Implementation of Mobile Intrusion Detection Controller [MIDC] for Affording Secure Service in MANET Environment

D.Jeyabharathi
Lecturer , Department of Computer Science and Engineering
Einstein College of Engineering, Tirunelveli,Tamil Nadu,India

D.Sasireka
Lecturer,Department of Information Technology
PSN College of Engineering and Technology,Tirunelveli,Tamil Nadu,India

D.Kesavaraja
Lecturer,Department of Computer Science and Engineering
Dr.Sivanthi Aditanar College of Engineering, Tiruchendur
Tamil Nadu,India

ABSTRACT
In this new millennium most of the transactions depend on wireless network. In this context highly secured transaction of information is the need of the hour. During the transaction there must not be any loss of information or there should be no intrusion to assure the secured data transmission. There are several approaches available for fixed network threats. But it is difficult to analyze the intrusion attacks in mobile networks due to its high mobile nature. In this present work we implemented a simulation tool to handle intrusion attacks in Mobile Ad Hoc Network (MANET). Using that we analyzed Route Disturbance, Node Isolation, Resource Consumption, Denial of Service (DoS) and Man in the Middle attacks. Using our approach it is easy to reduce throughput, easy to increase security, easy to avoid unauthorized intruders and also it is easy to avoid packet losses.

The implemented wireless intrusion detection system has been simulated using JAVA Platform. Our tool Mobile Intrusion Detection Controller (MIDC) is combined with the existing Ad Hoc On-demand Distant Vector (AODV) routing protocol. It is used to detect and magnify various attacks in a mobile network. These attacks have been simulated and performed using hacker software in java platform. It also includes an additional recovery phase to overcome threats and intruders.

Keywords
MANET, attacks, detection, node isolation, route disruption, resource consumption, ADODV, MIDC, DoS, Man in the Middle Attack..

1. INTRODUCTION
A Mobile AdHoc Network (MANET) is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end-system but also as a router to forward packets. Each MANET device is free to move independently, in any arbitrary direction, and thus each device will potentially change its link to other devices on a regular basis[1][2]. The primary challenge for building a MANET is, for each device we have to continuously maintain the information required to properly route the traffic.MANET does not require any fixed infrastructure such as base stations, therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously. Most existent protocols, applications and services for Mobile AdHoc Networks (MANETs) assume a cooperative and friendly network environment and do not accommodate security[3]. Therefore, the number of attacks in this environment is more and we aim to address the problem of attacks on mobile nodes. Here we presented a new method to detect and recover some attacks on mobile nodes[4].
Host centric methods usually analyze data collected from the host machine operating system's audit trails, system and application logs or audit data generated by kernel modules that intercept system calls to detect the attacks. Next, Network centric methods analyze data packets that travel over the actual mobile network[5]. These packets are examined and sometimes compared with experimental data to verify their uniqueness (malicious).

Another approach is Signature-based detection. In this misuse detection identifies attacks through attack pattern (i.e., signature) matching. Various data sources and types of pattern recognition techniques are used to separate attack signals from normal usage noise[6][7]. An attack signature is a known attack footprint abstraction. In other words, it is a descriptive material on known abnormal behavior. In general, signature detection designs have acceptable accuracy and they tend to produce fewer false positives (i.e., classifying an action as malicious when in fact it is not) than anomaly detection designs. The systems are easier to implement and simpler to configure, especially in large production networks[8]. However, signature detection is unable to detect novel attacks whose signatures are unknown. In addition, it requires updating signatures regularly due to the emergence of new variants of known attacks[9][10][11][12].
Anomaly detection, in contrast to signature detection, is able to detect novel attacks by recognizing any deviance from normal behaviors. Anomaly detection techniques can be subcategorized by the way of characterizing normal behaviors. They can be divided into two categories: profile-based detection and specification-based detection.

Profile-Based Detection
Profile-based detection is also known as behavior-based detection. Profile-based detection defines a profile of normal behavior and classifies any deviation of that profile as an anomaly[13]. The assumption of this type of detection is, attacks are events distinguishable from normal legitimate use of system resources. Although this type of anomaly detectors are able to

detect novel attacks, they are prune to high false positive rate due to the difficulty of clear segmentation between normal and abnormal activities and the use of insufficient or inadequate features to profile normal behaviors.

Specification-Based-Detection
Specification-based detection defines a set of constraints that describe the correct operation of a program or protocol and monitors the execution of the program with respect to the defined constraints. It has been show that specification-based techniques live up to their promise of detecting known as well as unknown attacks, while maintaining a very low rate of false positives. Since the increasing popularity of wireless networks to that of wired networks, security is being considered as a major threat in them. Wireless network exposes a risk that an unauthorized user can exploit and severely compromise the network. There can be different possible attacks in wireless network viz., active and passive attacks. So there is a need for secured system to analyze and detect attacks.

2. BACKGROUND

The most widely used protection system for Wired networks is the traditional intrusion detection systems. But the same intrusion detection systems face a lot of challenges when applied to wireless systems, which vary widely in the infrastructure and various other factors. The major factors that cause this inconvenience are lack of fixed infrastructure, mobility, vulnerability of wireless transmissions along with lack of clear separation between normal and abnormal behavior of the nodes present in the network. These features make it so difficult to use the Intrusion detection systems on a wireless network [14][15]. The wireless networks on the other hand are very easy to install in today's congested world in all scenario. But they have some disadvantages too. Since the access points are wireless links it produces a ad-hoc network exposed to various kinds of attacks like passive eavesdropping to active impersonation, message replay and message distortion. Since the nodes have no physical protection the possibility of them being compromised is very high. Hence in wireless networks the risk does not come from outside the networks but also from compromised nodes inside the network. Attacks like eavesdropping, Active attacks and various other forms of attacks make the network vulnerable and unsecure [16][17][18]. Hence wireless networks are much unsecure.

3. SYSTEM DESIGN

The design goal of this work is to identify various possible attacks in mobile network systems and to propose a method for detecting attacks in MANETs. The proposed work can be performed by combining our tool Mobile Intrusion Detection Controller (MIDC) with the existing Ad Hoc On-demand Distant Vector (AODV) routing protocol.

Recovery is the next logical step after an intrusion as been detected. As part of the recovery phase, the victim should be isolated. In this state, the victim is connected to neither the attacker nor the valid system. This ensures that the attacker does not have any influence on the victim. When a traffic flow has been identified as vulnerable to attacks, system instructs the access router to block the flow to prevent possible attacks to that flow. A detection system should have both types of capabilities.

The proposed work can be divided into three modules.

1.Packet Transfer

2.Intrusion Detection

3.Intrusion Recovery

3.1 Packet Transfer

This process is used to capture the packets in the mobile network either in normal and attack mode. It is the basic stage of capturing data using Jpcap in Java platform.

3.2 Intrusion Detection

This part is used to identify the possible intruder in the mobile environment which can be further sub-divided into normal mode and attack mode. Under normal mode there is no action of attack. Here packet transfer between the nodes takes place randomly without any intruder act over them. Under attack mode, the five different attacks (Route Disturbance, Node Isolation, Resource Consumption, Denial of Service (DoS) and Man in the Middle attacks) had been introduced to perform intruder attack over the system.

3.3 Intrusion Recovery

In the recovery process, the intruder which has been detected in the detection phase should be isolated from the network. The intruders have no action in the network environment since it has been isolated as the individual victim. Now the network environment is free from the action of intruder and thus results in the secure communication.

4. SYSTEM ARCHITECTURE

The overall description of Intrusion process is described using the following architecture. The Figure 1 shown below gives the conceptual model of the system.

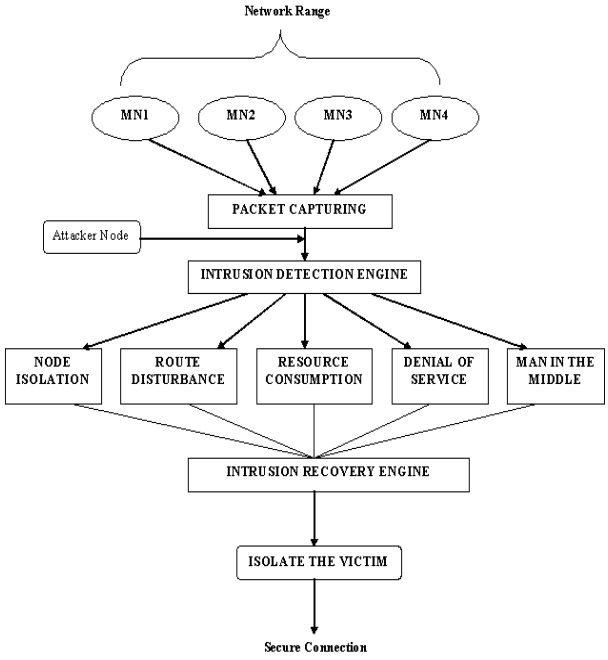

Figure 1: Conceptual Model

The overall system architecture has been shown in Figure. 2.

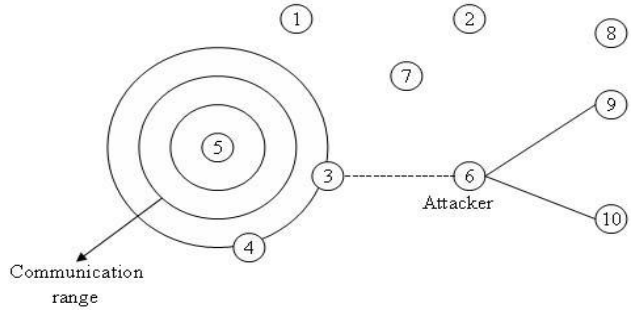

Figure 2: Overall System

This process is used to capture the packets in the mobile network either in normal and attack mode. It is the basic stage of capturing data using Jpcap in Java platform.

5. IMPLEMNETATION

The three modules are implemented using java platform.

5.1 Packets Transfer Under Normal Mode

30 different mobile nodes were simulated in the java environment. Each node sends and receives the packets randomly. Each packet size is of about 512 KB. The communication range between different nodes exists as predetermined. This mode is considered as normal mode, since each node while transferring data only there is a less number of chances that the packets drop in the intermediate. In normal mode also there is a packet loss but which is very small. This packet loss normally occurs in the wireless environment. Here it is considered there is no attacker. The packets which we sent from the source reaches destination but only minor loss. These can be verified by checking sent amount of packets with that of received packets and by plotting the graph using which gives details about network information, i.e., the number of packets sent and number of packets received between different nodes. From graphs also these details become clear.

5.2 Packets Transfer Under Attack Mode

This mode considered as attack mode since there is more chances of the packets drop. The packets which we sent from the source reaches destination with major loss. These can be verified by checking sent amount of packets with that of received packets and by plotting the graph which gives details about network information, i.e., the number of packets sent, number of packets received and number of dropped packets between different nodes.

5.3 Intrusion Detection

In this method we introduced attacks in the mobile environment to check how an intruder acts as an attacker and allowing the packets to drop. The attack which we introduced are generally the inside attackers.

The five different attacks which are introduced as follows:

- Route Disruption
- Node Isolation
- Resource Consumption
- Denial of Service
- Man in the Middle

5.4 Intrusion Recovery

Recovery from attacks can be explained by considering 30 different wireless nodes in the network environment. Each different node sends and receives the packets randomly. Each packet size is of about 512 KB. The communication range between different nodes exists as predetermined. In this module, the node which has been detected as the intruder should be isolated from the mobile environment. Also the route which has detected prone to attack should be diverted from the normal path. Hence further possible attacks can easily be prevented.

6. EXPERIMENTAL RESULT

The following used to find result analysis of MIDC.

6.1 Entropy Calculation

A measure used from MANET and many others used in decision tree construction is that of Entropy. It has been shown that entropy is related to information, in the sense that the higher the entropy, or uncertainty, of some data, then the more information is required in order to completely describe that data.

If S denotes the collection of Nodes. If D denotes the deceptive and ND denotes Non-Deceptive.

$$Entropy(S) = P(Positive)\log_2 P(Positive)$$
$$(Negative)\log_2 P(Negative)$$

Where,
P(positive): proportion of positive examples in S
P(negative): proportion of negative examples in S

6.2 Gain Calculation

$$GAIN(S,A)=Entropy(S)-\sum_{v=1}^{n}(|S_v|/|S|)*Entropy(S_v)$$

Where, , v is a value of A.
$|S_v|$ is the subset of instances of S A takes the value v,
|S| is the number of instances.
All the attributes the information gain is calculated. The attribute, which has the highest information gain, becomes the root node of the tree.

They are listed in the table as follows:

ATTACKS	**PARAMETERS**
SYN Floods	ACK , SYN
Scan For Vulnerable Ports	Port Number
Scanning Attack	Protocol Number
Buffer Overflow	Buffer Size

IP Spoofing	Source IP address
Tear Drop	Offset

Table 1: ATTACKS AND PARAMETERS

6.3 Alarm Generation

In our simulation, If an intrusion occurs, an alarm is produced a message box is displayed.

We have tested the internal behavior of the system and the logic manually.

6.4 Pie- Chart for Percentage of Intrusion

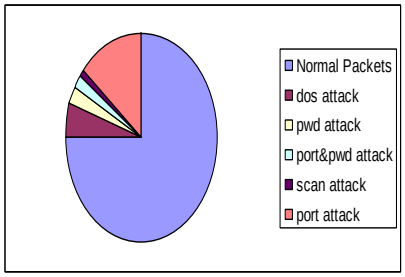

Figure 3: Pie-Chart for Intrusion

Figure 3 describes the details about the percentage of Intrusion.

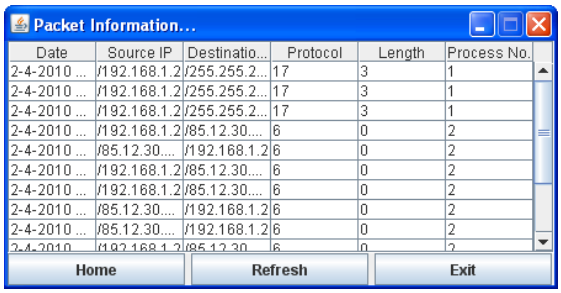

Figure 4 packet capture using java

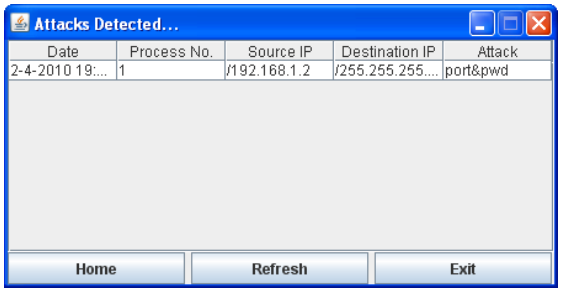

Figure 5 Output Snap Shot detected attacks

Figure 4 & 5 describes the details about the MIDC and its Alarm Generation Result .

7. PERFORMANCE ANALYSIS

The simulation experiments are conducted in the Java platform. A network in 1000×1000 m square area was considered with 30 mobile nodes. For each traffic flow, a source/destination pair is randomly selected from the node set and the transmission rate is 2 packets per second with a packet size of 512 bytes.

A fixed 64-packet send buffer is maintained at each node for packets waiting for available routes. Some details regarding simulation environment is given in the following tables.

Sl No	Under Normal	Under Attack
1	477	32
2	533	44
3	622	45
4	721	59
5	433	61
6	422	56
7	543	37
8	621	65
9	544	34
10	435	45

Table 2: Packets Drop (Analysis)

Using our approach it is predicted in a tabulated manner as shown in Table 3.

slno	Under Normal	Under Attack
1	433	4
2	531	7
3	811	5
4	721	9
5	266	21
6	438	16
7	434	7
8	622	5
9	541	3
10	723	4

Table 3: Packets Drop Using Our System

8. CONCLUSION

Our proposed approach is used for detecting and magnifying various attacks in a mobile network. These attacks have been performed using hacker software in java network platform. It is also used for finding packet loss, diverting the route and reducing resource consumption. It also includes an additional recovery phase to overcome threats and intruders.

In future, we have ideas for correcting the victim and use it appropriately in the same network and also to design a proper monitoring system in built with it.

9. .REFERENCES

[1] Anand, R., Nachiketh R. Potlapally, 2006. A study of the energy consumption characteristics of Cryptographic Algorithms and Security Protocols. IEEE Trans. Mob. Comput., 5(2), pp: 128-143. doi: 10.1109/TMC.2006.16

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

[3] Y. Zhang, W. Lee, and Y. Huang. Intrusion detection techniques for mobile wireless networks. ACM/Kluwer Mobile Networks and Applications (MONET), 2002.

[4] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R.Limprasittiporn, J. Rowe, and K. Levitt. A specificationbased intrusion detection system for AODV. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 125–134. ACM Press, 2003.

[5] Pirzada, Asad Amir, and McDonald, Chris. Establishing trust in pure ad-hoc networks. Proceedings of the 27th conference on Australasian Computer Science - Volume 26, pp 47-54, 2004

[6] Theodorakopoulos, George and Baras, John. Trust evaluation in ad-hoc networks. Proceedings of the 2004

[7] ACM workshop on Wireless security, pp. 1-10, 2004.

[8] Michiardi, P. and Molva, R., "Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks", Communication and Multimedia Security 2002 Conference.

[9] Albers, Patrick and Camp, Olivier. Security in Ad hoc Networks: a general Intrusion detection architecture enhancing trust based approaches. Proceedings of the First International Workshop on Wireless Information Systems 2002.

[10] Sun, Bo, Wu, Kui and Pooch, Udo. Alert aggregation in mobile ad hoc networks. Proceedings of the 2003 ACM workshop on Wireless security, pp.69 – 78, 2003.

[11] Puttini, R; Percher, JM; Me, L, Camp, O; de Sousa, R. A Modular Architecture for a Distributed IDS for Mobile Ad Hoc Networks. Lecture Notes on Computer Science vol.2669, Springer-Verlag, pp. 91-113, 2003.

[12] Ngai, Edith C. H., and Lyu, M. R.. Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks. 24th International Conference on Distributed Computing Systems Workshops, vol. 04, pp. 582-587, 2004.

[13] Parker, J., Undercoffer, J. L., Pinkston, J., and Joshi, A. On Intrusion Detection in Mobile Ad Hoc Networks. In 23rd IEEE International Performance Computing and Communications Conference – Workshop on Information Assurance. IEEE, April 2004.

[14] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (Mobicom '00), pp. 275- 283, 2000.

[15] Karygiannis, A. and Antonakakis, E. mLab: A Mobile Ad Hoc Network Test Bed. 1st Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing in conjunction with the IEEE International Conference in Pervasive Services 2005, July 14, 2005.

[16] V. Madhu Viswanatham and A.A. Chari: An Approach for Detecting Attacks in Mobile Adhoc Networks in Journal of Computer Science 4 (3): 245-251, 2008 ISSN 1549-3636 © 2008 Science Publications ww.scipub.org/fulltext/jcs/jcs 43245-251.pdf

[17] Sarat Sreepathi, Vamsi Venigalla, Akshay Lal :A Survey Paper on Security Issues Pertaining to Ad-Hoc Networks www4.ncsu.edu/~sssreepa/Adhoc-networks-Security-Survey.doc

[18] Arun Kumar Bayya ,Siddhartha Gupte,Yogesh Kumar Shukla and Anil Garikapati : Security in Ad-hoc Networks www.cs.uky.edu/~singhal/term-papers/Fourth-paper.doc