Asian Journal of Information Technology 11 (6-12): 237-243, 2012
ISSN: 1682-3915

Mobile Agent Framework for Network Intrusion Detection System with Classification Algorithm

[1]R. Sasikumar and [2]D. Manjula
[1]Department of Computer Science and Engineering, R.M.D. Engineering College,
Kavaraipettai, Chennai, Tamil Nadu, India
[2]Department of Computer Science and Engineering, College of Engineering,
Anna University, Chennai, Tamil Nadu, India

Abstract: Wireless computingis the delivery of computingas aservicerather than aproduct, whereby shared resources, software and information are provided to users over anetwork. Wireless computing entrusts services with a user's data, software and computation on a published Application Programming Interface (API) over a network. Wireless computing is defined in simplest terms as follows: A set of pooled computing resources, delivered over the web, powered by software. It is a form of computing that involves the interaction of several virtualized resources, meaning that many servers are connecting and sharing information that can expand and contract across servers depending on the amount of servers needed to manage the amount of traffic on various sites. Wireless allows the end users to use the application without installation and access their personal files at any computer with internet access. Apart from the advantages of wireless environment, security is the major issue. Due to the distributed nature, wireless environment is an easy target for intruders looking for the possible attacks to exploit. There are many advantages in wireless computing such as increased storage, highly automated, flexibility, mobility, etc. apart from these advantages the major issue in wireless environment is security. Due to the distributed nature of the wireless environment many users can access the wireless to utilize the service. So, there is a chance for an intruder or attacker to exploit an attack in the wireless environment. In order to address this issue in the wireless environment an Intrusion Detection System (IDS) is proposed based on the features of the mobile agent. The mobile agents are used to collect and analyze the data collected from wireless environment to identify attacks exploited by the intruders. The main objective of the proposed system is to detect the known and new attacks exploited by the intruders in the wireless environment.

Key words: Wireless computing, Intrusion Detection System, mobile communication, mobile agent, intruders, attacks

INTRODUCTION

Wireless computing means a distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service level agreements established through negotiation between the service provider and consumer. In wireless environment the systems are distributed in nature so there is greater chance of exploiting attacks by the intruders.

An Intruder is a person who attempts to gain unauthorized access to a system to damage that system or to disturb data on that system. In summary, this person attempts to violate security by interfering with system availability, data integrity or data confidentiality. Intrusion Detection (ID) is a type of Security Management System for computers and networks. An ID System gathers and analyzes information from various areas within a computer or a network to identify possible security breaches which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID use svulnerability assessment which is a technology developed to assess the security of a computer system or network. The functions of intrusion detection includes monitoring and analyzing both user and system activities, analyzing system configurations and vulnerabilities, assessing system and file integrity, ability to recognize patterns typical of attacks, analysis of abnormal activity patterns, tracking user policy violations.

To detect the intruders in the network the Intrusion Detection System was deployed. An Intrusion Detection

Corresponding Author: R. Sasikumar, Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, Chennai, Tamil Nadu, India

System (IDS) which inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. There are several ways to categorize IDS: misuse detection, anomaly detection, network-based and Host-Based Systems.

Misuse detection: In misuse detection, the IDS analyze the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS look for a specific attack that has already been documented.

Anomaly detection: In anomaly detection, the system administrator defines the baseline or normal, state of the network traffic load, breakdown, protocol and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

Network based system: In a Network-Based System or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall simplistic filtering rules.

Host Based Systems: In a Host-Based System, the IDS examines at the activity on each individual computer or host. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. An attack against a cloud computing system can be silent for a network based IDS deployed in its environment because node communication is usually encrypted. Attacks can also be invisible to host based IDS because cloud specific attacks don't necessarily leave traces in a Nodes Operating System where the host based IDS reside. In this way, traditional IDS can't appropriately identify suspicious attacks in cloud environment. The current IDS have some of the shortcomings such as:

- Most IDS detect attacks by analyzing information from a single host or a single network interface at many locations throughout the network. Consequently, IDS components miss the communication and the cooperation between each other. This fact hampers the capability to detect large-scale distributed attacks
- Most commercial IDS are built in hierarchical architecture which is a tree structure with a control system at the top, information aggregation units at the internal nodes and sensor units at the leaf nodes. In this kind of system, large amount of data transferred across the network may result in network congestion

In this study, the distributed IDS are deployed based on the mobile agent technology using data mining algorithm which accurately captures the behaviour of the network traffic. The mobile agent is an agent having the capability of moving from one host to another. It interacts with the other nodes to collect the data. The advantage of mobile agent technology are reduces the network overload, overcoming network latency, robust and fault tolerant and it works in heterogeneous environment. The mobile agent technology has been shown to be very suitable to solve intrusion detection in a distributed environment. In the proposed system the IDS is deployed based on the mobile agent technology to detect the known and new attacks. The known attacks are defined as misuse attacks and the new attacks are defined as anomaly attacks.

LITERATURE RIVIEW

The IDS should protect the system and needed to be able to resist attack and also needed to be fault tolerant, highly adaptable and configurable. According to the above characteristics, the agent technology is appropriate alternative to develop Intrusion Detection System. The mobile agent based Intrusion Detection System were developed (Taggu and Taggu, 2011) which uses the trace gray technique to detect the intrusions. A proposed efficient anomaly Intrusion Detection System in Ad-hoc by mobile agents (Jaisankar *et al*., 2009) which uses the data mining algorithm to detect the attacks exploited by the intruders. Mobile agent based Intrusion Detection System for MANET (Li and Qian, 2010) proposed by Yinan Li which uses the clustering and joint detection technique to identify the intruders. Imen Brahmi proposed in a distributed Mobile Agent based Intrusion Detection System, called MAD-IDS (Brahmi *et al*., 2010).

The architecture of the MAD-IDS is based on detection of known and unknown attacks which uses the clustering and rule mining technique. Intelligent Intrusion Detection System framework using mobile agents (Esfandi, 2010) which detects the intruders based on the user profile and process profile. Research on distributed Intrusion Detection System based on mobile agent (Cao and Zheng, 2008) which increases the system flexibility and security. Signature based method (Akyazi and Uyar, 2008) is used in distributed intrusion detection using mobile agents against DDoS attacks.

Sodhi proposed a distributed intrusion detection using aglet mobile agent technology (Singh and Sodhi, 2007) which uses the Anomaly Detection Method. Trust modeling technique (Krmicek *et al*., 2007) is used in agent based network Intrusion Detection System which detects the intruders based on the trust established between the systems. Bin Dong proposed a Intrusion Detection System based on agents which uses the STAT technique (Dong and Liu, 2007) to detect the attacks.

OVERVIEW OF IDS AND MOBILE AGENT

This study will give a detailed description about the mobile agent theory which is used to extract the relevant features for detecting the specific category of attacks from the generic 41 features present in the KDDCup99 dataset. With the selected features, the enhanced Classifier algorithm can achieve the low false alarm rate with high attack detection rate.

Intrusion Detection System (IDS): Intrusion detection (Denning, 1987) is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, like unauthorized entrance, activity or file modification. There are three steps in the process of intrusion detection which are:

- Monitoring and analyzing traffic
- Identifying abnormal activities
- Assessing severity and raising alarm

Intrusion Detection System (IDS) is software that automates the intrusion detection process and detects possible intrusions. Intrusion Detection Systems serve three essential security functions: they monitor, detect and respond to unauthorized activity by company insiders and outsider intrusion. An IDS is composed of several components:

- Sensors which generate security events
- Console to monitor events and alerts and control the sensors
- Central engine that records events logged by sensors in a database and uses a system of rules to generate alerts from security events received

IDS tools aim to detect computer attacks and computer misuse and to alert the proper individuals upon detection. IDSs use policies to define certain events that if detected will issue an alert. Certain IDS have the capability of sending out alerts so that the administrator of the IDS will receive a notification of a possible security incident in the form of a page, email or SNMP trap. Many IDSs not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account and launching of scripts. IDS are an integral and necessary element of a complete information security infrastructure performing as the logical complement to network firewalls.

Mobile agent: The software agent can be treated as mobile agent (Singh and Sodhi, 2007) as they are able to migrate from one computer to another computer. The mobile agents are very powerful programs which can act even in the absence of the machine that initiated them. After completion of their assigned tasks, the mobile agents return to the host machine to report the result or simply terminate. The advantages of using mobile agents in IDS are listed:

- Minimizing the network traffic
- Structure and platform independence
- Dynamic nature and scalability
- Operates in heterogeneous environment
- Robust and fault tolerant
- Overcomes network latency

PROPOSED WORK

The Intrusion Detection System for this environment is proposed based on the mobile agent which uses the data mining technique to detect the intrusions in the wireless environment.

System architecture: Figure 1 contains various mobile agents for collecting and analyzing the data in the wireless environment. There are different agents used to detect the intrusions, they are as follows, collector agent, misuse detection agent, anomaly detection agent, classifier agent and alert agent. These agents are used to collect and analyze the data collected from wireless environment to detect the attacks exploited by the intruders.

System description: Research in security is most active due to its role in Mobile Agent System. The issues and requirements of security in Mobile Agent System have been satisfied by the five basic security principles that a Mobile Agent System must realize:

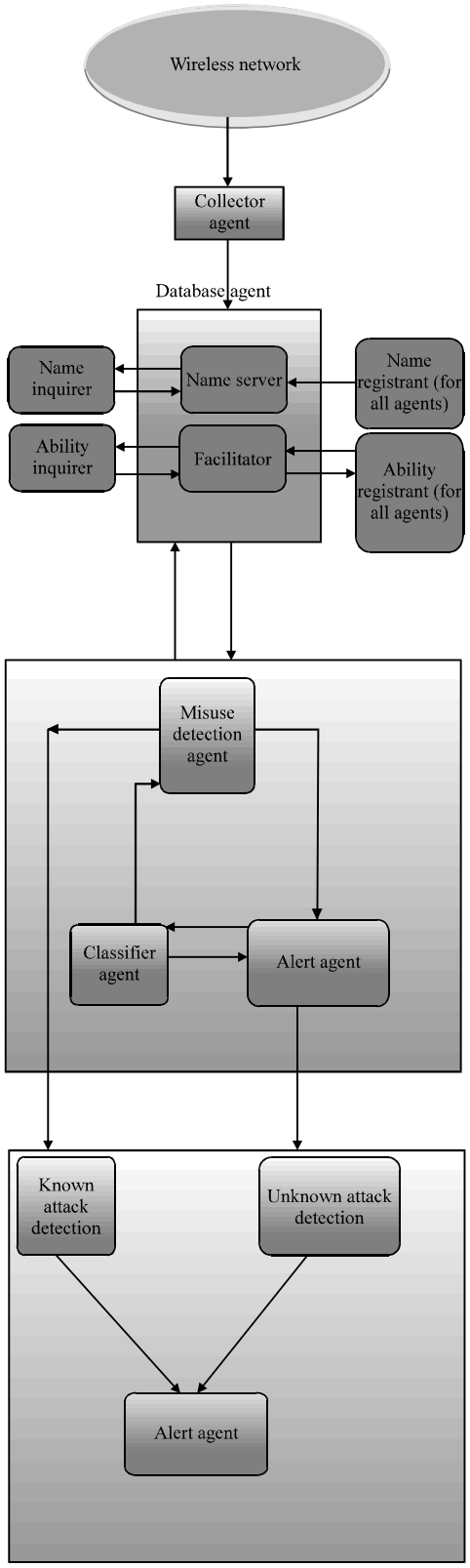

Fig. 1: System architecture

Collector agent: The collector agent is the first agent to work in the system since, it connects to the network. It collects the data from the wireless environment and stores those data in the file. This file is given as an input to the misuse detection agent.

Misuse detection agent: The misuse detection agent is used to analyze the data captured by the collector agent. It detects the known attacks in network by using the pattern matching algorithm. If there is a similarity between the collected packets and attack signatures in the database then it reports to alert agent.

Anomaly detection agent: The anomaly detection agent is used to detect the new or unknown attacks by using the classification techniques. The anomaly detection agent collects the data from the misuse detection agent to analyze the data to detect the unknown attacks, it feds the data to classifier agent to detect the new attack.

Classifier agent: The classifier agent uses the naive bayes classifier to detect the new attack. It classifies the data based on the dataset available in the database. If the incoming data is detected as attack means then it reports to anomaly agent which in turn reports to alert agent about the attack. It updates the detected attack in the database.

Alert agent: The alert agent is used to alert the system if any intrusion occurs in the network. It alerts the system based on the output of the misuse and anomaly detection agent.

Algorithms

Step 1: The threshold value is assigned by the user.

Step 2: The data received from the misuse detection agent is compared with the dataset available in database based on the threshold value.

Step 3: If the comparison of data exceeds the threshold value then it is detected as a attack and reports the anomaly detection agent.

Step 4: Then, the detected attack is updated in the database.

Step 5: The anomaly detection agent reports to the alert agent and then the alert is raised by the alert agent about the attack.

Algorithm to detect ping of death: A ping of death attack is simply sending an IP datagram, the size of which exceeds the standards. When such a datagram is received, this crashes the receiving system (Fig. 2).

Step 1: Get the packet size of the data send from one system to another system.

Step 2: The temporary value is assigned to the variable named inc.

Step 3: The limit value is calculated based on the condition:

$$Lmt = 2^{\wedge}inc$$

Step 4: The packet size is compared with the limit based on the condition:

$$If\ (Packetsize > lmt)$$

Step 5: The stored procedure is called if the packet size exceeds the limit and then it reports the attack.

Algorithm to detect land attack: A LAND attack involves IP packets where the source and destination address are set to address the same device. The reason a LAND attack works is because it causes the machine to reply to itself continuously (Fig. 3).

Step 1: Get the message details such as source IP and receiver IP.

Step 2: Checks whether the source and destination IP are same based on the condition:

$$If\ (nodeIP.equals(IreceiverP))$$

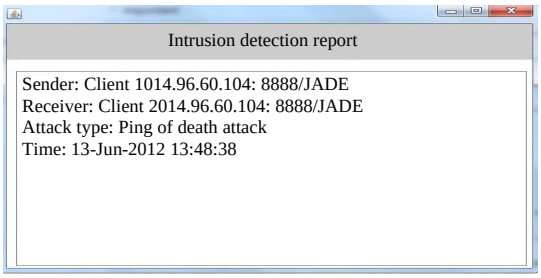

Fig. 2: Ping of death attack report

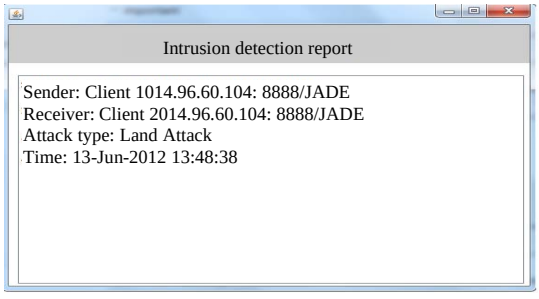

Fig. 3: Land attack report

Step 3: If the source IP and destination IP are equal means then the stored procedure is called for land attack

Step 4: It returns as attack if the IP address are equal.

Algorithm to detect tear drop attack: Tear drop attack means the packets are corrupted or overlap on each other when the packets are send from one system to another system. Now, the special characters are used in the message to denote the packets are corrupted (Fig. 4).

Step 1: Get the message send from the source system.

Step 2: The special character are defined in the function.

Step 3: It checks the message character by character for special characters based on the condition if (msg.contains (splchar.get (I). toString())).

Step 4: If the condition is true then it calls the stored procedure for the tear drop attack.

Step 5: The stored procedure returns the result as attack if the condition is true.

Algorithm to detect known attack: In this algorithm it checks for the similarity between the data and dataset available in the database. If the data is similar then it reports as known attack.

Step 1: Get the message and fetches the details such as source and destination IP, source and destination bytes, packet size.

Step 2: Checks the collected data with the data available in the database.

Step 3: The stored procedure is called for matching the data with the database. If the result is true then it reports the attack.

Step 4: The attack is the reported as pattern matching attack.

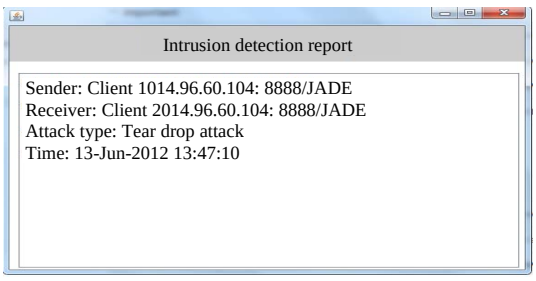

Fig. 4: Tear drop attack report

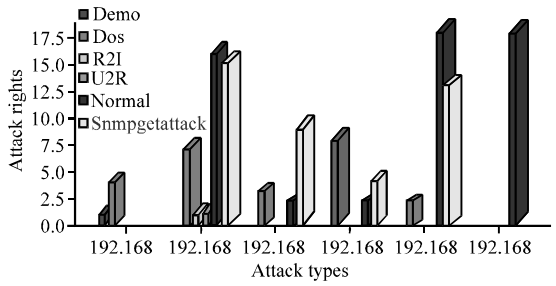

Fig. 5: Intrusion detection attack

EXPERIMENT RESULTS

The detection rate of the algorithm is compared with existing research and which is tested on the benchmark KDDCup'99 dataset. The performance of the proposed two stage filter was comparatively better than existing research in detecting the DoS, R2L and U2R attacks (DoS-98.8%, R2L-49.8% and U2R-87.6%). Hence, it should be considered for the building of IDS (Fig. 5).

CONCLUSION

The IDS for wireless computing is projected the mobile agent to identify well-known and anonymous attacks. All the mobile agents are configured in order to carry out the operations like collecting the data from wireless environment and these data are analyzed by the misuse detection agent. This agent checks whether the data collected are matching with the attack dataset available in the database. If any collected data is matched then the misuse detection agent informs the alert agent to alert the system about the intrusion. On the other hand, if the collected data is not matched with the dataset then the collected data are analyzed by anomaly detection agent which uses classifier technique to detect the unknown or new attacks. The results produced that the proposed model is professionally to classify the unpredictability profile from the normal profile. This proposed model has following advantages. First, false positive rate is low and true positive rate is high by adopting mobile agent selection algorithm. Second, real time potential is enhanced and bottleneck problem is overcome because the proposed model realized that computing progress to data by utilizing mobile agent. Third, dependability of the system is enhanced and compared with other Hierarchical Model; it surmounts single point of failure. In addition, the system is robust and fault-tolerant. The final result will be such that the known and unknown or new attacks are detected by the proposed architecture.

IMPLEMENTATION

JADE (Java Agent Development framework) is a software framework which is used to implement the mobile agents for the proposed Intrusion Detection System. The collector agent is assigned a task to collect the data from the wireless environment and stores it as a file. The file is then forwarded to the misuse detection agent, it analyses the data by matching the collected data with the attacks available in the database and if the data is similar to the patterns in the database then it reports to alert agent. If the data is not matched with the database then the classifier agent is used to classify the data based on the dataset and then it reports to alert agent and updates the database about the attack. The alert agent alerts the system based on the outcome of misuse and anomaly detection agent.

REFERENCES

Akyazi, U. and A.S.E. Uyar, 2008. Distributed Intrusion detection using mobile agents against DDoS attacks. Proceedings of the 23rd International Symposium on Computer and Information Sciences, October 27-29, 2008, Istanbul, Turkey, pp: 1-6.

Brahmi, I., S.B. Yahia and P. Poncelete, 2010. MAD-IDS novel intrusion detection system using mobile agents and data mining approaches. Proceedings of the Pacific Asia conference on Intelligence and Security Informatics, June 21-24, 2010, Hyderabad, India, pp: 73-76.

Cao, J.G. and G.P. Zheng, 2008. Research on distributed intrusion detection system based on mobile agents. Proceedings of the 7th International Conference on Machine Learning and Cybernetics, Volume 3, July 12-15, 2008, Kunming, China, pp: 1394-1399.

Denning, D.E., 1987. An Intrusion-Detection Model. IEEE Trans. Software Eng., SE-13: 222-232.

Dong, B. and X.L. Liu, 2007. An improved intrusion detection system based on agents. Proceedings of the International Conference on Machine Learning and Cybermatics, Volume 6, August 19-22, 2007, Hong Kong, pp: 3164-3167.

Esfandi, A., 2010. Efficient anomaly intrusion detection system in Ad-hoc networks by mobile agents. Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology, Volume 7, July 9-11, 2010, Chengdu, China, pp: 73-77.

Jaisankar, N., R. Saravanan and K. Duraisamy, 2009. Intelligent intrusion detection system framework using mobile agents. Int. J. Network Secur. Appl., 1: 72-88.

Krmicek, V., P. Celeda, M. Rehak and M. Pechoucek, 2007. Agent based network intrusion detection system. Proceedings of the International Conference on Intelligent Agent Technology, November 2-5, 2007, Fremont, CA, pp: 528-531.

Li, Y. and Z. Qian, 2010. Mobile agents-based intrusion detection system for mobile ad hoc networks. Proceedings of the Asia-Pacific Conference on Innovative Computing and Communication, International Conference on Information Technology and Ocean Engineering, January 30-31, 2010, Macau, China, pp: 145-148.

Singh, M. and S.S. Sodhi, 2007. Distributed intrusion detection using aglet mobile agent technology. Proceedings of the National Conference on Challenges and Opportunities in Information Technology, July 9-12, 2007, Orlando, FL, USA., pp: 148-153.

Taggu, A. and A. Taggu, 2011. TraceGray: An application-layer scheme for intrusion detection in MANET using mobile agents. Proceedings of the 3rd International Conference on Communication Systems and Networks, January 4-8, 2011, Bangalore, India, pp: 1-4.