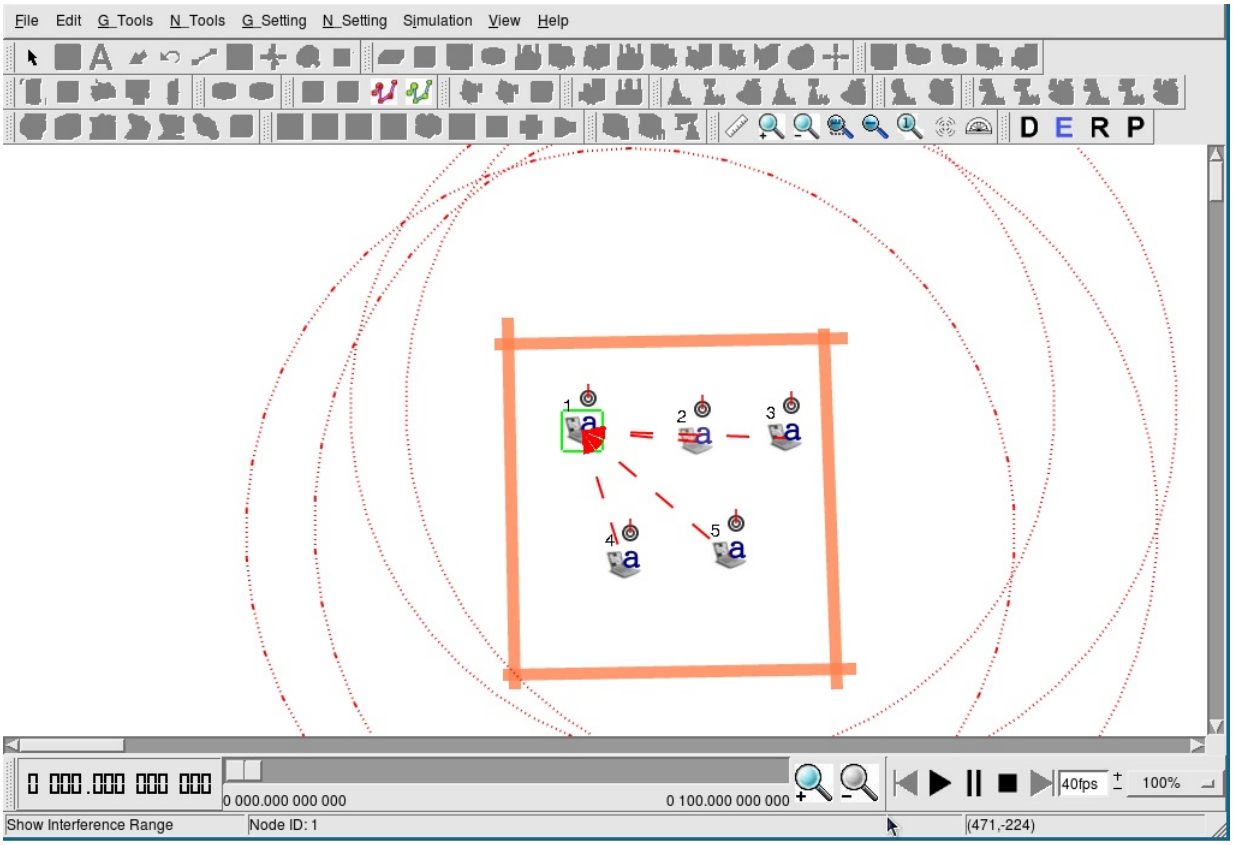

Figure 7.1: Five mobile nodes within radio range of each other

In this Figure7.1 it shows five mobile nodes are within radio range of each other

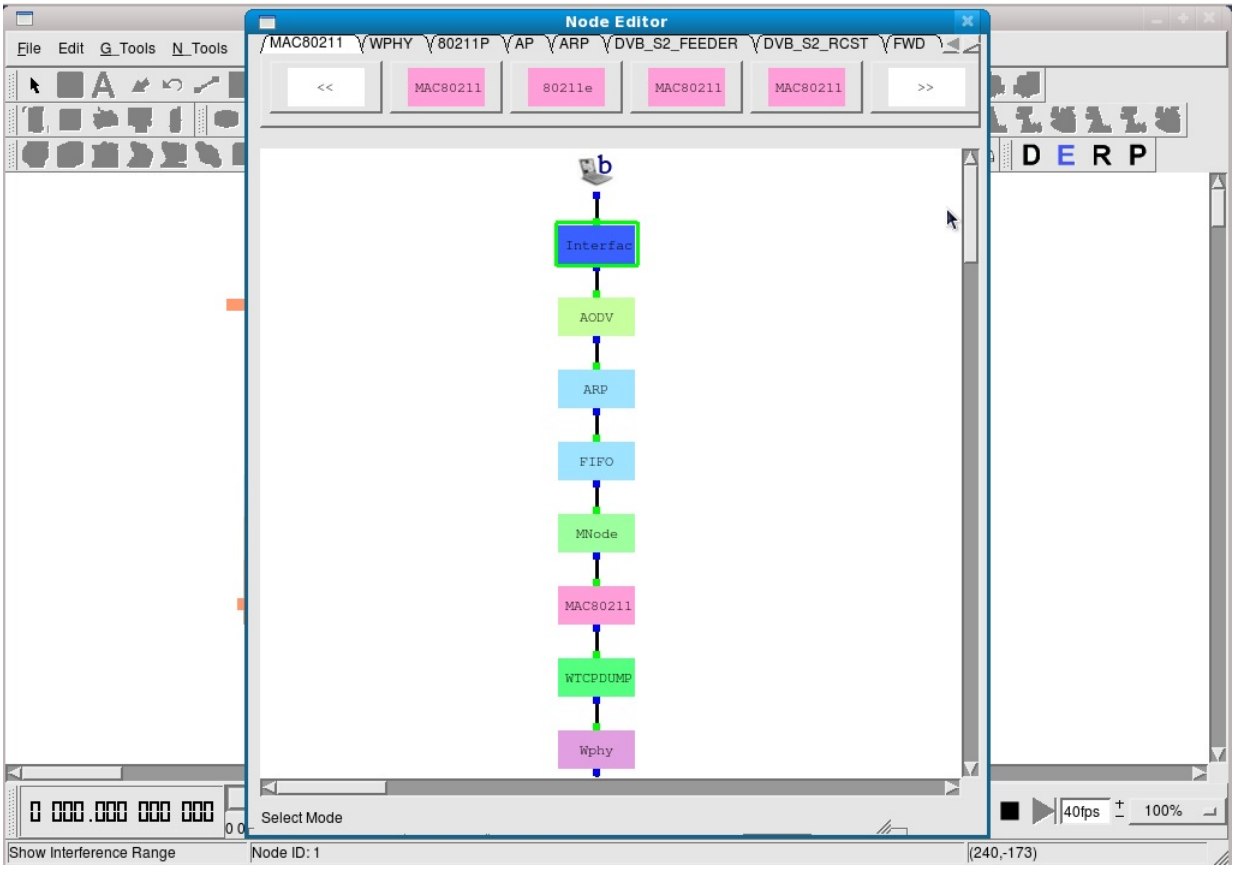

Figure 7.2: The node editor of NCTUns for 5 nodes

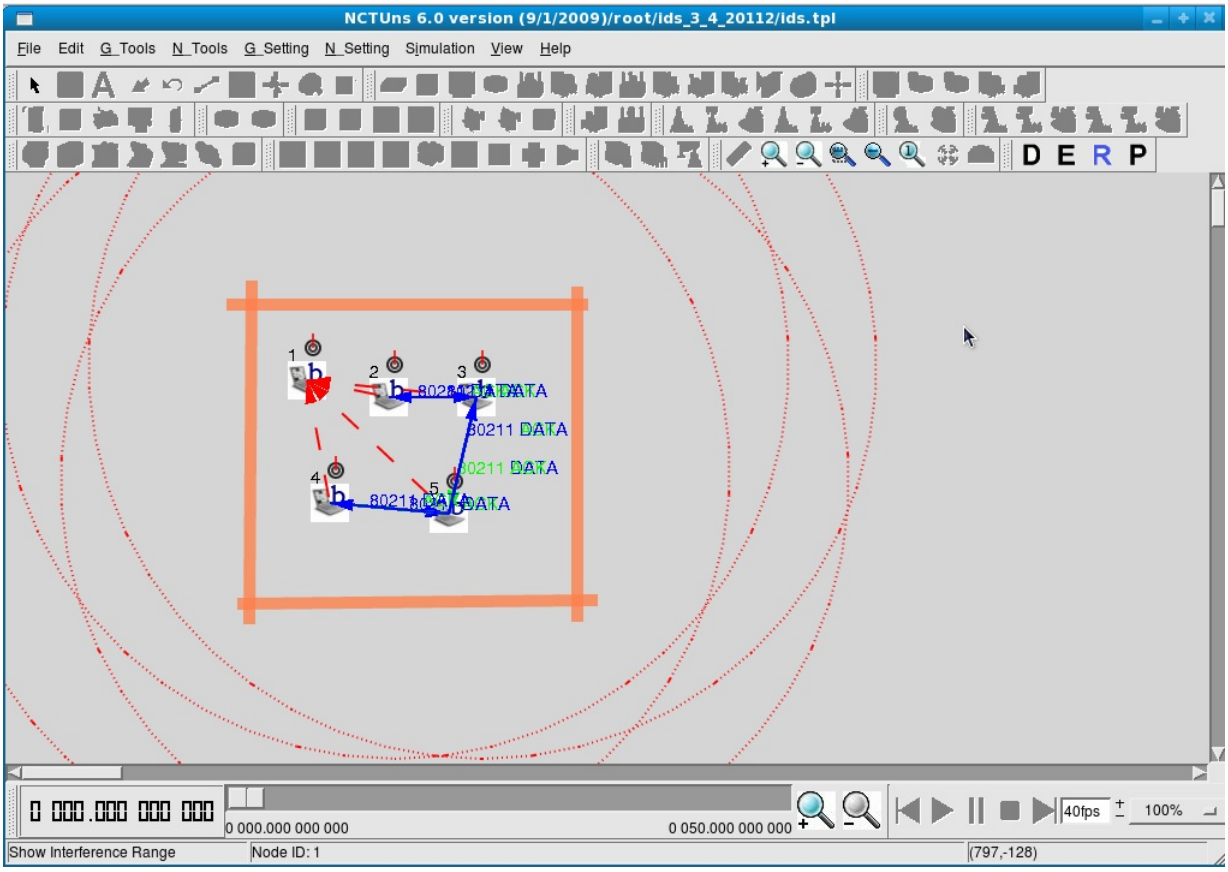

Figure 7.3: Data Transfer between 5 nodes in NCTUns

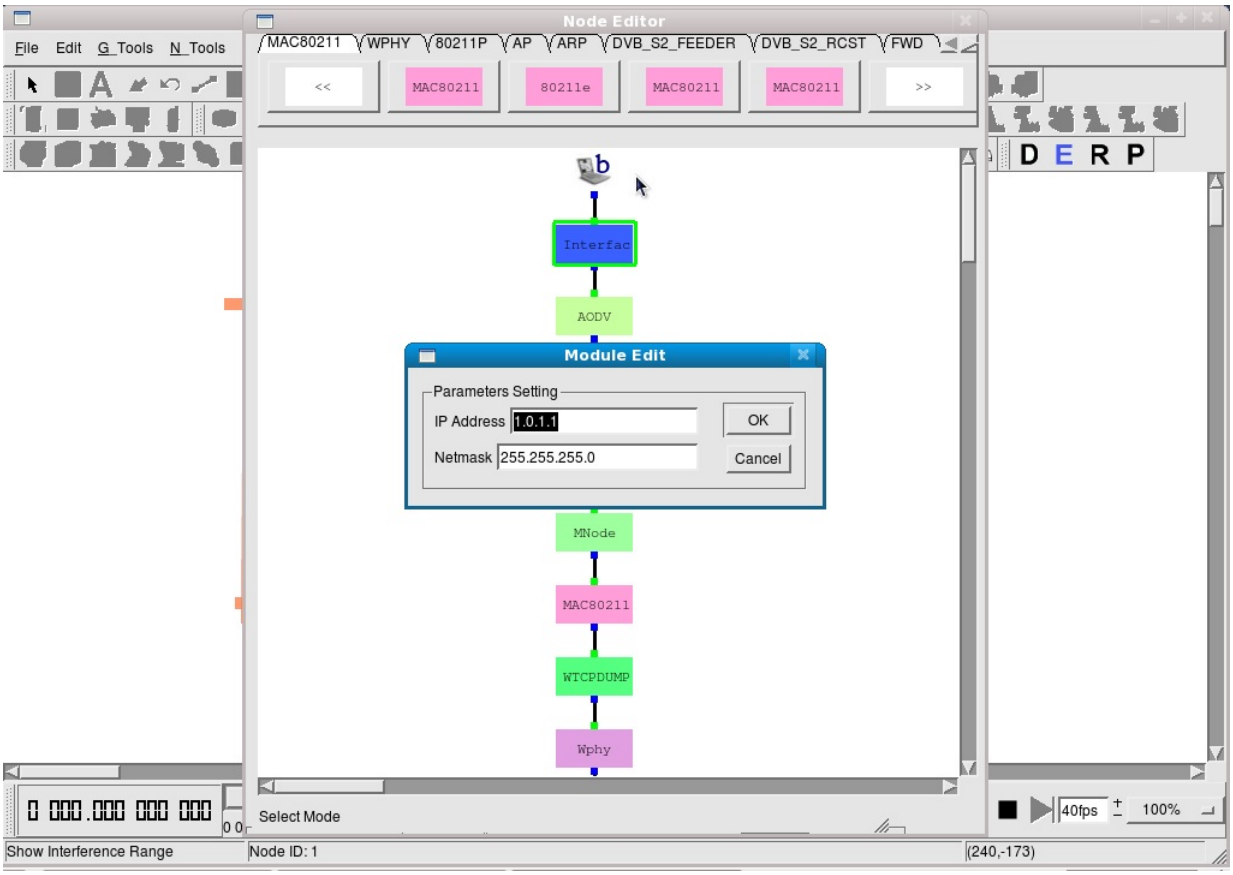

Figure 7.4: Interface Layer Parameter of nodes in NCTUns

7.3 Simulation Results

7.3.1 Average Accuracy of Detection Vs. Packet Collision

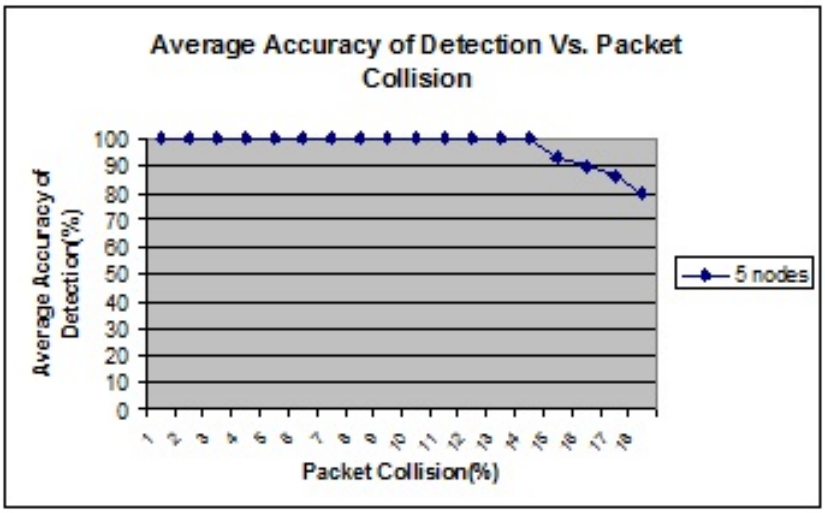

Figure 7.5: Average Accuracy of Detection Vs. Packet Collision for 5 nodes

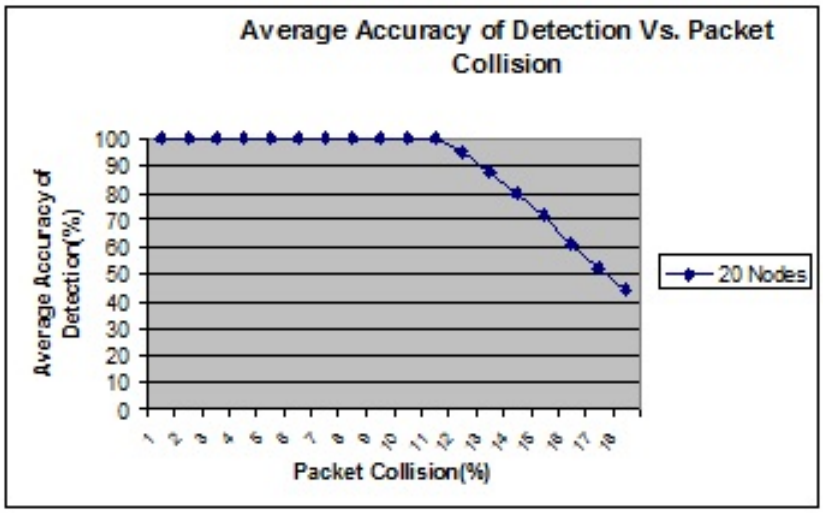

Figure 7.6: Average Accuracy of Detection Vs. Packet Collision for 20 nodes

The average accuracy of detection for the neighborhood of 5 nodes shown in Figure7.5 is 100%. Even for the case when the collision of packets is as high as 14%. Similarly, for the neighborhood of 20 nodes, the accuracy of detection shown

in Figure7.6 decreases as the percentage of collision increases as expected. However, it is noticed that as compared to the scenario of a neighborhood size of 5 nodes the decrease is more rapid. This is due to the reason that for the same percentage of collision the number of collisions is more in a neighborhood of size 20 than in a neighborhood of size 5. More number of collisions would mean higher loss of messages passed between the nodes and hence more adverse effect on the correct working of the algorithm.

7.3.2 Average False Detection Vs. Packet Collision

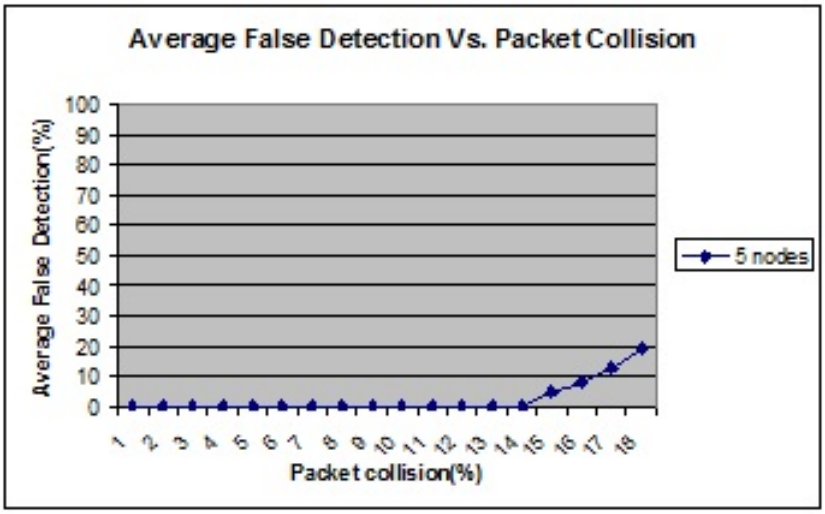

Figure 7.7: Average False Detection vs. Packet Collision for 5 nodes

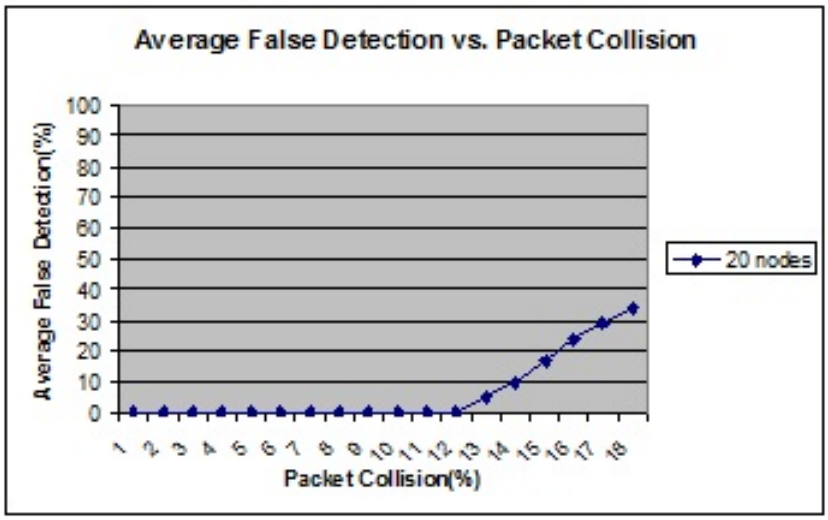

Figure 7.8: Average False Detection vs. Packet Collision for 20 nodes

False positives (false detection of non-malicious nodes) were seen to appear only when the percentage of collision is more than 14% shown in Figure7.7. The average false detection is found to be nil for collisions up to 14% for the neighborhood of 5 nodes. Similarly, for the neighborhood of 20 nodes,average false detection is found to be nil for collisions up to 12% shown in Figure 7.8. The average false detection is

found to be nil for collisions up to 12%. compare to above results more number of collisions would mean higher loss of messages passed between the nodes and hence more false detection of non-malicious nodes.

Chapter 8

Conclusion and Future Work

8.1 Conclusion

The algorithm uses collaborative efforts from a group of nodes for determining malicious nodes. For analyzing a particular node, the monitor node requests for the data packets from those two nodes that were to receive packets from the node under consideration. If even one of the two messages returned by the nodes matches with the actual data, the node is deemed as secure. Else, the node is marked as suspicious. The monitor node then uses the secure nodes to detect the malicious node(s) from the set of suspicious nodes. This method guarantees that no secure node is falsely accused to be malicious. Thus the algorithm detects the malicious nodes with high accuracy. Also, since each node has to forward messages to only 2 other nodes, hence this method greatly reduces congestion, and the probability of collision reduces further.

It can be seen from the simulation results that the proposed algorithm detects the malicious nodes successfully with a high percentage of accuracy when at most k malicious nodes are present in a set of n nodes even when there is a realistic percentage of packet collision (message destruction). Besides, average false detection is also minimal in such a scenario.

8.2 Future Work

- Implementation and test this algorithm with more number of messages transfer between monitor node and nodes to test accuracy of detection of malicious node.
- Extend this algorithm to select the monitor node which takes into account its degree, transmission power also.

Appendix A

INSTALLATION OF NCTUns

A.1 Download File:

http://nsl10.csie.nctu.edu.tw/products/nctuns/download/download2.php

Extract File:

[root@sunil] # tar xzvf NCTUns-allinone-linux-2.6.31.6-f12.20100113.tar.gz

Check Linux Version:

[root@sunil NCTUns-6.0]# uname -r

2.6.29.4-167.fc11.i686.PAE

A.2 Installation:

[root@sunil NCTUns-6.0]# ./install.sh

[root@sunil NCTUns-6.0]# yum –enablerepo=updates-testing update rpm

[root@sunil NCTUns-6.0]# yum install xinetd

[root@sunil NCTUns-6.0]# yum update yum -y

[root@sunil NCTUns-6.0]# ldconfig

[root@sunil NCTUns-6.0]#yum update xz-libs

[root@sunil NCTUns-6.0]# yum install xz-libs*

[root@sunil NCTUns-6.0]# yum install libICE.so.6

[root@sunil NCTUns-6.0]# yum install cronie

[root@sunil NCTUns-6.0]# yum install rsh-server

disable selinux

[root@sunil /]# echo 0 /etc/selinux/enforce

At final installation : you can see this message

==========

** Before you start using NCTUns, please check whether you have done

** all of these steps. According to our technical support experiences,

** most problems are caused by not performing all of these steps.

==========

** 0. The NCTUns programs have been successfully compiled and installed.

** 1. You have rebooted your system and is using the newly-built kernel.

** 2. The rlogin and rsh services in /etc/xinetd.d/rlogin and /etc/xinetd.d/rsh have been enabled.

** 3.$The NCTUNSHOME, NCTUNS_TOOLS, and NCTUNS_BIN environment variables$

** have been set properly.You can use the following command to do this job:

** [*csh/tcsh*]#*source/usr/local/nctuns/etc/nctuns.csh*

** [*bash*]#*source/usr/local/nctuns/etc/nctuns.bash*

** 4. You have stopped the iptables service by executing

** "service iptables stop".

** 5. You have set "SELINUX=disabled" in /etc/sysconfig/selinux

==========

** If you would like to seek helps or exchange your ideas/questions

** with other NCTUns users, you may check and use the following services:

** (1) NCTUns mailing list: http://nsl10.cs.nctu.edu.tw/pipermail/nctuns/

** (2) NCTUns forum: http://nsl10.cs.nctu.edu.tw/phpBB/

** Thank you.

Important Notice!

If your X-window system adopts KDE as the default desktop manager program, please BE SURE to upgrade your KDE version to 4.0.5 or higher. It is found that KDE 4.0.3 is likely to trigger unexpected signals to the NCTUns simulation engine, which may cause the simulation engine to run abnormally.

Besides, we suggest to upgrade the OpenGL library into the newest version because of the display of the GUI. If you have a video card equipped on your machine, please find the latest driver for your video card.

A.3 Upgrade KDE and OpenGL libraries:

To upgrade KDE and OpenGL libraries, you can use the following command:

yum update

Although this command will update all programs contained in Fedora 11 (including KDE, OpenGL libraries) and thus may take a long time, it is the easiest way to upgrade KDE. If you just upgrade KDE, some dependency problems may result.

#Restart your pc

#login in nctuns user name

usrname and password is nctuns

/etc/xinetd.d rlogin and rsh have been enabled.

service iptables stop

[root@sunil]# vim /etc/sysconfig/selinux

check selinux is disabled or not.

Execute NCTU Simulator

[root@sunil]# cd /usr/local/nctuns/bin/

[root@sunil bin]# ./nctunsclient

Appendix B

List of publication

Paper accepted at 'Indian Journal of Computer Science and Engineering' - May, 2011.
Paper Title **'Collaborative Anomaly-based Intrusion Detection in MANET'.**

References

[1] Marco Conti, Body, "Personal and Local Ad Hoc Wireless Networks",*in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.*

[2] M.S. Corson, J.P. Maker, and J.H. Cernicione, "Internet-based Mobile Ad Hoc Networking",*IEEE Internet Computing, pages 6370, July-August 1999.*

[3] Amitabh Mishra and Ketan M. Nadkarni, "Security in Wireless Ad Hoc Networks",*in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.*

[4] S. Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks",*in 6th International Conference on Mobile computing and Networking,MOBICOM00, P255-265, Aug 2000.*

[5] A. Hasswa, M. Zulker, and H. Hassanein,"Routeguard: an intrusion detection and response system for mobile ad hoc networks",*Wireless And Mobile Computing, Networking And Communication 2005, P336-343, Vol. 3, August 2005.*

[6] C. Manikopoulos, Li Ling, "Architecture of the mobile ad hoc network security (MANS) system",*in: Proceedings of the IEEE International conference on Systems. Man and Cybernetics, vol. 4, October 2003, pp. 3122-3127.*

[7] K. Nadkarni, A. Mishra,"Intrusion detection in MANETs the second wall of defense"*in: Proceedings of the IEEE Industrial Electronics Society Conference2003, Roanoke, Virginia, USA, November 26, 2003, pp. 12351239.*

[8] A. Partwardan, J. Parker, A. Joshi, M. Iorga, T. Karygiannis,"Secure routing and intrusion detection in ad-hoc networks",*in: Proceedings of Third IEEE International Conference on Pervasive Computing and Communications, Hawaii Island, Hawaii, March 812, 2005.*

[9] Y. Zhang, W. Lee, "Intrusion Detection in Wireless Ad-hoc Networks",*Mobicom 2000, August 611, 2000, Boston, Massachusetts, USA.*

[10] Y. Zhang, W. Lee, Y. Huang,*"Intrusion Detection Techniques for Mobile Wireless Networks",ACM WINET.*

[11] Tiranuch Anantvalee, Jie Wu, "A survey on intrusion detection in mobile ad hoc networks",*in: Y. Xiao, X. Shen,D.-Z. Du (Eds.), Wireless/Mobile Network Security, Springer, 2006, pp. 170196.*

[12] P. Albers, O. Camp, J.-M. Percher, B. Jouga, L. Me, R. Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches",*in:Proceedings of First International Workshop on Wireless Information Systems (WIS-2002)*

[13] O. Kachirski, R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks",*in: Proceedings of 36th Annual Hawaii International Conference on System sciences (HICSS03), January 2003, p. 57.1*

[14] S. Buchegger, J. Le Boudec, "Performance analysis of the CONFIDANT protocol Cooperation of nodes fairness in dynamic ad-hoc networks" *in: Proceedings Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc02), June 2002, pp. 226336.*

[15] P. Michiardi, R. Molva, Core,"A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks",*in: Proceedings of Sixth IFIP Communication and Multimedia Security Conference (CMS02), September 2002.*

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

[17] N. Marchang, R. Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks",*2007*

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

[19] M. Chatterjee, S.K. Das, D. Turgut, "WCA: a weighted clustering algorithm for mobile ad hoc networks",*Journal of Cluster Computing (Special Issue on Mobile Ad hoc Networks) 5 (2002) 193204.*

[20] Hendrik vom Lehn Elias Weingartner and Klaus Wehrle, "A performance comparison of recent network simulators",*http://jist.ece.cornell.edu/*

Index