creative commons
COMMONS DEED

저작자표시 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.
- 이차적 저작물을 작성할 수 있습니다.
- 이 저작물을 영리 목적으로 이용할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

[UCI]I804:24011-200000239616

February 2010

Master's Degree Thesis

Intrusion Detection System in Mobile Ad-hoc Networks Incorporating Cross Layer

Graduate School of Chosun University

Department of Information and Communication Engineering

Rakesh Shrestha

RAKESH SHRESTHA

Intrusion Detection System in Mobile Ad-hoc Networks Incorporating Cross Layer

Master's Degree Thesis

February 2010

Intrusion Detection System in Mobile Ad-hoc Networks Incorporating Cross Layer

February 25, 2010

Graduate School of Chosun University

Department of Information and Communication Engineering

Rakesh Shrestha

Intrusion Detection System in Mobile Ad-hoc Networks Incorporating Cross Layer

Advisor: Prof. Seung-Jo Han

This thesis is submitted to Chosun University in partial fulfillment of the requirements for a Master's Degree

October 2009

Graduate School of Chosun University

Department of Information and Communication Engineering

Rakesh Shrestha

Rakesh Shrestha's
Master's Degree Thesis
Approval

Committee Chairperson Prof. Jong-An Park (인)

Committee Member Prof. Seung-Jo Han (인)

Committee Member Prof. Goo-Rak Kwon (인)

November 2009

Graduate School of Chosun University

Table of Contents

ABSTRACT

Ⅰ. Introduction ····· 1

A. Overview ····· 1

B. Motivation ····· 3

C. Thesis contribution ····· 4

D. Thesis organization ····· 5

Ⅱ. Related Works ····· 6

Ⅲ. MANET Routing Protocols ····· 8

Ⅳ. Intrusion Detection System ····· 10

A. Intrusion detection overview and techniques ····· 10

1. Misuse based detection ····· 12

2. Anomaly based detection ····· 13

3. Specification-based detection systems ····· 15

B. Challenges and vulnerabilities of IDS in MANET ····· 16

C. Cross layer techniques in IDS ····· 17
D. Association module ····· 19
E. Intrusion detection module ····· 23
1. Local data collection ····· 24
2. Local detection ····· 24
3. Co-operative detection ····· 25
4. Alert management ····· 26

V. Anomaly Detection Mechanism in MANET ··· 27
A. Construction of normal dataset ····· 28
B. Feature construction ····· 28
C. Training normal data using clustering mechanism ···· 29
D. Fixed width algorithm ····· 30
E. Explanation of the algorithm ····· 32
F. Testing phase ····· 33

VI. Attacks in Different Protocol Layers ····· 34

VII. Performance Evaluation ····· 38
A. Simulation setup ····· 38

B. Evaluation of results 41

VIII. Conclusions and Future Work 50

References 51

List of Figures

Figure 1.1 General Ad-hoc working principle ····· 2
Figure 3.1 Routing scenario of an AODV ····· 9
Figure 4.1 A typical misuse detection system ····· 13
Figure 4.2 A typical anomaly detection system ····· 14
Figure 4.3 IDS techniques ····· 16
Figure 4.4 Proposed IDS architecture in MANET ····· 24
Figure 7.1 Simulation scenario ····· 40
Figure 7.2 UDP traffic analysis in destination node ····· 42
Figure 7.3 Time-average in AODV routing traffic sent ····· 43
Figure 7.4 Wireless LAN data traffic received (bits/sec) ····· 44
Figure 7.5 Wireless LAN control traffic (bits/sec) ····· 46
Figure 7.6 Wireless LAN data traffic (bits/sec) ····· 47
Figure 7.7 Wireless LAN load (bits/sec) on random nodes ····· 48

List of Table

Table 6.1 Attacks in wireless ad-hoc networks ····· 37

Table 7.1 Simulation parameters ····· 40

Table 7.2 Comparison with other intrusion detection system.....49

List of Acronyms

AODV : Ad hoc On-demand Distance Vector
DoS : Denial of Service
HIDS : Host Intrusion Detection System
ICMP : Internet Control Message Protocol
IDS : Intrusion Detection System
IP : Internet Protocol
MAC : Medium Access Control
MANET: Mobile Ad-Hoc Network
NIDS : Network Intrusion Detection System
Pkt : Packet
RERR : Route Error
RREP : Route Reply
RREQ : Route Request
UDP : User Datagram Protocol

초 록

크로스 층을 통합하고 있는 모마일 에드-혹 네트워크의 침입 탐지 시스템

Rakesh Shrestha
지도 교수 : 교수 한승조
정보통신공학과
조선대학교 일반대학원

무선네트워크 기술의 인기 속에는 위협과 안보의 문제가 있다. MANET는 무선 모바일 Ad hoc네트워크의 진화를 가져왔으나 다른 측면에서는 동적인 네트워크 토폴로지, 집중화 부족, 부적절한 인증과정, 불안전한 라우팅에 직면했고, 이런 측면에서 여러 종류의 공격에 취약하다. 따라서, 침입 탐지는 무선일 뿐만 아니라 유선의 안전의 필수 불가결한 구성요소를 형성한다. 전통적으로, 침입 탐지는 하나의 층에서 사용된다. 그러나 증대하는 경향에 뒤지지 않고 따라가기 위해, 하나의 층 발견 기술을 멀티 층 발견으로 교체할 중대한 필요가 있다. 다른 타입의 DoS 공격은 인가된 사용자를 네트워크에 접근하는 것에서 방해합니다. 그리고 우리는 그 공격의 일부를 발견하고 또한 경감하려고 노력을 한다. 탐지의 정확성을 개선하기 위해 프로토콜 스택의 다른 층을 가로질러 정보를

침입하는 악의적 노드를 발견하기 위해 새로운 크로스 레이어 침입 탐지 시스템 구조를 제안한다. 우리는 침입 탐지 함께 향상된 변칙적 기술로 제안된 구조를 사용한다. 우리 제안된 구조는 단체 모델을 사용하여 데이터 오버헤드를 줄이는 것을 도와준다. 단체 모델 방법은 데이터 탐지 기술과 같은 방법으로 사용되며, 고정 폭 알고리즘은 비정상적인 행동을 구별하는 훈련과 테스트를 위해 사용되었다. 제안된 구조의 시뮬레이션은 OPNET 모의 장치에서 실행했으며 그리고 그 결과는 분석했다.

ABSTRACT

Intrusion Detection System in Mobile Ad-hoc Networks Incorporating Cross Layer

Rakesh Shrestha
Advisor: Prof. Seung-Jo Han
Department of Information and Communication Engineering,
Graduate School of
Chosun University

With the popularity of wireless technology there are always threats and security issues. MANET brings evolution in Wireless mobile Ad-hoc networks but it has to face many difficulties due to the dynamic network topologies, lack of centralization, inadequate authentication mechanism, and insecure routing. They are vulnerable to different types of attacks. Therefore, intrusion detection forms an indispensable component of wired as well as wireless security. Traditionally, intrusion detection is used in single layer but to keep pace with the growing trends, there is a critical need to replace single layer detection technology with multi layer detection. Different types of Denial of Service (DoS) attacks thwart authorized users from gaining access to the networks and most of them are detect as well as alleviated. A novel cross layer intrusion detection architecture is proposed to discover the malicious nodes by

exploiting the information available across different layers of protocol stack in order to improve the accuracy of detection. A cooperative intrusion detection with anomaly technique is used to enhance the proposed architecture. The proposed architecture helps to reduce the data overhead by using association model. A clustering method is used as a data mining technique and fixed width algorithm is used for the training and testing phase in order to discriminate the abnormal behavior from the normal behavior. The simulation of the proposed architecture is performed in OPNET simulator and the results are analyzed.

Ⅰ. Introduction

A. Overview

MANET is a self configuring ad-hoc network of mobile nodes and associated hosts connected by wireless links. Some of the characteristic features of MANET are nodes are free to move randomly i.e. they have high mobility, organize themselves arbitrarily, dynamic network topology, and hence they have decentralized network control. Such a network may operate in a standalone fashion, or may be connected to the larger network, and consume very low power as well as resources. One of the differences between fixed wired and mobile wireless networks is that mobile nodes have a very limited bandwidth and battery power because efficient host-based monitoring requires large amounts of CPU processing power, and hence is energy consuming.

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. Nodes within each other's radio range communicate directly via wireless links, while those that are out of range use other nodes as relays or routers. Nodes usually share the same physical media; they transmit and acquire signals at

the same frequency band, and follow the same hopping sequence or spreading code. The data link layer manages the wireless link resources and coordinates medium access among neighboring nodes. The medium access control (MAC) protocol allows mobile nodes to share a common broadcast channel. The network layer holds the multi hop communication paths across the network. All nodes must function as routers that discover and maintain routes to other nodes in the network.

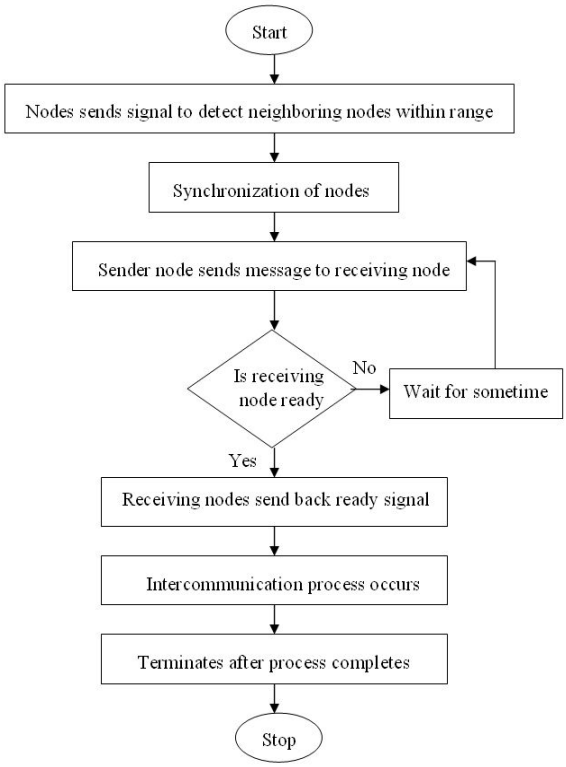

Figure.1.1 General working principle of Ad-hoc networks

There are various applications of ad-hoc networks like emergency search-and-rescue missions, military, data collection etc. The flowchart in figure 1.1 depicts the general working principle of any general ad-hoc networks [1].

Some of the main characteristics of MANET are discussed in [2] like the MANET node is autonomous and works as router and host. It is distributive as well as dynamic, and multi-hop is necessary if the receiver node is out of radio range and it has unstable link bandwidth.

B. Motivation

Wireless mobile ad-hoc network is an evolving technology which has to face many difficulties due to the dynamic network topologies, lack of centralization, inadequate authentication mechanism, insecure routing and are vulnerable to different types of attacks. A new challenges and opportunities were created by this new networking environment and explore new approaches to secure its communication. AODV routing protocol has been implemented because it offers quick adaptation to dynamic link conditions, low processing and memory overhead and low network utilization.

It is also difficult for IDS to fully detect routing attacks due to MANET's characteristics. So, the IDS needs a scalable architecture

to collect sufficient evidences to detect those attacks effectively. A malicious node may take advantage of the MANET nodes to launch different types of attacks because the nodes act as routers to communicate with each other. Also, the wireless links between the nodes, and the mobility raises the challenges of IDS to detect the attacks. Hence, a new IDS architecture is designed which involves cross layer design to efficiently detect the abnormalities in the wireless networks.

C. Thesis contribution

The characteristic parts of the carried research work are discussed under the title of the thesis contribution. As we know, many works has been carried out in the field of wireless IDS and most of them focuses on one or two aspects of intrusion detection and most of the works are carried out on independent single layer. A new intrusion detection architecture has been proposed which incorporates cross layer that interacts between the layers. Association module has been used which helps in low overhead in the data collection. The fixed width clustering algorithm has been implemented in anomaly detection engine for efficient detection of intrusion in the ad-hoc networks.

D. Thesis Organization

The content of this thesis is organized in modular chapters. Chapter II is devoted to brief description of related works in MANET intrusion detection. Chapter III argues about the MANET routing protocols. Chapter IV is a detail description of Intrusion detection system and its underlying architecture module. The anomaly detection mechanism used in MANET is discussed in chapter V. Similarly, various types of attacks that occur in different protocols layers are handled in chapter VI. Chapter VII is dedicated on the performance evaluation under which the simulation scenario and the evaluation of results are presented for the verification of the proposed architecture. Then, the last chapter concludes the thesis with wrapping text for the summary of the carried research and possible future works.

Ⅱ. Related Works

A lot of studies have been done on security prevention measures for infrastructure-based wireless networks but few works has been done on the prospect of intrusion detection [3]. Some general approach has been used in a distributed manner to insure the authenticity and integrity of routing information such as key generation and management on the prevention side. Authentication based approaches are used to secure the integrity and the authenticity of routing messages such as [4], [5]. There are some difficulties that have to be faced in realizing some of the schemes like cryptography, and they are relatively expensive on MANET because of computational capacity. Also, authentication is more difficult to implement due to lack of central authority and these schemes can only prevent from external attacks but difficult to prevent from internal attacks [6]. A number of intrusion detection schemes for intrusion detection system have been presented for ad-hoc networks. In [7], the paper proposed architecture for a distributed and cooperative intrusion detection system for ad-hoc networks based on statistical anomaly detection techniques but they have not properly mentioned about the simulation scenario and the type of mobility they have used. Mishra emphasizes the challenge for intrusion detection in ad-hoc network and purpose the use of

anomaly detection, but do not provide a detailed solution or implementation for the problem [8]. In [9], Huang details an anomaly detection technique that explores the correlations among the features of nodes and discusses about the routing anomalies. Loo, presents an intrusion detection method using a clustering algorithm for routing attacks in sensor networks [10]. It is able to detect three important types of routing attacks. They are able to detect sink hole attacks effectively which are intense form of attacks. There are some flaws like; there is no development of a simulation platform that can support a wider variety of attacks on larger scale networks. Several specifications based IDSs have been proposed that model the behavior of the routing protocol using a Finite State Machine (FSM) and try to classify anomalies - deviations from expected behavior, as attacks. Tseng describes several attacks possible in the base AODV protocol [11]. They illustrated the use of a finite state machine to detect anomalous behavior in order to determine attacks. Fixed width clustering algorithm has shown to be highly effective for anomaly detection in network intrusion [12]. It presents a geometric framework for unsupervised anomaly detection. This paper needs more feature maps over different kinds of data and needs to perform more extensive experiments evaluating the methods presented.

Ⅲ. MANET Routing Protocols

The IDS model is based on Ad-hoc On-Demand Distance Vector (AODV) routing protocol which is a forwarded routing protocol that provide efficient and low over head protection. The route building process relies heavily on forwarded messages; the malicious node can change the other nodes' routing table and launch sophisticated routing attacks such as man in the middle attack and DoS attacks by comprehensively manipulating forged contents of forwarded routing messages.

The AODV routing protocol uses an on-demand approach for finding routes, i.e a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. A sequence number can be updated by the source or the destination. It has small size routing messages, which contain only routing information for the source and destination. While a source node S requires a route toward a destination node D, node S broadcasts a RREQ message to request for the route. Upon receiving RREQ, the receiver discards it if it formerly received the same RREQ message; by checking RREQ with the same source address and the same RREQ ID. Otherwise, the receiver updates and stores the reverse

route towards the source if RREQ has a higher source sequence number or an equal sequence number than that the receiver had in the routing table. If the receiver has a valid route toward the destination D or the receiver itself is the destination D, it will generate a RREP message and unicast reply along the reverse route toward the source S. The source node or the intermediate nodes that receives RREP message will update their forward route to destination in the routing tables else they continue broadcasting the RREQ. If a node receives a RREQ message that has already processed, it discards the RREQ and does not forward it. After the route has been established between source node S and destination node D, if one intermediate node X notices that it cannot reach another node Y which was previously reachable from Z, in that case route error packets (RERR) are broadcasted to announce this broken link. RERR are propagated to the source node along the reverse route and all intermediate nodes will erase the entry in their routing table [13].

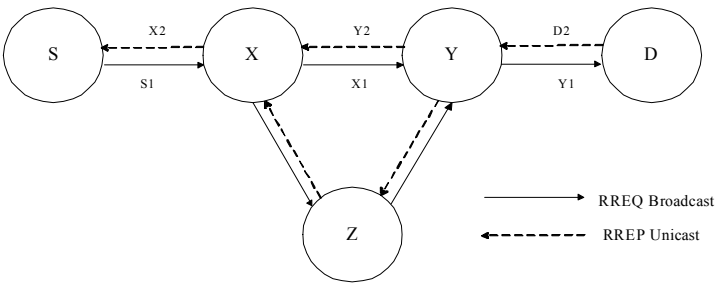

Figure. 3.1 Routing scenario of an AODV

Ⅳ. Intrusion Detection System

A. Intrusion detection overview and techniques

An Intrusion Detection System (IDS) is a software or hardware tool used to detect unauthorized access of a computer system or network. An intruder attempts to access information, or manipulate information causing a system unreliable or unusable. Intrusion prevention techniques such as using password or biometrics are the first line of defense and are not adequate in MANET due to its decentralized structure [14]. In a wireless ad-hoc network, a dedicated gateway node can not be assumed because of the fugacious nature of the network. IDS can be used as a second wall of defense to guard the network systems as once the intrusion is detected in the early stage of the DoS attack; damages can be minimized, gather evidence for prosecution and even lunch counter-attacks. Intrusion detection involves capturing audit data and reasoning about the evidence in the data to determine if the system is under attack or not. Depending upon the detection model IDS is classified as signature-based and anomaly based detection. More detail about Anomaly detection is discussed in chapter V. Security services like access controls and authentication services can enhance

the security of the ad-hoc networks. Intrusion detection involves the runtime gathering of data from system operations, and the subsequent analysis of the data; these data can be audit logs generated by an operation systems or packets sniffed from a network [13].

An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once IDS determines an unusual activity or an activity that is known to be an attack, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity. Although there are several intrusion detection techniques developed for wired networks today, they are not suitable for wireless networks due to the differences in their characteristics. Therefore, those techniques must be modified or new techniques must be developed to make intrusion detection work effectively in MANETs [15].

Depending on the scope of protection or deployment, and according to audit data used, IDS can be classified as network-based, host-based or hybrid. A Network Intrusion Detection System (NIDS) identifies intrusions by examining network traffic and monitors multiple hosts and gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort. But a Host-based

Intrusion Detection System (HIDS) consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications and other host activities and state. Where as Hybrid Intrusion Detection System combines both approaches and have certain benefits over the two.

In addition, IDS may be classified based on the detection technique as described below:

1. Misuse based detection systems

In case of misuse detection system, also known as Signature based detection, the attacks are represented in the form of a pattern or signature so that even the variation of the same attack can be detected. The main issues in misuse detection systems are how to write a signature that encompasses all possible variations of the pertinent attack, and also how to write signatures that do not match non-intrusive activity. The system keeps signatures of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. This technique may achieve low false positive rates, but does not perform well at detecting previously unknown attacks. One of the problems with signature detection system is that it must have a signature defined for all of the possible attacks that an attacker may launch which requires frequent signatures updates to keep the data base

up-to-date. Some of the approaches to misuse based detection system are Expert system, keystroke monitoring, model based intrusion detection and state transition analysis [16]. A block diagram of typical misuse detection system is shown in figure 4.1.

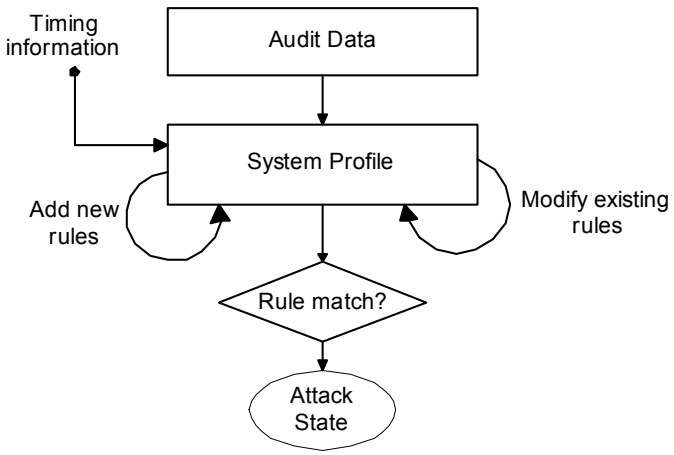

Figure 4.1 A typical misuse detection system

2. Anomaly based detection systems

Anomaly detection systems assume that all the intrusive activities are anomalous activities which mean if we could establish a normal activity profile for a system, all the system states varying from the established profile could be flagged by statistically significant amounts of intrusion attempts. The normal profiles or behaviors of users are kept in the system. The system compares the captured data with these profiles, and then deal with any activity that deviates from the baseline as a possible intrusion by informing

system administrators or initializing a proper response. Anomaly detection system can detect new and unknown attacks and can generate an alarm if the system detects an intrusive activity. This system is suitable for unknown attacks but it gives high false positives rates. Also, Anomaly detection technique requires less modification on current routing protocols. The advantages of anomaly detection is that there are possibility of detection of novel attacks as intrusions, attacks are recognized without getting inside their causes, and characteristics as well as ability to detect abuse of user privileges. The main issue in anomaly detection system is the selection of the threshold levels and the selection of features to monitor. Some of the approaches to anomaly intrusion detection system are Statistical approach, predictive pattern generation, neural networks, data mining etc. The typical block diagram of anomaly detection system is shown in figure 4.2.

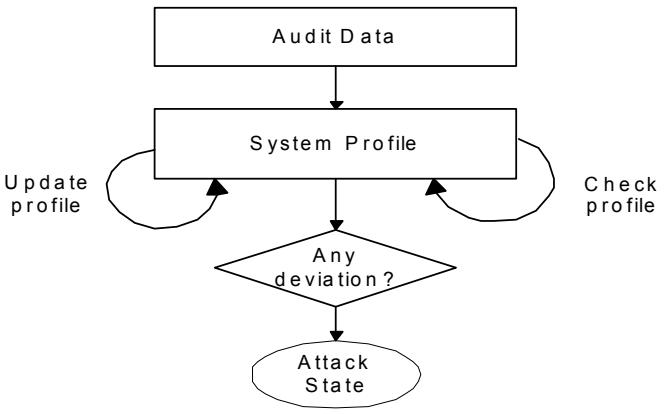

Figure 4.2 A typical anomaly detection system

3. Specification-based detection systems

The specification-based detection system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints. This technique may provide the capability to detect previously unknown attacks, while exhibiting a low false positive rate. Usually, this system involves the use of finite state machines for specifying correct routing behavior and distributed network monitors for detecting run-time violation of the specifications. In [17], the correct behaviors of critical objects are manually abstracted and crafted as security specifications, and this is compared with the actual behaviors of the objects. Intrusions can be detected without exact knowledge about them; which usually cause objects to behave in an incorrect manner.

Another classification based on IDS architecture classifies the existing IDSs into three categories: stand alone, distributed and hierarchical. A more detailed taxonomy and information about IDSs can be found in [15] [18] [19].

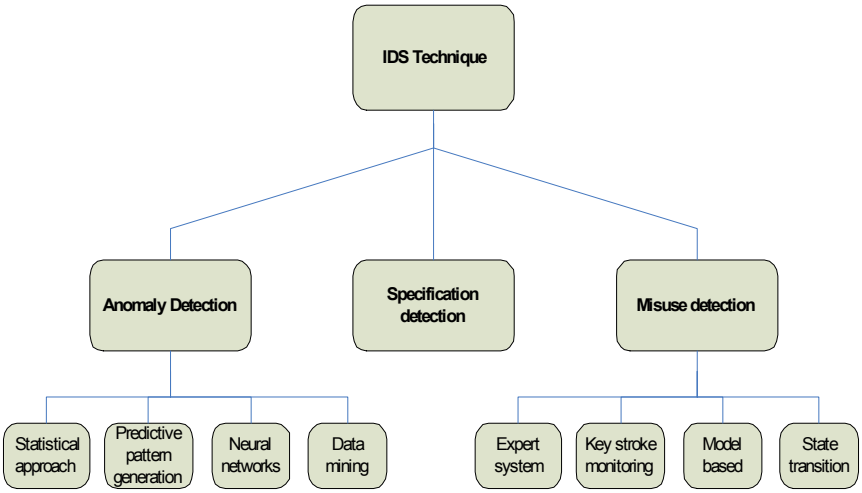

Figure 4.3 IDS techniques

B. Challenges and Vulnerabilities of IDS in MANET

Because of wireless features and ad-hoc structure of MANET, some limitations are incurred and MANET has to face different challenges in compared with wired networks. The very advantage of mobility in MANET leads to its vulnerabilities. But the inherent nature of the wireless medium makes it susceptible to security attacks ranging from passive eavesdropping to active interference. Authentication mechanisms are not sufficient and effective against internal attacks as the secret key is compromised when its node is compromised. In order to secure MANET, we need a second line of defense to detect the intrusions [20]. MANETs are vulnerable to

DoS attacks due to open medium, limited bandwidth, slower links, higher costs, battery constrains and disconnected operations. Also, wireless links between mobile nodes in MANET are very unreliable than those in wired network; so the detection mechanism must be capable of tolerating message loss in order to have sufficient data to analyze and to maintain detection accuracy. In addition, MANETs do not have trust management between them, so attacks may spread and immobilize the network.

C. Cross layer techniques in IDS

The traditional way of layering network approach that is separating routing, scheduling, rate and power control is not efficient for ad-hoc wireless networks. A. Goldsmith discussed that rate control, power control, medium access and routing are building block of wireless network design [21]. Generally, routing is considered in a routing layer and medium access in MAC layer whereas power control and rate control are sometimes considered in a PHY and sometimes in a MAC layer. If there is no cross layer interaction then the routing can select between several routes and have no information about congestion or malicious nodes. As a result, it selects a congested route or it selects a route that includes malicious nodes. With the help of cross layer interaction, the routing

forwards possible route choices to MAC. MAC decides on possible routes using congestion and IDS information as well as returns the result to the routing.

The selection of correct combination of layers in the design of cross layer IDS is very critical to detect attacks targeted at or sourced from any layers rapidly. It is optimal to incorporate MAC layer in the cross layer design for IDS as DoS attack is better detected at this layer. The routing protocol layer and MAC layer are chosen for detecting routing attacks in an efficient way. Data with behavioral information that consists of layer specific information are collected from multiple layers and forward it to data analysis module which is located in an optimal location [22]. This cross layer technique incorporating IDS leads to an escalating detection rate in the number of malicious behavior of nodes increasing the true positive and reducing false positives in the MANET. It also alleviates the congestion which can adapt to changing network and traffic characteristics. In order to evade congestion and reroute traffic MAC and routing layers have to cooperate with each other with the IDS in order to avoid insertion of malicious nodes in the new routes. The physical layer collects various types of communication activities including remote access and logons, user activities, data traffics and attack traces. MAC contains information regarding congestion and interference. The detection mechanism for misbehaving nodes

interacts with routing layer for the detection process as MAC layer also helps in detection of certain routing attacks. MAC also interacts with the physical layer to determine the quality of suggested path [23]. By combining cross layer features, attacks between the layers inconsistency can be detected. Furthermore, these schemes provide a comprehensive detection mechanism for all the layers i.e attacks originating from any layers can be detected with better detection accuracy.

D. Association module

Association rule describes alliance of attributes within transaction records of an inspection data set. Once association rules are extracted from multiple segments of a training data set, they are then aggregated into a rule set. The feature sets consist of control and data frames from MAC frames and control packets like RREQ, RREPand RERR including data packets of IP packets from network layer. All the control packets are combined into one category as routing control packet and IP data packet as routing data packet. So, the payloads in MAC data frames contain either a routing CtrlPkt or routing DataPkt [24]. The feature set is foreshortened by associating one or more features from different layers to specific MAC layer feature so that the overhead of learning is minimized.

The characteristics are assorted based on dependency on time, traffic and other features [25].

The association rule is of the form X→ c,sup, and the itemsets are given by

$$X \cap Y = \emptyset \qquad (4-1)$$

$$\text{and } c = \frac{\sup(X \cup Y)}{\sup(X)} \qquad (4-2)$$

where X and Y are itemsets, sup(XUY) is the support of the rule, and c is the confidence.

Let D be database of traffic and the association rules have support and confidence greater than minimum support (minsup) and minimum confidence (minconf) respectively [26]. Support and confidence are generally used to measure the relevance of the association rules. The association rule is decomposed into itemsets and the rules. The itemsets with minimum supports are called frequent itemsets. In the Apriori algorithm, the contender itemsets to be counted is given permission by using only the itemsets found frequently in the previous permission without considering the transactions in the database. The contender itemsets having k items can be generated by joining frequent itemsets having k−1 items, and removing those which contain any subset that is not frequent hence reducing the number of contender itemsets. Let F_k be the set of frequent k−itemsets having minimum support and C_k be the set of

contender k−itemsets with potentially frequent itemsets and E be the events. Each of these itemsets has itemset and support count fields. The initial pass of the algorithm simply counts item occurrence to determine the frequent 1−itemsets. A succeeding pass k consists of two phases. The first phase consists of frequent itemsets F_{k-1} found in the (k−1)th permission that are used to generate the candidate itemsets C_k . In the other phase, the database is scanned and the support of candidates in C_k is counted. The Apriori algorithm is as follows:

F_k := {frequent 1−itemsets};

k :=2; // k is the permission number

while ($F_{k-1} \neq \emptyset$) **do begin**

C_k: =New contender of size k generated from F_{k-1}

forall transactions $E \in D$ **do begin**

Increment the count of all contenders in C_k that are contained in E.

end

F_k: = All contenders in C_k with minimum support.

k := k+1;

end

Basic algorithm for rule:

All non−empty subsets of f is found to generate rules for every frequent itemset f. For every subset a, a rule of the form a⇒

(f−a) is output if the ratio of support (f) to support (a) is at least minconf. All subsets of f are considered to generate rules with multiple consequents.

A simple rule algorithm is as follows:

```
forall frequent itemsets f_k , k≥2 do
        call genrules (f_k, f_k);

// The genrules generates all valid rules ã⇒(f_k− ã), for all ã⊂a_m
procedure genrules (f_k: frequent k−itemset, a_m: frequent m−itemset)
A := {(m-1)-itemsets a_m-1 | a_m-1 ⊂a_m };

forall a_m-1 ∈ A do begin
        conf :=support (f_k)/support (a_m-1);
        if (conf≥ minconf) then begin
                output the rule a_m-1 ⇒(f_k− a_m-1), with confidence=conf
                        and support=support (f_k);
                if (m−1> 1) then
                call genrules (f_k, a_m-1); //to generate rules with subsets of a_m-1
                                                // as the antecedents
                end
        end
```

E. Intrusion detection module

Data mining techniques in Intrusion detection system has been used in order to improve the efficiency and effectiveness of the proposed architecture. It is found out that among all the data mining intrusion detection techniques, clustering-based intrusion detection is the most potential one because of its ability to detect new attacks. Many traditional intrusion detection techniques are limited with collection of training data from real networks and manually labeled as normal or abnormal. It is very time consuming and expensive to manually collect pure normal data and classify data in wireless networks. [27].

I have used an association algorithm such as Apriori which can be utilized to achieve traffic features which is then followed by clustering algorithm. In [27], it states that a good efficiency and performance is obtained with association algorithm and clustering algorithm. Association rule and clustering are used as the root for accompanying anomaly detection of routing and other DoS attacks in mobile ad-hoc networks. The proposed IDS architecture is shown in figure 4.4 and the IDS module is described below.

1. Local data collection

The local data collection module collects data streams of various information, traffic patterns and attack traces from physical, MAC and network layers via association module. The data streams can include system, user and mobile nodes' communication activities within the radio range. The audit data collects useful application data and system log files; and monitors the events. It then computes time, traffic, and other statistics; and records the feature values.

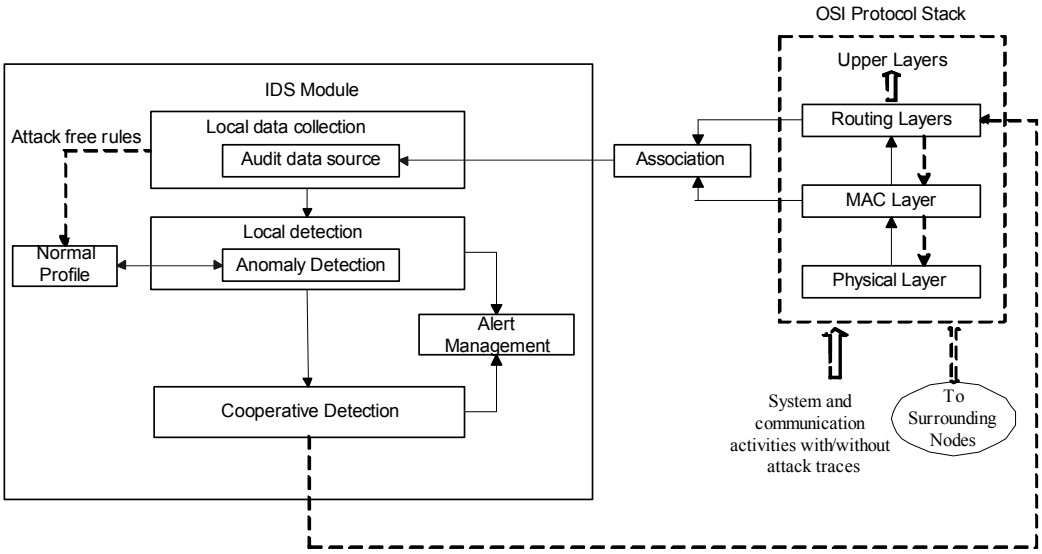

Figure 4.4 Proposed IDS architecture in MANET

2. Local detection

The local detection module consists of anomaly detection engine.

The local detection module analyzes the local data traces gathered by the local data collection module for evidence of anomalies. A normal profile is an aggregated rule set of multiple training data segments. According to Teresa, "A profile is a description of the normal behavior of a user with respect to a particular measure" [28]. New and updated detection rules across ad-hoc networks are obtained from normal profile. The normal profile consists of normal behavior patterns that are computed using trace data from a training process where all activities are normal. During testing process, normal and abnormal activities are processed and the deviations from the normal profiles are recorded. The anomaly detection distinguishes normalcy from anomalies by comparing with the test data profiles with the expected normal profiles. If any detection rules deviate beyond a threshold interval and if it has a very high accuracy rate it can determine independently that the network is under attack and initiates the alert management. The detail of anomaly detection mechanism is discussed in chapter V.

3. Cooperative detection

When the support and confidence level is low or intrusion evidence is weak and inconclusive in the detecting node then it can make collaborative decision by gathering intelligence from its

surrounding nodes via protected communication channel. The decision of cooperative detection is based on the majority of the voting of the received reports indicating an intrusion or anomaly. If the majority of the neighboring nodes indicate that there is an anomaly then it concludes that the network is under attack.

4. Alert management

The alert management receives the alert from the local detection or co-operative detection depending on the strength of intrusion evidence. It collects them in the alert cache for t seconds. If there are more abnormal predictions than the normal predictions then it is regarded as "abnormal" and with adequate information an alarm is generated to inform that an intrusive activity is in the system. But one has to be careful about the false alarm rate. In order to reduce the false alarm rate, filters are used. Hence, repeated trials are needed before a good anomaly detection model is produced.

Ⅴ. Anomaly Detection Mechanism in MANET

The anomaly detection system creates a normal base line profile of the normal activities of the network traffic activity. Then, the activity that diverges from the baseline is treated as a possible intrusion. The main objective is to collect set of useful features from the traffic to make the decision whether the sampled traffic is normal or abnormal. Anomaly detection system can detect new as well as unknown attacks, it can detect insider attacks, and it is very difficult for the attacker to carry out the attacks without setting off an alarm [29]. The process of anomaly detection comprises of training and testing phases. For normal behavior, basic frame work is built by collecting the noticeable characteristic from the audit data. The data mining technique has been used for building IDS to describe the anomaly detection mechanism. The basic anomaly detection mechanism is as follows:

1) Choosing the data from the audit data to form normal dataset
2) Construct the feature sets
3) Train the normal data using the cluster mechanism
4) Apply clustering algorithm to test the data
5) Post process alarms to produce intrusion reports

A. Construction of normal dataset

The data obtained from the audit data sources mostly contains local routing information, data and control information from MAC, and routing layers information along with other traffic statistics. The training of data may entail modeling the allotment of a given set of training points or characteristic network traffic samples. Few assumptions have to be made so that the traced traffic from the network contains no attack traffic [30]:

- The normal traffic occurs more frequently than the attack traffic i.e the normal traffic immensely outnumbers the number of anomalies. This is used to differentiate between the normal and attack traffic.
- The attack traffic samples are statistically different from the normal connections.

Since, two assumptions have been used; the attacks will appear as outliers in the feature space resulting in detection of the attacks by analyzing and identifying anomalies in the data set.

B. Feature construction

For feature construction, an unsupervised method is used to construct the feature set. Clustering algorithm is used to construct

features from the audit data. The feature set is created by using the audit data and most common feature set are selected as essential feature set which has weight not smaller than the minimum threshold. A set of considerable features should be obtained from the incoming traffic that differentiates the normal data from the intrusive data. Few and semantic information is captured which results in better detection performance and saves computation time. While feature construction, traffic related features as well as non-traffic related features are collected which represents routing conditions. Some of the features are used for detecting DoS attacks and attacks that manipulate routing protocol. The number of data packets received is used to detect unusual level of data traffic which may indicate a DoS attack based on a data traffic flood.

C. Training normal data using cluster mechanism

Cluster here is defined as a collection of data objects that are similar to one another within the same cluster and are dissimilar to the objects in other clusters [31]. In data mining, Clustering is a dynamic field of research with a large numbers of clustering algorithms developed. Outlier analysis tries to identify which data objects do not comply with the general behavior or model of the data and are inconsistent with the remaining set of data [31].

Outlier detection and analysis can also be referred as outlier mining.

The fixed−width clustering algorithm has been implemented as an approach to anomaly detection. It calculates how many points near each point in the feature space. In fixed width clustering technique, set of clusters are formed in which each clusters has fixed radius w also know as cluster width in the feature space [32]. The cluster width w is chosen as the maximum threshold radius of a cluster. The fixed width clustering algorithm that has been used in anomaly detection system is given in section D.

D. Fixed width algorithm

$S_T = \{s_i , i = 1,2\cdots\cdots N_T \}$

Where S_T is the training sample set and $s_i = <x_1,\cdots\cdots, x_d >$

Initial set of clusters $\Psi := \{\}$, the number of clusters $C := 0$

Normalizing S_T,

For each training sample $s_i \in S_T$

If $C=0$ **then**

Make new cluster ψ_1 with centroid ψ_1^* from s_i

$\psi_1 := \{s_1\}$, $\psi_1^* := s_i$, $\Psi := \{\psi_1\}$, $C = C+1$

Else

Find the nearest cluster ψ_n to s_i

$n := \text{argmin}_k \{\text{Distance } (s_i,\psi_1^*)\}$, where $k=1\cdots\cdots C$

If distance to nearest cluster Distance (s_i, ψ_l^*) < w then

Add s_i to cluster ψ_n and update cluster centroid ψ_n^*

$\psi_n := \{s_i\} \cup \psi_n$

Else

a new cluster is created as ψ_{C+1} with centroid ψ_{C+1}^* from s_i

$\psi_{C+1} := \{ s_i \}$,

$\psi_{C+1}^* := s_i$,

$\Psi := \{\psi_{C+1}\} \cup \Psi$,

$C := C+1$

For every cluster ψ_k,

Find the outermost point s_{max} in cluster ψ_k

$s_{max} := \text{argmin}_i \{\text{Distance } (s_i, \psi_k^*)\}$,

where $s_i \in \psi_k$ and $i = 1 \cdots\cdots\cdots N_T$

Set width w_k of cluster ψ_k ;

$w_k :=$ Distance (s_{max}, ψ_k^*)

Cluster Labeling:

If $|\psi_k|/N_T <$ classification threshold τ then

Label ψ_k as anomalous

Else

Label ψ_k as normal

E. Explanation of the algorithm

A set of network traffic sample S_T are obtained from the audit data for training purpose. Each sample s_i in the training set is represented by a *d*−dimensional vector of attributes. In the beginning, the set of clusters as well as the number of clusters are null.

Since, there is significant variation in each attribute. While calculating the distance between points, normalization is done before mapping into the feature space to ensure that all features have the same outcome. It is obtained by normalizing each continuous attribute in terms of the number of standard deviations from the mean. The first point of the data forms the centre of the new cluster. A new cluster ψ_1 is formed having centroid ψ_1^* from sample s_i. For every succeeding point, the distance of each traffic sample s_i to the centroid of each cluster ψ_1^* is measured that has been generated by the cluster set Ψ. If the distance to the nearest cluster ψ_n is within *w* of cluster center, then the point is assigned to the cluster, and the centroid of the closest cluster is updated. The total number of points in the cluster is incremented. Else, the new point forms the centroid of a new cluster. Euclidean distance as well as argmin is used because it is more convenient to have items which minimizes the functions as a result the computational load is

decreased. Moreover, the traffic samples are not stored and only one pass is required through the traffic samples. In the final stage of training, labeling of cluster is done based on the initial assumptions like ratio of the normal traffic is very small than attack traffic and the anomalous data points are statistically different to normal data points. If the cluster contains less than a threshold τ % of the total set of points then it is considered as anomalous. Otherwise, the clusters are labeled as normal. Besides, the points in the dense regions will be higher than the threshold, only the points that are outliers are considered.

F. Testing phase

The testing phase takes place by comparing each new traffic samples with the cluster set Ψ to determine the anonymity. The distance between a new traffic sample point s_i and each cluster centroid ψ_l^* is calculated. If the distance from the test point s to the centroid of its nearest cluster is less than cluster width parameter w, then the traffic sample shares the label as either normal or anomalous of its nearest cluster. If the distance from s to the nearest cluster is greater than w, then s lies in less dense region of the feature space, and is labeled as anomalous.

Ⅵ. Attacks in different protocol layers

Ad-hoc networks are more easily attacked than a wired network due to their underlying architecture. The attacks prevailing on ad-hoc routing protocols can be broadly classified into passive and active attacks.

A Passive Attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Passive attacks basically involve obtaining vital routing information by sniffing about the network. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated. Even if it is not possible to identify the exact location of a node, one may be able to discover information about the network topology, using these attacks.

On the other hand, an active attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The goal is basically to attract all packets to the attacker for analysis or to disable the network. Such attacks can be detected and the nodes can be identified.

The main interest is to detect different types of active attacks. It is difficult to identify intrusions in the networks as nodes may fail to provide services due to genuine reasons such as network

congestion, link failure or topology changes, thus causing high false positives. DoS attacks could be launched at multiple layers of the protocol suite [33]. In DoS attack, the attacker weakens the resources of the network and causes it to function improperly. At the physical layer, jamming and tampering attacks occurs. In case of jamming attack, the nodes radio frequencies are interfered and tampering refers to the physical altering or even damaging of the nodes [34].

At the link layer, the attacker can generate collisions and also exhaustion may be caused from protocols that attempts re-transmissions repeatedly even when triggered by an unusual and suspicious collision. By detecting abnormal behavior at different layers and using information across layers, malicious nodes can be detected with increasing accuracy. An example of link layer attack is a collision attack in which an adversary node can induce a collision in the wireless channel by transmitting when another node in its range is already in transmission. The purpose of this attack is to either prevent access to a certain node or to exhaust the transmitting node's resources by continuous re-transmissions.

A packet drop attack is a network layer attack in which the adversary node can randomly drop the control or data packets. This results in DoS attack at the destination node, hence affecting the availability of the node.

Misdirection attack is a routing protocol DoS attack which occurs when the adversary node forwards the data packet to the wrong destination node also the adversary node can deny the availability of an existing route to the destination by sending false RERR messages.

In Sink hole attacks, artificial routes are generated that results other nodes to request routes. It sends a RREQ message for a route to the receiving node regardless of whether a path already exists. This is immediately followed by sending of a RREP message, which contains the maximum Destination Sequence Number and minimum hop count. Neighboring nodes that receive the initial route request will reply to the compromised node if a route to the destination node exists in their routing table, or else will forward the request message.

A UDP flood attack is a kind of DoS attack which is a sessionless and connectionless computer network protocol using UDP protocol. In UDP flooding attack, DoS service is initiated by sending a large number of forged UDP packets to random diagnostic ports on remote target hosts. And the host will check the application listening at that port and replying with an ICMP destination unreachable packet. Thus, the CPU time, memory and Bandwidth required to process these packets may cause the target to become unavailable for the legitimate nodes.

Some of the different types of attacks in wireless ad-hoc network is given in table below [35].

Table 6.1 Attacks in wireless ad-hoc networks

Attacks	Initiator	Intention	Cause/ Vulnerability	Impact
Sybil attack	Malicious node	Masquerade	Autonomous behavior node	Forge multiple identities to hamper on data integrity and illegal access or information
Wormhole	Outside Attacker	Denial of Service (DoS)	Lack of centralized authority	Transmit information between two nodes secretly. Trigger route oscillation
Rushing Attack	Malicious Nodes	Eavesdropping	Ad-hoc routing	Observe traffic to get the information about source to destination path
Network Partition Attack	Outside Attacker	Denial of Service (DoS)	Lack of centralized authority	Nodes can't communicate each other through path exit between them
Sleep Deprivation	Malicious node	Denial of Service (DoS)	Low Battery Power	Can not perform further operation
Man-in-the middle attack	Malicious node	active eavesdropping	impersonate	An attacker sits between the sender and the receiver and sniffs any information being sent between two ends

Ⅶ. Performance Evaluation

A. Simulation Setup

Simulators are considered as the main tool in MANET for testing IDS. Simulators help researchers to study the performance and the reliability of their proposed IDS without using real mobile nodes. It will give researchers an idea on how their IDS will work in reality and under different circumstances. For this reason and to achieve better results, researchers must know the requirements that make simulations more trustworthy.

The simulation is done in OPNET simulator in windows XP machine [36]. The experimental set up consists of 21 similar wireless mobile nodes stations. All the nodes use AODV as a routing protocol within the area of 600m x 600m campus network. AODV protocol is a suitable approach for mobile networks due to low message overhead. The simulation is run for 320 seconds. The simulation statistics is shown in table 7.1. Custom applications with a streaming multimedia of packet size 1024 have been used which starts at around 20 sec. Here, UDP traffic has been used as an underlying transport protocols. During simulation UDP data traffic is

sent in bytes/sec by the source node to the destination node as well as the attack traffic has been implemented to disrupt the normal data traffic. UDP flooding attack along with the normal traffics are used in this scenario. Mobility configuration has been implemented for defining random way point and random direction mobility to the mobile nodes. The mobility causes the network topology to be highly dynamic as a result the detectors should have upto date evidence to detect attacks with low false positive and negative rates. These settings are typical ad-hoc settings with adequate mobility and data load overhead; and are used in the experiments. One running trace of normal data has been used as training set. For evaluation purposes, several other traces with only normal data and few traces composed with different types of attacks have been used. The existing node model is modified at its IP layer and MAC layer for capturing the incoming and outgoing traffics for detecting intrusive activities as the IDS checks the payload of the traffics [37]. The traffics are captured from IP and MAC layer and filters out UDP packets and send them to association model. The packet format and contents are checked by de-capsulating the payload and required UDP segments and port number are extracted from it.

Table 7.1 Simulation parameters

Statistics	Values
Scenario size	600mX600m
802.11b data rate	11 Mbps
Transmission Range	<250 meter
Power of each node	0.005 W
Simulation Time	320 seconds
No. of mobile nodes	21
Mobility	Random waypoint, random direction mobility

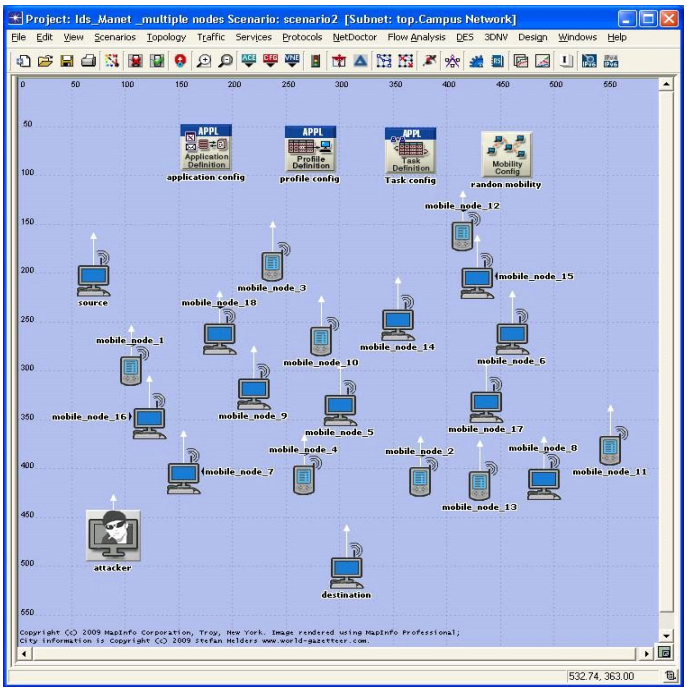

Figure 7.1 Simulation scenario

In the association model, the common control and data packets

from MAC and network layer are combined into one category as either routing control packets or routing data packets using association rules. The packets are then sent to the IDS module for evaluating and verifying the Intrusion Detection. The IDS module consists of fixed width algorithms for detecting anomalous behavior. The normal traffic behavior is recorded as a profile in normal profile. When packets arrive in this module, a stream of interrupts is issued and the packet is processed for intrusion detection.

B. Evaluation of results

Several evaluation methods have been proposed but there is no globally acceptable standard or metrics for evaluating an intrusion detection system [29]. AODV routing protocol is used in 21 mobile nodes and random mobility is implemented using mobility configuration. For evaluation purpose; source, destination, and attacker nodes are considered and other nodes assists in routing of the packets and communicate with each other nodes. During the training phase, the attacker node is disabled so that the normal traffic can be trained without any interference.

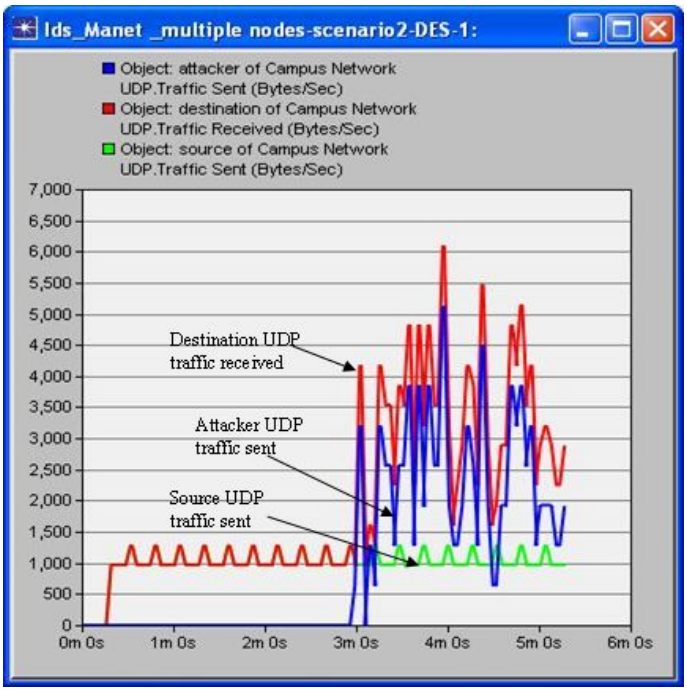

Figure 7.2 UDP traffic analysis in destination node

Figure 7.2 shows the streaming multimedia UDP data traffic sent by the source to the destination node along with the anomalous traffic. The source node sends the data traffic at around 20 seconds which is almost a consistent UDP data traffic indicated by green color. The attacker starts to send the custom anomalous unidirectional traffic to the same destination node at around 3 minutes. This anomalous traffic consists of high request count and tries to flood the normal traffic at the destination node. The destination node receives the normal multimedia traffic from 20 seconds but at around 3 minutes, it receives abnormal data traffic till the end of

the simulation. These data traffic are captured and collected by the association module and then sent to IDS specification module where the data traffics are compared with the normal behavior of the normal profile. If the traffic samples at the destination does not match with the normal traffic generated by the fixed width algorithm and lies in the sparse region then an irregularity is detected. If any deviation is found from the normal behavior then an anomaly is observed and an alarm is generated if the anomaly is of intrusive behavior. In this case, an anomaly is detected and IDS treats this anomalous activity as an intrusive activity.

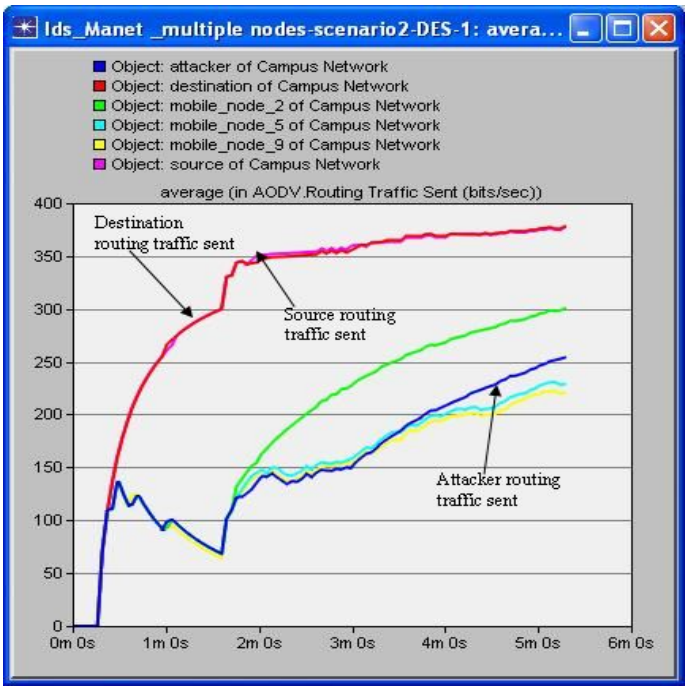

Figure 7.3 Time-average in AODV routing traffic sent

Figure 7.3 shows the time-average in AODV routing traffic sent in bits/sec at source, attacker, destination, and other mobile nodes. The source, destination and other intermediate nodes are in random way point mobility as assigned by the mobility configuration module. The transmission of data starts at 20 seconds. The time-average AODV routing traffic sent of source and destination is higher than other nodes because of continuous RREQ, RREP, and Hello messages between the two nodes while transferring the UDP traffic. The sink hole attacks cause artificial routes resulting other nodes to request route. A route request message is sent to the receiving node despite of the already existed path. So, there is increase in routing

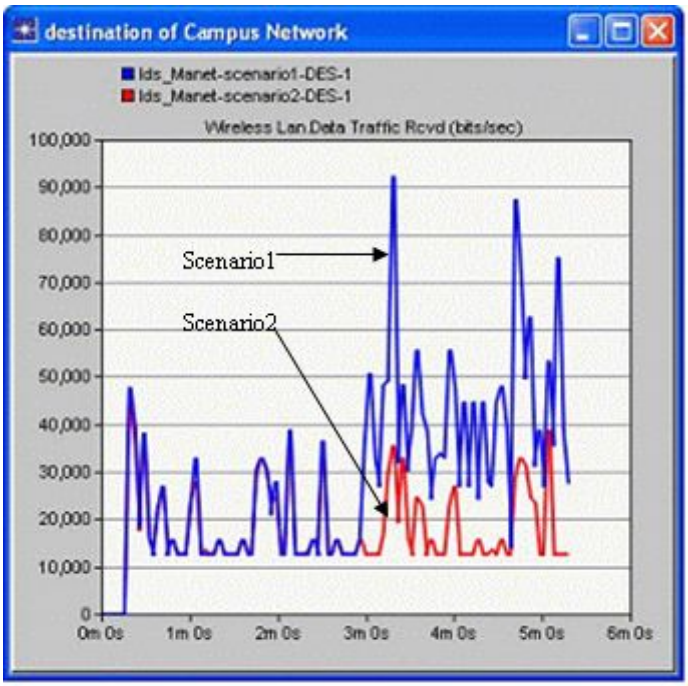

Figure 7.4 Wireless LAN data traffic received (bits/sec)

traffic in destination of campus node. Also, the attacker node starts to send anomalous traffic to the destination node at around 3 minutes, so there is sudden raise in the routing traffic as it is sending RREQ and RREP messages.

The simulation is run in two scenarios, one with attacker node and other without the attacker node. In the figure 7.4, during the testing process, the abnormal behavior can be seen in the wireless data traffic received after 3 minutes interval time. The red color shows the data traffic without the attacker node while the blue one is in the presence of the attacker node. During the training phase i.e in the absence of the attacker nodes, the normal traffic are recorded in the normal profile of the anomaly detection engine using fixed width clustering algorithm. Deviation between the normal and abnormal traffic in the destination node can be seen in figure 7.4. In the testing phase, these abnormal traffics are collected and are compared in the anomaly detection engine which employ fixed width clustering algorithm. It can distinguish the abnormal activities in the sparse region and the abnormal traffic is regarded as malicious behavior. The wireless LAN control and data traffic in bits/sec have been captured which are shown in figure 7.5 and figure 7.6. These

feature sets of control and data frames from MAC frames are combined into one category. All the control packets are combined as routing control packets and IP data packets as routing data packets.

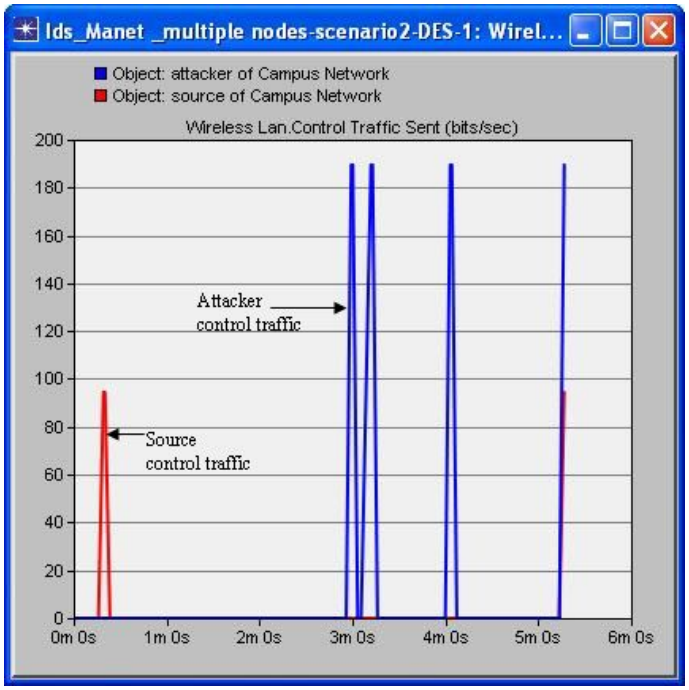

Figure 7.5 Wireless LAN Control traffic (bits/sec)

As a result, the payload in the MAC data frames are foreshortened in the association module. The captured Control and data traffic of the attacker and the source are different from each other. The normal traffic occurs more frequently than the attacker traffic as well as the nature of the attacker traffic is statistically different. So, the anomaly technique can distinguish the normal behavior from the anomaly behavior.

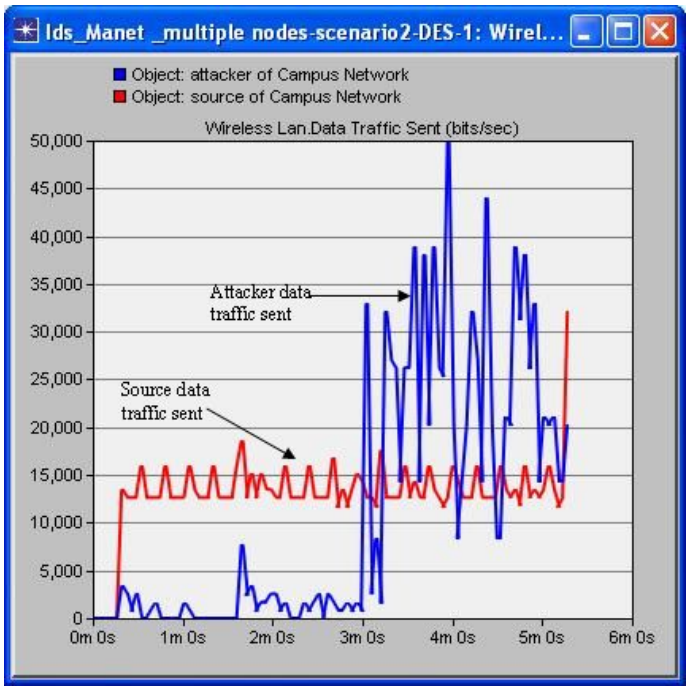

Figure 7.6. Wireless LAN data traffic (bits/sec)

While analyzing the load on different nodes in the scenario, it is found that the load of the attacker node is higher than any other nodes as shown in figure 7.7. It is due to the fact that the attacker node is sending UDP flooding attack towards the destination node. A large number of forged UDP packets are sent to the destination node. Also, the bandwidth and CPU time required for these packets cause the destination node become inaccessible for the legitimate nodes. Hence, there is a high LAN load in the attacker node.

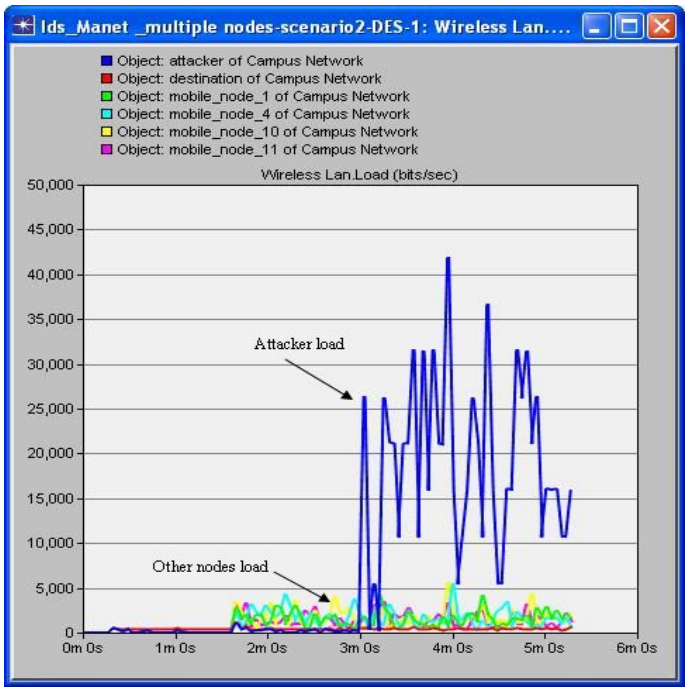

Figure 7.7 Wireless LAN load (bits/sec) on random nodes

Table 7.2 Comparison with other intrusion detection system

Reference	IDS Method	Input	Output	Detection Methodology	Cross Layers	Advantage	Disadvantage
Y.Liu	Collaborative IDS	Network packets activities with in one hop	Intrusive Alarm	Anomaly	Routing and MAC	Low energy consumption and Bayesian network is used.	Detection within one hop perimeter only
C.J. John Felix	Local and collaborative IDS	Network packets; topology statistics	Intrusive Alarm	Anomaly	Routing and MAC	Data reduction technique is used	Complexity of the system due to non linear pattern recognition
J.S. Baras	Local IDS	Data Traffic	Intrusive Alarm and Global response	Finite State Machine	Routing, MAC and Physical	Global Response	Message Overhead & battery constrain
Proposed Architecture	Local and collaborative IDS	Audit data collected on Local nodes	Intrusive Alarm	Anomaly	Routing and MAC	Association rule is used to comply with anomaly profiling &low energy consumption	Many protocols are not coordinated. Not yet implemented.

The proposed architecture is compared with other different cross layer Intrusion Detection Systems as shown in table 7.2. Most of the IDS worked on routing and MAC layers but J.S Baras worked on routing, MAC and Physical layers so there are some disadvantages like message overhead and battery constrains. Most of the IDS focused on data reduction and low energy consumption and there are disadvantages like message overhead, system complexity and battery constrain. In the proposed architecture, a single detection module is presented that collects and analyzed so the data overhead and energy consumption are reduced.

Ⅷ. Conclusions and Future Work

Hence, a better intrusion detection mechanism based on anomaly detection is presented in this thesis utilizing cluster data mining technique. The proposed architecture has been implemented with fixed width clustering algorithm and done the simulation in OPNET and analyzed the results. The proposed cross layer based intrusion detection architecture is designed to detect different DoS attacks at different layers of the protocol stack. The cross layer detection confirms the misbehavior caused by the malicious nodes, thus reducing the false positive rates and enhanced the accuracy in detecting attacks. All the anomalous behaviors are trained and tested in the anomaly detection module. All the UDP traffics are analyzed and evaluated and anomaly is detected. Since, the data are collected from single data collection module, the data analysis overhead is reduced. The load on different nodes are captured and found that load on the attacker node is higher than other nodes.

Future work will involve research into more robust and intelligent IDS system which includes further analysis of the simulation results with richer semantic information.

References

[1] Yi-an Huang, "Anomaly Detection for Wireless Ad-Hoc Routing Protocols," Master Thesis, North Carolina State University, June, 2001.

[2] Y. Li and J. Wei, "Guidelines on Selecting Intrusion Detection Methods in MANET," in the Proceedings of the Information Systems Education Conference, vol 21 pp.1542-7382, 2004.

[3] S. Jacobs, S. Glass, T. Hiller, and C. Perkins. "Mobile IP authentication, authorization, and accounting requirements," Request for Comments 2977, Internet Engineering Task Force, Oct. 2000.

[4] K. Sanzgiri, B. Dahill, B.N. Levine, E.B. Royer, and C. Shields, "A Secure Routing Protocol for Ad-hoc Networks," in the Proceedings of International Conference on Network Protocols (ICNP), 2002.

[5] Y.C. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," in the Proceedings of MobiCom, 2002.

[6] R. Shrestha, J.Y Sung, S.D. Lee, P.S. Yun, D.Y. Choi, and S.J. Han, "A Secure Intrusion Detection System with Authentication in Mobile Ad hoc Network," in the Proceedings of Pacific-Asia Conference on Circuits, Communications and Systems, pp.759-762, May 2009.

[7] Y. Zhang, W. Lee, and Y.-A. Huang. "Intrusion Detection Techniques for Mobile Wireless Networks," ACM Journal Wireless Networks. pp. 545-556, 2003.

[8] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in

Wireless Ad-Hoc Networks," in IEEE Wireless Communications, pp.48-60, Feb. 2004.

[9] Y. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in the Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS) Providence, RI, pp. 478-487, Sep. 2002.

[10] C. Loo, M. Ng, C. Leckie, and M. Palaniswami, "Intrusion Detection for Routing attacks in Sensor Networks," in International Journal of Distributed Sensor Networks, pp. 313-332, Dec. 2006.

[11] C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for AODV," in the Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM Press, pp. 125-134, 2003.

[12] E. Eskin, A. Arnold, M. Prerau, L. Portnoy, and S. Stolfo, "A geometric framework for unsupervised anomaly detection: detecting intrusions in unlabeled data," in Applications of Data Mining in Computer Security, Kluwe, 2002.

[13] C.Y.H. Tseng, "Distributed Intrusion Detection Models for Mobile Ad Hoc Networks," PhD Thesis, University of California Davis, CA, USA, 2006.

[14] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad-hoc networks," IEEE Wireless Communications, Vol. 11, pp. 48-60 Feb. 2004.

[15] Y. Xiao, X. Shen, and D.Z. Du (Eds.), "A Survey on Intrusion Detection in Mobile Ad-hoc Networks," in Wireless/Mobile Network

Security, pp. 170-196, 2006.

[16] http://www.acm.org/crossroads/xrds2-4/intrus.htm

[17] C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A Specification-based Intrusion Detection System for AODV," in the Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 125 -134, 2003.

[18] S. Axelsson, "Intrusion Detection Systems: A Taxonomy and Survey," in Tech. report no. 99-15, Dept. of Comp. Eng., Chalmers University of Technology, Sweden, Mar. 2003.

[19] B. Mukherjee. L.T Heberlein, and K. N. Levitt, "Network intrusion detection," in IEEE Network, vol.8, no.3, pp.26-41, Jun. 1994.

[20] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in the Proceedings of MobileComputing and Networking, pp. 275-283, 2000.

[21] A. Goldsmith and S. B. Wicker, "Design challenges for energy-constrained ad hoc wireless networks," in IEEE Wireless Communications, pp. 9(4):8-27, Aug. 2002.

[22] C. J. John Felix, A. Das, B.C. Seet, and B.S. Lee, "Cross Layer versus Single Layer Approaches for Intrusion Detection in MANET," in IEEE International Conference on Networks, Adelaide, pp. 194-199, Nov. 2007.

[23] J. S. Baras and S. Radosavac, "Attacks and Defenses Utilizing Cross-Layer Interactions in MANET," in workshop on Cross-Layer Issues in the Design of Tactical Mobile Ad Hoc Wireless Networks: Integration of Communication and Networking Functions to Support

Optimal Information Management, Washington, DC, Jun. 2004.

[24] L. Yu, L. Yang, and M. Hong, "Short Paper: A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks," in the Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, Athens, Greece, pp. 418-420, Sept. 2005.

[25] C. J. John Felix, A. Das, B.C. Seet, and B.S. Lee, "CRADS: Integrated Cross Layer Approach for Detecting Routing Attacks in MANETs," in IEEE Wireless Communications and Networking Conference (WCNC), Las Vegas, CA, USA, pp. 1525-1530, Mar. 2008.

[26] R. Shrikant, "Fast algorithm for mining association rule and sequential pattern," PhD Thesis , University of Wisconsin, Madison, 1996.

[27] J.H Song, and C.X Ma, "Anomaly Detection Based on Data-Mining for Routing Attacks in Wireless Sensor Networks," in Second International Conference on Communications and Networking in China, CHINACOM, pp. 296-300, Aug. 2007.

[28] T.F. Lunt and R. Jagannathan, "A prototype real-time intrusion-detection expert system," in the Proceedings of the IEEE Symposium on Security and Privacy, pp. 59-66, Apr. 1988.

[29] A. Patcha and J.M. Park, "An overview of anomaly detection techniques: existing solutions and latest technological trends," in Elsevier Computer Networks, Vol. 51, Issue 12, pp. 3448-3470, 2007.

[30] L. Portnoy, E. Eskin, and S. Stolfo, "Intrusion detection with

unlabeled data using clustering," in the Proceedings of the Workshop on Data Mining for Security Applications, Nov. 2001

[31] J. Han and M. Kamber, "Data Mining: Concepts and Techniques," Morgan Kaufmann Publisher 2000.

[32] C. Loo, M. Ng, C. Leckie, and M. Palaniswami, "Intrusion Detection for Routing attacks in Sensor Networks," in International Journal of Distributed Sensor Networks, pp. 313-332, Dec. 2006.

[33] G. Thamilarasu, "A cross-layer based intrusion detection approach for wireless ad-hoc networks," in IEEE International Conference on Mobile Ad hoc and Sensor Systems, Washington, DC, pp. 861-868, Nov. 2005.

[34] R. Shrestha, S.D. Lee, D.Y. Choi, and S.J. Han, "Detecting Jamming Attacks in MANET," in The Journal of the Korea Institute of Maritime Information & Communication Sciences, Vol. 13, No. 3, pp. 482-488, Mar. 2009.

[35] P. B. Chanda and A. A. Khan, "Intrusion Detection System (IDS) Framework for Wireless Ad-Hoc network," Masters Thesis, Stockholm University and Royal Institute of Technology, May 2007.

[36] http://www.opnet.com

[37] T. Phit and K. Abe, "Protocol Specification-based Intrusion Detection System for VoIP," Technical Report of IEICE, vol. 107, pp. 5-10, Feb. 2008.

Acknowledgement

This thesis is the outcome of two years of research work that has been carried out since I came to Chosun University. By that time, I have worked with a number of people whose contribution to the research and making of the thesis, deserve special mention. It is a pleasure to convey my appreciation to them all in my humble acknowledgement.

First and foremost, I would like to express my deep and sincere gratitude to my supervisor, Prof. Seung-Jo Han. His guidance, advice, and continuous support have played an infinite role throughout my entire course period. I gratefully acknowledge Prof. Dong-You Choi for his supervision, advice and guidance in my research work. My sincere thanks goes to Prof. Jong-an Park, Prof. Jae-Young Pyun, and Prof. Goo-Rak Kwon for their detailed review and excellent advice to overcome my doubts during the preparation of this thesis.

I express my special acknowledge to Dr. Binod Vaidya for providing me an opportunity to study in Chosun University and very much thankful for his supervision, advice, and guidance from the very early stage of this research as well as giving me extraordinary experiences throughout the work and providing me relentless encouragement and support in various ways.

Collective and individual acknowledgements and thanks should be given to all my colleagues and lab mates in Computer Network and Internet Security (CNIS) lab whose presence somehow continually refreshed, helpful and memorable. Also, special thanks to Dr. Sang-Duck Lee, Kyong-Heon Han, Kyu-Jin Park, Jeong-Yeop Seung, Anish Shrestha, Roja Kiran Basukala, and other lab members.

I am immensely indebted to my mother Ahilya Shrestha, my family, and friends for their distant care, love and support throughout my studies. I am very grateful to all my relatives and siblings for their concern.

Also, I would like to thank everybody who gave me support to write my thesis successfully directly or indirectly and expressing my apology for not mentioning the name personally one by one.

Finally, I would like to show my gratitude to the Government of the Republic of Korea, Institute of Information Technology Advancements (IITA) for awarding me Information Technology Scholarship which financially supported me to study and research. Also, I wish to thank Chosun University for waiving tuition fee and providing academic support for pursuing my masters degree.

저작물 이용 허락서

학 과	정보통신공학과	학 번	20087734	과 정	석사
성 명	한글 라케쉬 쉬레스타 영문 Rakesh Shrestha				
주 소	광주광역시 동구 서석동 조선대학교 전자정보공과대학 817호				
연락처	E-mail : rakez_shre@yahoo.com				
논문 제목	한글 크로스 층을 통합하고 있는 모마일 에드-혹 네트워크의 침입 탐지 시스템				
	영문 Intrusion Detection System in Mobile Ad-hoc Networks Incorporating Cross Layer				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건 아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함.
2. 위의 목적을 위하여 필요한 범위 내에서의 편집과 형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사 표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물 이용의 허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음.
7. 소속 대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의(○) 반대( )

2010년 2월 25일

저작자 : Rakesh Shrestha (인)

조선대학교 총장 귀하