IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24, 2007. pp.360-365.

Multi-Layer Integrated Anomaly Intrusion Detection System for Mobile Adhoc Networks

S. Bose[1], S. Bharathimurugan[2] and A. Kannan[3]

Abstract: **Most intrusion detection systems for mobile ad hoc networks are focusing on either routing protocols or MAC layer traffic. This paper focuses on the design of a new anomaly detection system for each node of the network, which contains detection subsystem for MAC layer, routing layer and application layer. Audit data taken from MAC level/Network level/Application level from the traces in Glomosim and are preprocessed separately for each layer's detection subsystem. Feature data sets for each layer are selected from normal transactions. The Detection subsystem contains normal profiles obtained from the feature vectors of training data sets. In our work, we used Bayesian classification algorithm, Markov chain construction algorithm and association rule mining algorithm for anomaly detection in MAC layer, routing layer and application layer respectively for effective intrusion detection. Test data obtained from the network traffic is feed in to the detection subsystems. If there is any deviation from normal behavior, it is considered as abnormal or anomaly based on predefined thresholds. Intrusion results from detection subsystems of all the three layers are integrated at local integration module and the final result is sent to the global integration module. Intrusion results are received also from the neighbor nodes and are sent to the global integration module for making a final decision.**

I. INTRODUCTION

A mobile ad hoc network (MANET) is formed by a group of mobile wireless nodes without the assistance of fixed network infrastructure. The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The nature of mobility creates new vulnerabilities due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management points and yet many of the proven security measures turn out to be ineffective. Therefore, the traditional way of protecting wired/wireless networks with firewalls and encryption software is no longer sufficient. We need to develop new architecture and mechanisms to protect the wireless networks and mobile computing applications.

In our work, we proposed a new architecture that consists of three layers in wireless ad hoc networks namely MAC layer, routing layer, and application layer to find an effective anomaly detection model with less false positive rate in a distributed environment. There are three major steps involved in our work to find the intruders. First, we collect the intrusion results from each anomaly detection subsystem. Second, we obtain the anomaly results from the local subsystem model using each layer subsystem results and finally we integrate the local subsystem anomaly results and neighbor node's anomaly detection result and decide the final intrusion results. The main advantage of this multi-layer approach is the increase in detection rate due to the fact that the intruders who escaped from the detection system of one layer are caught in the other layer. This intrusion result has been sent to the host. Comparing with the existing works, our work is different in many ways. First, we use a cross layer approach to improve the detection rate. Second, we use intelligent agents and data mining algorithms for effective intrusion detection in local and global integration. Third, we use a majority-voting scheme to get the best results from data mining algorithms. The main focus of this paper is on experimental results rather than theoretical analysis. Hence, the mathematical models developed in our research work are not dealt with in this paper. However, from our mathematical analysis on the sample data sets and results, we found that 5% level of significances a good statistical measure for decision-making and hence the threshold has been fixed at 5% level. This intrusion result has been sent to the host. The rest of the paper is organized as follows. Section 2 explains the related works. Section 3 shows the proposed system architecture. Section 4 illustrates the experiments and its results for the proposed architecture. Finally, Section 5 concludes this paper with future research.

II. RELATED WORK

Intrusion detection means identifying any set of actions that attempt to compromise the integrity, confidentiality or

[1] Department of Computer Science and Engineering, Anna University, Chennai-600044, India.
Email: sbs@cs.annauniv.edu[1], bharathimurugans@yahoo.co.in[2], kannan@annauniv.edu[3]

1-4244-0997-7/07/$25.00 ©2007 IEEE

availability of resource [3]. There are three types of intrusion detection as follows

- Anomaly detection: Deviation from baseline profile of normal systems.
- Misuse detection: On the basis of knowledge of a model of intrusion process.
- Specification-based detection: Defines set of constraints (correct operation of a program or protocol).

In [4], it is given that that following procedure is utilized for anomaly detection:

- Select (or partition) audit data so that the normal dataset has low (conditional) entropy.
- Perform appropriate data transformation according to the entropy measures (e.g., constructing new features with high information gain).
- Compute the classifier using training data.
- Apply the classifier to test data.
- Post-process alarms to produce intrusion reports.

The vast difference between the fixed network where current intrusion detection research is taking place and the mobile ad-hoc network makes it very difficult to apply intrusion detection techniques developed for one environment to another. The most important difference is perhaps that the latter does not have a fixed infrastructure, and today's network-based IDSs, which rely on real-time traffic analysis, can no longer function well in the new environment. In [1], a mechanism for intrusion detection and response has been proposed.

Compared with wired networks where traffic monitoring is usually done at switches, routers and gateways, the mobile ad-hoc environment does not have such traffic concentration points where the IDS can collect audit data for the entire network. Therefore, at any one time, the only available audit trace will be limited to communication activities taking place within the radio range, and the intrusion detection algorithms must be made to work on this partial and localized information [2].

In summary, we must answer the following questions in developing a viable intrusion detection system for mobile ad-hoc networks:

- What is a good system architecture for building intrusion detection and response systems that fits the features of mobile ad-hoc networks?
- What are the appropriate audit data sources? How do we detect anomaly based on partial, local audit traces – if they are the only reliable audit source?
- What is a good model of activities in a mobile computing environment that can separate anomaly when under attacks from the normalcy?

In their pioneering work on intrusion detection in MANETs, [1] Zhang and Lee describe a distributed and cooperative intrusion detection model where every node in the network participates in intrusion detection and response [2]. In this model, an IDS agent runs at each mobile node, and performs local data collection and local detection, whereas cooperative detection and global intrusion response can be triggered when a node reports an anomaly. In paper [8], a cluster based intrusion detection approach is proposed. It is explained how to provide more accurate information on attack types when an anomaly is found. Moreover, a set of rules that can identify the attack types of several well-known attacks is presented. In paper [9], a statistical anomaly detection algorithm based on Markov chains has been proposed. It involves two steps, construction of test suite and construction of a classifier. Construction of test suite contains the training data and test data. Statistical model is created using the Markov chain construction algorithm.

Construction of classifier involves building a model, which will detect anomalous behavior. The result of the system will be anomalous or normal. In paper [7], Markov chains are used to describe the normal transitions that occur for different TCP and IP headers. In [4], a data mining method that performs cross-feature analysis to capture the inter-feature correlation patterns in normal traffic has been proposed. In [5], MAC layer anomaly detection based on cross-feature analysis to capture the inter-correlation patterns among features of MAC layer has been proposed. In [6], routing anomaly detection based on Markov chains has been proposed. In paper [10], a specification based intrusion detection system to detect attacks on AODV (Ad hoc On-Demand Distance Vector) has been proposed. In paper [11], real-time intrusion detection that uses knowledge base to detect real-time attacks has been proposed. In [12], an algorithm for prevention and detection of MAC layer misbehavior to deal with problems of colluding selfish nodes has been proposed. In [13], it is given that a straightforward way to detect power attacks, to measure the power on a process-by-process basis, thus determining which processes were responsible for consuming large amounts of energy. In [14], three main forms of sleep deprivation attack on general-purpose mobile computers namely Service request attacks, benign power attacks, and malignant power attacks have been proposed. In [15], IDS model architecture with agents to monitor attack related activity within a wireless local area network has been proposed.

Comparing with all the works in the literature, our work presented in this paper is different in many ways. First, it is distributive and to be placed in each node of the network. Second, it is cooperative, since it considers the neighbor node's intrusion result in the decision process. Finally it has detection subsystems for three layers namely, MAC, routing, application. Our simulated results show that our integrated

anomaly detection system gives better performance compared to individual anomaly detection sub systems.

Data collection

The proposed system architecture is shown in figure 1. Data collection module is included for each anomaly detection subsystem to collect the values of features for corresponding layer. Normal profile is created using the data collected during the normal scenario. Attack data is collected during the attack scenario.

Data preprocess

The audit data is collected in a file and it is smoothed so that it can be used for anomaly detection. The value space is divided to bins. Each value is replaced by their corresponding bin median values. Depending upon the range of the value space for each feature, the size of the bins is selected. In the entire three layer anomaly detection systems, the above-mentioned preprocessing technique is used.

III. SYSTEM ARCHITECTURE

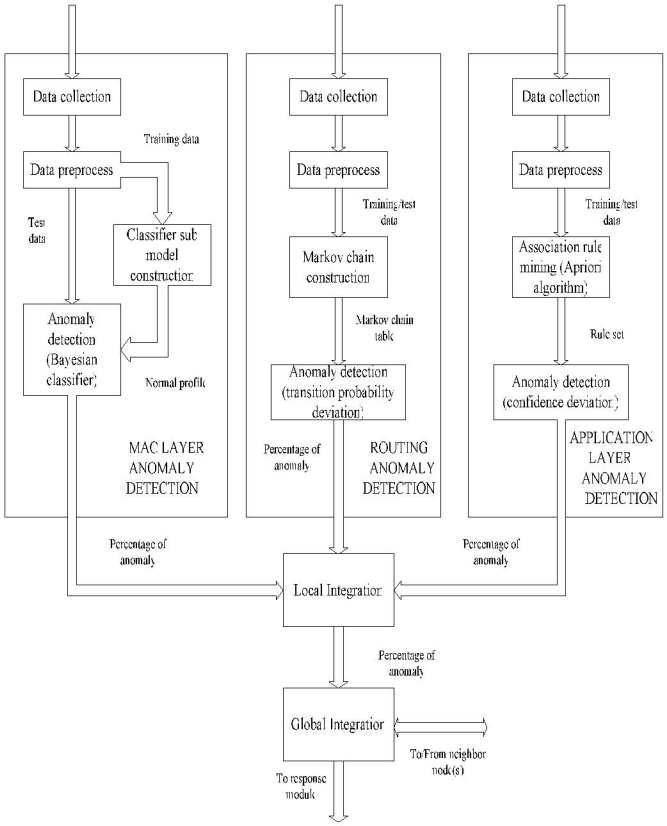

Fig. 1. Proposed System Architecture

MAC layer anomaly detection

This module is used to detect MAC layer anomalies produced in the neighborhood of the working node. Cross feature analysis technique is used to find the inter feature correlation.

Cross feature analysis for classifier sub model construction:

1. For each feature vector **f** in the training data set, compute classifier C_i for each feature f_i using $\{f_1, f_2, \ldots, f_{i-1}, f_{i+1}, \ldots, f_k\}$. C_i is learned from the training data set using Naïve Bayesian classification algorithm. The probability P_i $(f_i|f_1, f_2, \ldots, f_{i-1}, f_{i+1}, \ldots, f_k)$ is learned.
2. Compute the average probability for each feature vector **f**, and save in a probability distribution matrix M. A decision threshold **θ** is learned from the training data set.

Normal profile is created using the threshold value. If the probability is greater than threshold value it is labeled as normal, otherwise it is labeled as abnormal.

MAC layer anomaly detection

Input: Preprocessed train data, preprocessed test data

Output: Percentage of anomaly

1. Read train data set file
2. Call Bayesian classifier program for training the classifier for anomaly detection
3. Read the test data file
4. Test the classifier model with the test data file
5. Print the confusion matrix to show the actual class vs. predicted class
6. Percentage of anomaly is calculated as follows

$$\text{Percentage} = \frac{\text{Number of predicted abnormal class}}{\text{Total number of traces}} * 100$$

Routing layer anomaly detection

This module is for detection of routing anomalies in the network. Markov chain based anomaly detection is used for normal profiling.

Features used

- Number of routes selected
- Number of hop counts

Routing anomaly detection

Input: Preprocessed train data, preprocessed test data
Output: Percentage of anomaly

1. Read the preprocessed train data file
2. Create Markov chains (state transitions) for the sequence in the train data
3. Construct transition probability table T1 for train data as follows

$$P(s1, s2) = \frac{N(s1, s2)}{N(s1)} \quad (1)$$

Where s1, s2 – states,
N (s1, s2) - Number of transitions from s1 to s2 in the sequence,
N (s1) - Number of states s1 in the sequence,
P (s1, s2) – transition probability.

4. Read preprocessed test data file
5. Create Markov chains (state transitions) for the sequence in the test data
6. Construct transition probability table T2 for test data using equation 1.
7. For Each entry in T2
   For each entry in T1
   If state transition matched
   Difference in probability is calculated
   If (difference > 0.1)
   AC ++
   Exit loop
   Else
   NC++
   Exit loop
   Else
   AC ++
   Exit loop
8. Percentage of anomaly is calculated as follows

$$Percentage = \frac{AC}{AC + NC} * 100$$

Application layer anomaly detection

This module is used to detect anomaly in the application layer. Association rule mining technique is employed. Apriori algorithm is used to generate frequent item sets. Rule set is generated from frequent item set obtained. Application layer anomaly detected using minimum support threshold and minimum confidence threshold.

Features used

- Source node
- Destination node
- Packets received

I. Application layer anomaly detection

Input: Minimum support value, Minimum confidence value, Preprocessed train data file, preprocessed test data file
Output: Percentage of anomaly

Get minimum support value, minimum confidence value
1. Read preprocessed train data file
2. Frequent item set F1 is generated for train data
3. Association rule set AR1 is generated for F1
4. Read preprocessed test data file
5. Frequent item set F2 is generated for test data
6. Association rule set AR2 for F2 is generated
7. Anomaly detection is done as follows
8. For each entry in AR2
   For each entry in AR1
   If rule is matched
   Difference in confidence value is calculated
   If difference > 5
   Then AC++
   Else
   NC++
   End If
   Else
   Abnormal count++
   End If
9. Percentage of anomaly is calculated as follows

$$Percentage = \frac{AC}{AC + NC} * 100$$

Local integration

Local integration module takes the results from three anomaly detection systems. Weight for each layer is assigned. Average of weighted sum gives the output of the local integration.

Global integration

Global integration module is used to find the intrusion result for entire network. The aim of global integration is to consider the neighbor node(s) result for taking decision towards response module.

IV. Implementation and Results

GloMoSim 2.03 is used for generating the normal and abnormal data sets for the anomaly detection systems. Java 1.5 and Active perl 5.8 are used for implementing the anomaly detection system. GloMoSim needs Microsoft VC++ 6.0 for run. Windows 2000 platform is used. Configuration settings to simulate the ad hoc network environment is given in the Table 1.

Table 1: Configuration Settings

Parameters	Values
No of nodes	30
Terrain range	2000 x 2000 Meters
Mac layer protocol	802.11
Routing layer protocol	DSR
Mobility model	Random way point

Table 2: Comparison of Detection Rate

Detection module	Detection rate
MAC Layer Anomaly Detection using Bayesian Classification (A)	80%
Routing Anomaly Detection (B) using Markov Chain	75%
Application Layer Anomaly detection (C)	93.75%
Local Integration (D)	95.41%
Global Integration (E)	94.33%

Table 3: Comparison of False Positive Rate

Detection module	False positive rate
MAC Layer Anomaly Detection (A)	1.0%
Routing Anomaly Detection (B)	1.2%
Application Layer Anomaly Detection (C)	1.3%
Local Integration (D)	0.8%
Global Integration (E)	0.75%

Detailed algorithm-Local Integration
Input: MAC layer anomaly result (%),
Routing layer anomaly result (%),
Application layer anomaly result (%)
Output: Local Integration result (%)

1. Read result files from three anomaly detection systems
2. Assign weights for each anomaly detection system
3. Average of weighted sum is calculated
4. The result is sent to Global integration module

Detailed algorithm-Global Integration
Input: Neighbor node (s) result, local result
Output: Overall result for the entire network

1. Read neighbor node (s) result, local result files
2. Weights are assigned to current node and neighbor node (s)
3. Weighted sum of inputs is considered as overall result

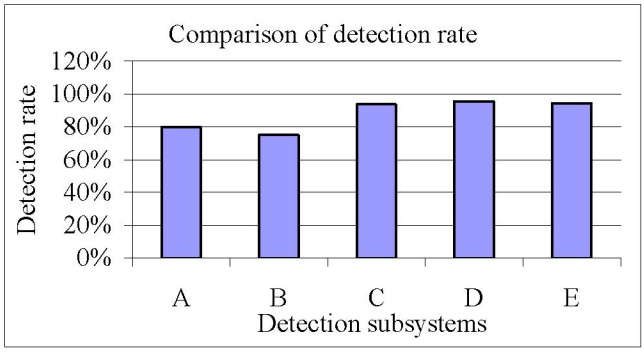

Fig. 2. Comparison of Detection Rate

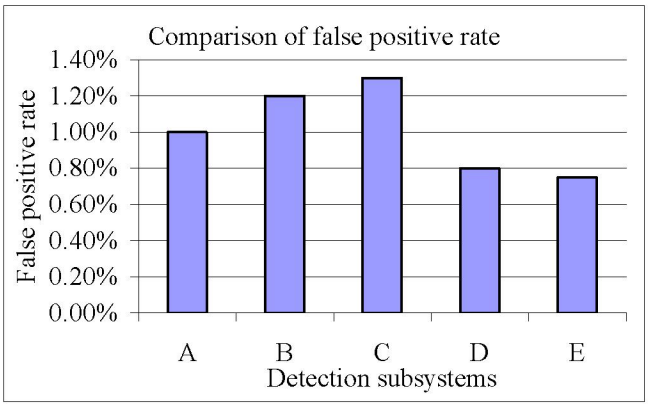

Fig. 3. Comparison of False Positive Rate

Table 2 shows the detection rate for the anomaly detection subsystems and integration modules. Table 3 shows the false positive rate for the anomaly detection subsystems and integration modules. Figure 2 illustrates the comparison of detection rate. Figure 3 illustrates comparison of false positive rate.

V. Conclusions and Future Work

In this work, an anomaly detection system comprises of detection modules for detecting anomalies in MAC layer, routing layer and application layer traffic. This system is cooperative and distributive; it considers the anomaly detection result from the neighbor node(s) and sends the current working node's result to its neighbor node(s). Experimental results show that detection rate is increased when compared to the anomaly detection based on individual layer traffic. False positive rate is also reduced.

Feature selection algorithms may be used in selection of features for each layer detection system. Based on the information gain measures, features having more information gain are taken for anomaly detection process. Results from adjacent layer detection module can be used in the next layer. This can be achieved by cross layer structure based anomaly

detection system, in which result of one layer detection module is sent to next level detection module. Regression analysis methods can be followed to assign weights for each detection module and for assigning weights for current working node and neighbor node(s).

REFERENCES

[1] Y. Zhang and W. Lee, 'Intrusion Detection in Wireless Ad Hoc Networks', 6th Int'l. Conf. Mobile Comp. and Net. Aug. 2000, pp. 275–83.

[2] Y. Zhang, W. Lee, and Y. A. Huang, 'Intrusion Detection Techniques for Mobile Wireless Networks', ACM J. Wireless Net., vol. 9, no. 5, Sept. 2003, pp.545–56

[3] Amitabh Mishra, Ketan Nadkarni, and Animesh Patcha, Virginia Tech 'Intrusion Detection in Wireless Ad Hoc Networks', IEEE Wireless Communications, February 2004, pp. 48-60.

[4] Y. Huang, W. Fan, W. Lee, and P. S. Yu, 'Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies', Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems, 2003, pp. 478-487.

[5] Yu Liu, Yang Li and Hong Man, 'MAC Layer Anomaly Detection in Ad Hoc Networks', Proceedings of the 6th IEEE Information Assurance Workshop, June 17, 2005, pp. 402-409.

[6] B. Sun, K. Wu, and U. Pooch, 'Routing Anomaly Detection in Mobile Ad Hoc Networks', Proceedings of the 12th IEEE Int'l Conf. on Computer Communications and Networks (ICCCN'03), Dallas, TX, Oct. 2003, pp. 25-31.

[7] Rena Hixon, Don M. Gruenbacher, 'Markov Chains in Network Intrusion Detection', Proceedings of the IEEE Workshop on Information Assurance, United States Military Academy, 2004, pp.432-433.

[8] Yia-an Huang, WEnke Lee, 'A Cooperative Intrusion Detection System for Ad hoc Networks', Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, 2003, pp. 135-147.

[9] S. Jha, K. Tan, and R. Maxion, 'Markov chains, classifiers, and intrusion detection', Proceedings of 14th IEEE Computer Security Foundations Workshop, 2001, pp. 206-219

[10] Baolin Sun, Hua Chen, Layuan Li, 'An Intrusion Detection System for AODV', Proceedings of the 10th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS '05), 2005, pp. 358-365.

[11] Iaonna Stamouli, Patroklos G. rgyroudis, Hitesh Tewari, 'Real-time Intrusion Detection for Ad Hoc Networks', Proceedings of the 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, 2005, pp. 374-380.

[12] A.A.Cardenas, S.Radosavac, J.S.Baras, 'Detection and Prevention of MAC Layer Misbehavior in Ad Hoc Networks', Proceedings of the 2nd ACM workshop on Security of Ad hoc Networks and Sensor Networks, 2004, pp. 17-22.

[13] Daniel C.Nash, Thomas L. Martin, Dong S. Ha, and Michael S. Hsiao, 'Towards an Intrusion Detection System for Battery Exhaustion Attacks on Mobile Computing Devices' IEEE Int'l Conf. on Pervasive Computing and Communications Workshops, 2005, pp. 141-145.

[14] T.Martin, M.Hsiao, D.Ha, and J.Krishnaswami, 'Denial of-Service Attacks on Battery-powered Mobile Computers', Second IEEE International Conference on Pervasive Computing and Communications, March 2004, pp. 309-318.

[15] Hang Yu Yang, Li-Xia Xie, 'Agent based Intrusion Detection for a Wireless Local Area Network', Proceedings of the IEEE third International Conference on Machine Learning and Cybermatics, 2004, pp. 2640-2643.