IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010
ISSN: 1793-8236

Agent Based Efficient Anomaly Intrusion Detection System in Adhoc networks

R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai

Abstract—**Networks are protected using many firewalls and encryption software's. But many of them are not sufficient and effective. Most intrusion detection systems for mobile ad hoc networks are focusing on either routing protocols or its efficiency, but it fails to address the security issues. Some of the nodes may be selfish, for example, by not forwarding the packets to the destination, thereby saving the battery power. Some others may act malicious by launching security attacks like denial of service or hack the information. The ultimate goal of the security solutions for wireless networks is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. This paper incorporates agents and data mining techniques to prevent anomaly intrusion in mobile adhoc networks. Home agents present in each system collects the data from its own system and using data mining techniques to observed the local anomalies. The Mobile agents monitoring the neighboring nodes and collect the information from neighboring home agents to determine the correlation among the observed anomalous patterns before it will send the data. This system was able to stop all of the successful attacks in an adhoc networks and reduce the false alarm positives.**

Index Terms—**Mobile agents, Intrusion detection system, Adhoc networks, Network Security.**

I. Introduction

Intrusion detection is an important part of computer security. It provides an additional layer of defense against computer is use after physical, authentication and access control [5]. A mobile ad hoc network is a collection of wireless mobile hosts forming a dynamic network infrastructure without any standard infrastructure or centralized administration. The flexibility in space and time induces new challenges towards the security infrastructure. 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 [7]. Military, University campuses and conference settings also gain on account of these wireless networks since they allow easy collaboration and efficient communication on the fly without the need for costly network infrastructure.

Expectations are also high with respect to the use of these networks in places like hotels, airports etc. But a vital problem that must be solved in order to realize these applications of ad hoc networks is that concerning the security aspects of such networks [8].Intrusion detection is used in the networks by comparing the set of baselines of the system with the present behavior of the system [3]. Thus, a basic assumption is that the normal and abnormal behaviors of the system can be characterized. The intrusion detection community has been deals mainly on wired networks, but it is lack of security in wireless networks. Anomaly detection and misuse detection or signature detection are the two techniques used for intrusion detection system. Anomaly detection describes the abnormal patterns of behavior, where "abnormal" patterns are defined beforehand. Misuse detection relies on the use of specifically known patterns of unauthorized behavior. Thus these techniques rely on sniffing packets and using the sniffed packets for analysis. In order to realize these ID techniques the packets can be sniffed on each of the end hosts. This is called as host intrusion detection (HID). It is also possible to sniff these packets on certain predetermined machines in the network. This is called as network intrusion detection (NID).

Mobile agents are a special type of agents defined as "processes capable of roaming through large networks such as the adhoc wireless network, interacting with machines, collecting information and returning after executing the tasks adjusted by the user". The nature of mobility in a wireless networks creates an vulnerability due to the open medium, dynamically changing networks. In order to avoid such circumstance, to develop new architecture and mechanisms to protect the wireless networks and mobile computing applications [7].

The remainder of the paper is organized as follows, Section 2 contains related work, Section 3 describes our proposed approach, and Section 4 describes the Results and conclusion.

II. Related Work

Traditional security mechanism such as intrusion detection system, firewall and encryption methods are not sufficient to

Manuscript received July 1, 2009.

R. Nakkeeran is with the Department of Computer Science and Engineering, Dr Pauls engineering College (Affiliated to Anna University, Chennai), Vanur Taluk, Villupuram -605 109, India. （Phone: +91 9787718933; +91 4142 329090）

S T. Aruldoss Albert is with the University Department of Electrical Engineering, Anna University Coimbatore, Coimbatore - 641 013, India.

R. Ezumalai is with the Department of Computer Science and Engineering, Dr Pauls engineering College (Affiliated to Anna University, Chennai)., Vanur Taluk, Villupuram -605 109, India. (Phone: +91 9345486422).

provide security in an adhoc networks. Countering threats to an organization's wireless adhoc network is an important area of research. Intrusion detection means identifying any set of actions that attempt to compromise the integrity, confidentiality or availability of resource [3]. Many techniques have been discussed to prevent attacks in an wireless adhoc networks as follows.

Ricardo Puttini et al [16], propose design and development of the IDS are considered in 3 main stages. A parametrical mixture model is used for behavior modeling from reference data. The associated Bayesian classification leads to the detection algorithm [15]. MIB variables are used to provide IDS needed information. Experiments of DoS and scanner attacks validating the model are presented as well. João B. D. Cabrera Et al [17], provides the solution of intrusion detection in Mobile Ad-Hoc Networks (MANETs), utilizing ensemble methods. A three-level hierarchical system for data collection, processing and transmission is described. Local IDS (intrusion detection systems) are attached to each node of the MANET, collecting raw data of network operation, and computing a local anomaly index measuring the mismatch between the current node operation and a baseline of normal operation. The complete suite of algorithms was implemented and tested, under two types of MANET routing protocols and two types of attacks against the routing infrastructure.

Yongguang Zhang et al [18], propose new intrusion detection and response mechanisms are developing for wireless ad- hoc networks. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Many of the intrusion detection techniques developed on a fixed wired network are not applicable in this new environment. Farroq et al [19] propose the signature detection technique and investigate the ability of various routing protocols to facilitate intrusion detection when the attack signatures are completely known. We show that reactive ad-hoc routing protocols suffer from a serious problem due to which it might be difficult to detect intrusions even in the absence of mobility. Mobility makes the problem of detecting intruders harder.

Vijay Bhuse et al [10], propose lightweight methods to detect anomaly intrusions in wireless sensor networks (WSNs). The main idea is to reuse the already available system information that is generated at various layers of a network stack. This is the different approach for anomaly intrusion detection in WSNs. Hongmei Deng et al [21], propose the underlying distributed and cooperative nature of wireless ad hoc networks and adds one more dimension of cooperation to the intrusion detection process. That is, the anomaly detection is performed in a cooperative way involving the participation of multiple mobile nodes. Unlike traditional signature-based misuse detection approaches, the proposed scheme detects various types of intrusions/attacks based on the model learned only from normal network behaviors. Without the requirements of pre-labeled attack data, the approach eliminates the time-consuming labeling process and the impacts of imbalanced dataset.

Bo Sun et al [22], propose we first introduce two different approaches, a Markov chain-based approach and a Hotelling's T2 test based approach, to construct local IDSs for MANETs. Then demonstrate that nodes' moving speed, a commonly used parameter in tuning IDS performances, is not an effective metric to tune IDS performances under different mobility models. To solve this problem, author further propose an adaptive scheme, in which suitable normal profiles and corresponding proper thresholds can be selected adaptively by each local IDS through periodically measuring its local link change rate, a proposed unified performance metric.

Haiguang Chen et al [23], propose lightweight anomaly intrusions detection. In the scheme, author investigates different key features for WSNs and defines some rules to building an efficient, accurate and effective Intrusion Detection Systems (IDSs). We also propose a moving window function method to gather the current activity data. The scheme fits the demands and restrictions of WSNs. The scheme does not need any cooperation among monitor nodes. Simulation results show that the proposed IDSs are efficient and accurate in detecting different kinds of attacks.

Gabriela F. Cretu et al [24], propose the use of model exchange as a device moves between different networks as a means to minimize computation and traffic utilization. Any node should be able to obtain peers' model(s) and evaluate it against its own model of "normal" behavior.

Yu Liu et al [25], propose game theoretic framework to analyze the interactions between pairs of attacking/defending nodes using a Bayesian formulation. We study the achievable Nash equilibrium for the attacker/defender game in both static and dynamic scenarios. The dynamic Bayesian game is a more realistic model, since it allows the defender to consistently update his belief on his opponent's maliciousness as the game evolves. A new Bayesian hybrid detection approach is suggested for the defender, in which a lightweight monitoring system is used to estimate his opponent's actions, and a heavyweight monitoring system acts as a last resort of defense.

Many authors proposed different techniques to prevent attacks in wireless adhoc networks. But all these methods reported to have a lot of pros and cons of its own proposal. The authors mainly classified their mechanism as signature method, anomaly method. In Signature Based Method, a threat is always be stored in database. New threat being discovered in the wild and the signature for detecting that threat. This Mechanism would be unable to detect the new threat. In Anomaly Based Method, it monitors system and its network behaviors. It set the baseline of network and system. This mechanism work effectively against wireless networks but it generates some false positive results. In this paper, a new attempt has been made and worked out effectively against attacks in wireless networks. This paper incorporates agent and data mining method to provide solution against security issues in MANET networks. With the help of home agent and mobile agents, it gathers information from its own system and

neighboring system to identify any attack and through data mining techniques to find out the attacks has been made in that networks.

III. Our Approach

Our approach is entirely based on anomaly based method, which has been used to address security problems related to attacks in a wireless networks. This paper incorporates new methodology such as mining and agents to provide solutions against wireless networks. Our Proposal provides the three different techniques to provide suffice security solution to current node, Neighboring Node and Global networks. The following figure clearly depicts the architecture of the system to prevent the attacks in wireless networks. The following section outlines each module's work in detail.

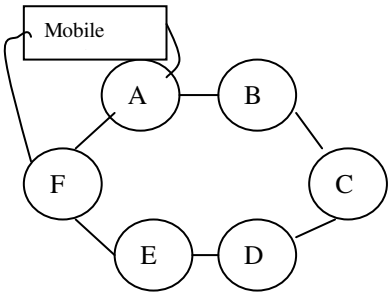

Fig 1: Proposed System Architecture Outlines

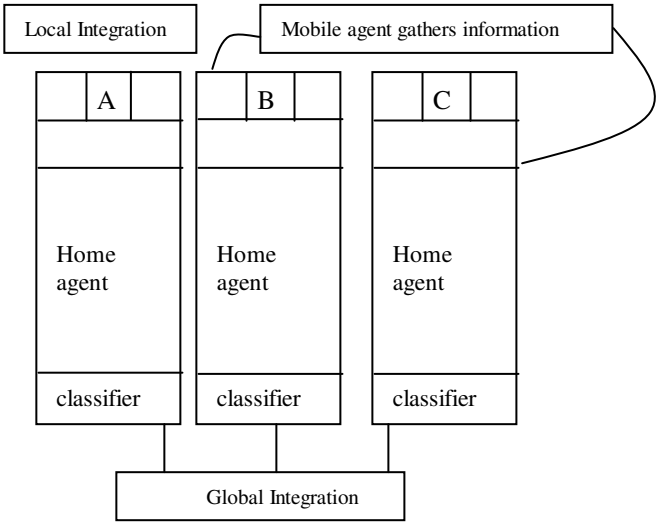

Fig 2: Proposed System Architecture

A. *Home agent*

Home agent is present in each system and it gathers information about its system from application layer to routing layer. Our proposed system provides solution in three techniques. 1. It monitors its own system and its environment dynamically. It uses classifier construction to find out the local anomaly. 2. Whenever the node want to transfer the information from the node F to B. It broadcast the message to E and A. Before it sends the message, it gathers the neighboring nodes (E &B) information using mobile agent. It calls the classifier rule to find out the attacks with help of test train data. 3. It provides same type of solution through out the global networks. It has been explained in the following section.

1) Current node - Home Agent is present in the system and it monitors its own system continuously. If an attacker sends any packet to gather information or broadcast through this system, it calls the classifier construction to find out the attacks. If an attack has been made, it will filter the respective system from the global networks.
2) Neighbouring node - Any system in the network transfer any information to some other system, it broadcast through intermediate system. Before it transfer the message, it send mobile agent to the neighboring node and gather all the information and it return back to the system and it calls classifier rule to find out the attacks. If there is no suspicious activity, then it will forward the message to neighboring node.
3) Data collection - Data collection module is included for each anomaly detection subsystem to collect the values of features for corresponding layer in an system. Normal profile is created using the data collected during the normal scenario. Attack data is collected during the attack scenario.
4) Data preprocess - The audit data is collected in a file and it is smoothed so that it can be used for anomaly detection. Data preprocess is a technique to process the information with the test train data. In the entire layer anomaly detection systems, the above mentioned preprocessing technique is used.

B. *Cross feature analysis for classifier sub model construction*

1) Each feature or character vector f in the training data set, calculate classifier C, for each feature fi using {f1, f2... fi -I, fi+.-f k} - Ci is learned from the training data set using Naïve Bayesian classification algorithm. The probability P. (filfl, f2 ...,I fi- i, f+1, ..., fk) is learned.
2) 2. Compute the average probability for each feature vector f, and save in a probability distribution matrix M. A decision threshold 0 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. Anomaly detection

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

1) Read processed 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

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

C. Local integration

Local integration module concentrate on self system and it find out the local anomaly attacks. Each and every system under hat wireless networks follows the same methodology to provide a secure global networks.

D. 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. Experimental Results

There are many number of attacks has been tested to prevent attacks in wireless network. This system not only blocks the application oriented issues and it stops some of the network security issues. Consider this limited number of attacks and tested with this proposed system to find out the attacks and got a encourage results. These are the parameters has been take to analyze the proposed system to find out the efficiency.

TABLE 1: INPUT PARAMETER CONSIDERATION

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

This system can tested with limited number of attacks present in the wireless networks. It shows the encouragement results to support the proposed system. Detection rate of anomaly rate in our proposed system is high and it encourages the system.

TABLE 2: DETECTION RATE OF THE PROPOSED SYSTEM

Detection Module	Detection Rate
Anomaly Detection (A)	80%
Local Integration (D)	95.41%
Global Integration (E)	94.33%

This system act as an Intrusion prevention system to detect and prevent the attacks. But the drawback of existing Intrusion prevention system can generate the more false alarms, but it may work efficiently. This system can able to stop the attacks as well as it could not generate the false alarms and it work effectively against the web parameter attacks. Consider this limited number of access and tested with this proposed system to find out the alarm rates.

TABLE 3: ALARM RATE OF THE PROPOSED SYSTEM

Detection Module	False positivity
Anomaly Detection	1.0%
Local Integration (D)	0.8%
Global Integration	0.75%

V. Conclusion

In this work, an anomaly detection system comprises of detection modules for detecting anomalies in each layer. 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 other mechanism. False positive rate is also reduced in this mechanism. Traditional security mechanism such as IDS and firewall have not been sufficient to provide the security of wireless networks, however, this mechanism is able to block abnormal approach to wireless networks and to detect previously unknown attacks as well as variations of known attacks.

References

[1] Y. Zhang and W. Lee, 'Intrusion Detection in Wireless AdHoc 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'lConf. on Computer Communications and Networks (ICCCN'03), Dallas, TX, Oct. 2003, pp. 25-3 1.
[7] Rena Hixon, Don M. Gruenbacher, 'Markov Chains in Network Intrusion Detection', Proceedings of the IEEE Workshopon Information Assurance, United States MilitaryAcademy, 2004, pp.432-433.
[8] Yia-an Huang, WEnke Lee, 'A Cooperative Intrusion Detection System for Ad hoc Networks', Proceedings of the Ist 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 1 oth 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 MichaelS. Hsiao, 'Towards an Intrusion Detection System for BatteryExhaustion 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.
[16] Ricardo Puttini, Maíra Hanashiro, Javier García-Villalba, C. J. Barenco, " On the Anomaly Intrusion-Detection in Mobile Ad Hoc Network Environments", Personal Wireless Communications ,Volume 4217/2006, Springerlink, September 30, 2006
[17] João B. D. Cabrera, Carlos Gutiérrez , Raman . Mehra ,"Ensemble methods for anomaly detection and distributed intrusion detection in Mobile Ad-Hoc Networks", Volume 9 , Issue 1 (January 2008) table of contents, Pages 96-119 , Elsevier Science Publishers, 2008.
[18] Yongguang Zhang , Wenke Lee, " Intrusion detection in wireless ad-hoc networks", Pages: 275 - 283 Year of Publication: 2000 ISBN:1-58113-197-6, ACM, 2000.
[19] Farooq Anjum Dhanant Subhadrabandhu and Saswati Sarkar,"Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A comparative study of various routing protocols", Seas, 2008.
[20] Vijay Bhuse , Ajay Gupta , " Anomaly intrusion detection in wireless sensor networks" , Special issue on trusted internet workshop (TIW) 2004, Journal of High Speed Networks, Volume 15 , Issue 1 (January 2006), ACM, 2006.
[21] Hongmei Deng; Xu, R.; Li, J.; Zhang, F.; Levy, R.; Wenke Lee, " Agent-based cooperative anomaly detection for wireless ad hoc networks", Parallel and Distributed Systems, Volume 1, Issue , 0-0 0 Page(s):8, 2008.
[22] Bo Sun 1 *, Kui Wu 2, Yang Xiao 3, Ruhai Wang 4, "Integration of mobility and intrusion detection for wireless ad hoc networks", 2006.
[23] [23] Haiguang Chen, Peng Han, Xi Zhou, Chuanshan Gao, "Lightweight Anomaly Intrusion Detection in Wireless Sensor Networks", Intelligence and Security Informatics, Springerlink, 2007.
[24] Gabriela F. Cretu, Janak J. Parekh, Ke Wang, Salvatore J. Stolfo, "Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks.
[25] Yu Liu, Cristina Comaniciu, Hong Man, "A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks", ACM 159593507X, 2006.

Mr. R. Nakkeeran pursuing PhD in Anna University Coimbatore and received the M.E Degree in Computer Science and Engineering from Jayam College of Engineering and Technology , Anna University, Chennai. His current research involves In Data Mining and mobile Computing. Presently working with Dr. Pauls Engineering College (Affiliated to Anna University, Chennai) as Professor in the Department of Computer Science and Engineering.