World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 145-149, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.csea.2245

Intrusion Detection Techniques in Distributed Grid Environment Using Analysis Service

K.P. Thooyamani, R. Udayakumar and V. Khanaa

School of Computing Science, Bharath University, Chennai-73, India

Abstract: Grid computing is distributed computing in essence and because of this we suggest that intrusion detection and its alert system should be distributed and cooperative. In our solution, each node is responsible for identifying and alerting the other nodes of local events that may represent security violations. These individual IDS will cooperatively participate in the intrusion detection.Grid Node is an entity which contains resources. Event auditor is the key piece in the system and is responsible for capturing data from various sources, such as the log system, service and node messages. IDS Service analyzes data captured by the auditor and applies detection techniques based on user behavior and knowledge of previous attacks. The IDS Service is conceived to increase a grid's security level by applying two methods of intrusion detection. The behavior-based method dictates how to compare recent user actions to his usual behavior. The knowledge-based method consists of detecting known trails left by attacks or certain sequences of actions from a user that may represent an attack. In this work we focused on using a feed-forward artificial neural network.

Key words: Intrusion Detection Method · IDS · GRID · Real-Time information

INTRODUCTION

Grid Systems must be monitored to detect successful and unsuccessful attempts to breach security. This paper thesis discusses the major concerns for intrusion detection in Grid and proposes a novel solution to effectively detect intrusions, building a Grid-Based Intrusion Detection System. Intrusion Detection Systems (IDS) have a very important role in Grid security management. For the execution of large scale applications there is clearly a need to detect intrusions and any other kind of dangerous events. This goal can be achieved through integration with lower level or Network IDSs, each providing intrusion detection for a domain or sub domain of the Grid system. There are also a number of additional constraints like the ease of integration with external IDS. The lower level or local IDS monitoring the resources where a part of the application is currently running must be able to send alerts to the Grid level Intrusion Detection System (G-IDS) in case of a detected intrusion.

The G-IDS also provides mechanisms to correlate separate alerts from different local IDS in the case of possibly related intrusions, which is the focus of this paper. A possible intruder might also be interested in altering the entire execution of a complex application which is running on a large number of geographically distributed resources. Because of this the G-IDS must be aware of the running applications and should correctly identify a single intruder when receiving multiple alerts from lower level IDSs which are related to different resources belonging to the same application. To achieve this goal the G-IDS also receives real-time information from Grid monitoring systems which offers a global view of the context in which an attack might take place. This project introduces a novel approach to Grid Intrusion Detection, based on the correlation of alerts received from lower level IDSs. The design of this system is modular and can be easily integrated with existing network intrusion detection system.

Corresponding Author: R. Udayakumar, School of Computing Science, Bharath University, Chennai-73, India.

System Analysis: Existing System: In the Present work, Host based IDS and Network based IDS are implemented which can avoid the intrusions that occur only on the server and during communication. The security measure that can be of great value in such systems is the employment of Intrusion Detection Systems (IDS) to investigate configurations, logs, network traffic and user actions to detect typical attack behavior. The limitations in Existing System are as follows:

- IDS does not cover the middleware layer.
- Traditional IDS cannot appropriately identify suspicious activities in a grid and cloud environment.

Proposed System: The IDS proposed in this project has an audit system designed to cover attacks that network-based and host based systems can´t detect. We call this IDS architecture GIDS-Grid Computing Intrusion Detection System-which integrates knowledge analysis and behavior analysis to detect specific intrusions. In the proposed intrusion detection system we address intrusion at the middleware layer. IDS must be distributed in order to work in a grid computing environment. Each node must be monitored by a part of the intrusion detection system and, when an attack occurs, alerts must be sent to the other nodes in the environment and cooperation must follow. The advantages of Proposed System are as follows:

- Improved security in the entire Distributed Network
- Awareness to all neighboring nodes

The applications include in fields of IT Sector, Banking Sectors and Research Academy.

Behavior Based Analysis: In this work we focus on using a feed-forward artificial neural network because, in contrast to traditional methods, this type of network can achieve fast processing of information, self learning and a great ability to tolerate little deviations of behavior. In this particular case, we need to recognize expected behavior (legitimate use) or a severe deviation of behavior. Training plays a key role in the pattern recognition done by feed-forward networks. Only after we have the network correctly trained we can achieve efficiency in its intrusion detection abilities. For a given intrusion sample set, the network will learn to identify them by means of its back propagation algorithm. However, we focus on identifying user behavioral patterns and deviations from it. With this strategy, we are able to cover a wider range of unknown attacks.

Neural Network: In recent times, artificial intelligent (AI) techniques in general and neural network (NN) in particular have been used widely in solving problem like optimization, adaptive filtering, digital signal processing and pattern recognition and classification. Neural network techniques aim to construct useful "computers" to carry out useful computations while solving real-world problems of classification. Current intrusion detection techniques cannot detect new and novel attacks; instead the consensus solution seems to be those that detect known intrusion detection techniques. New intruding techniques are usually passed as authorized traffic. The relevance of NN in intrusion detection becomes apparent when one views the intrusion detection problem as a pattern classification problem. By building profiles of authorized computer users, one can train the NN to classify the incoming computer traffic into authorized traffic or not authorized traffic (i.e. intrusion traffic).

Problem Definition: The task of intrusion detection is to construct a model that captures a set of user attributes and determine if that user's set of attributes belongs to the authorized user or those of the intruder. The input attribute set consists of the unique characteristics of the user logging onto a computer network.

The output set is of two types-authorized user and intruder. Thus, the problem now has been reduced to a pattern recognition problem. Mathematically speaking, the problem can be stated as:
Given a data set S

$$S = \left\{ (x_i, y_i) : x_i \in R^p, y_i \in R, i = 1,...,m \right\} \quad (3.1)$$

Where:

x = input vector consisting a user's attributes
y = {authorized user, intruder}

We want to map the input set x to an output class y.

The solution to the above problem is to find a mapping function from the p-dimensional input space to the 1-dimensional output space. From a modeling perspective, we seek a model that provides the best fit to training data and the best prediction on future data while minimizing model complexity. The resulting model would be employed to predict output values y' for future observed inputs x' where only the inputs x' would be available.

To accomplish the above objective, we need to come up with a model and train it prior to using that model for intrusion detection.

During the training phase, for each input data vector *x*, we already know the associated output *y* and the desired output *d*. This desired output is compared with the actual network output *y*. That is,

d = desired output
y = actual output

Thus, the error of our model is:

e = d-y

In an ideal situation, *'e'* is equal to zero. Our objective is to minimize the error term *'e'* to improve our model. Neural Network first undergoes training from a set of training data.

Back Propagation Method: The back propagation method is a technique used in training multilayer neural networks in a supervised manner. The back propagation method, also known as the error back propagation algorithm, is based on the error-correction learning rule. It consists of two passes through the different layers of the network: a forward pass and a backward pass. In the forward pass, an activity pattern is applied to the input nodes of the network and its effect propagates through the network layer by layer. Finally, a set of outputs is produced as the actual response of the network.

During the forward pass the synaptic weights of the networks are all fixed. During the backward pass, the synaptic weights are all adjusted in accordance with an error-correction rule. The actual response of the network is subtracted from a desired response to produce an error signal. This error signal is then propagated backward through the network. The synaptic weights are adjusted to make the actual response of the network move closer to the desired response in a statistical sense. The weight adjustment is made according to the generalized delta rule to minimize the error. An example of a multilayer perceptron with two hidden layers is shown in Figure 1.

Module Explanation: Creation of Grid Environment*:* Node is an entity which contains resources. These resources are accessed homogeneously through the middleware, which also is responsible for controlling access control policies and supporting a service oriented environment.

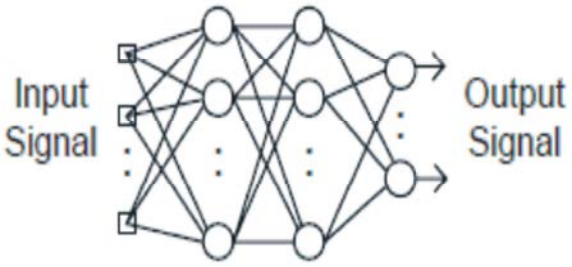

Fig 1: Multilayer Perceptron with Two Hidden Layers

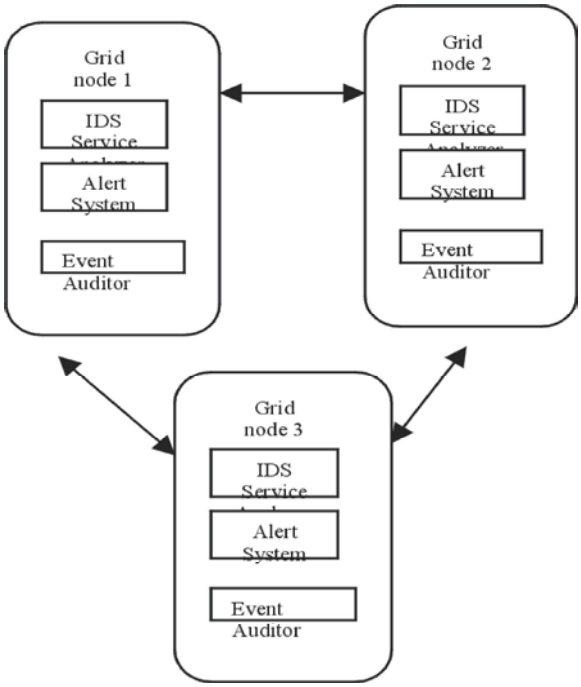

Fig 2: Architecture Diagram

IDS Service*:* The IDS Service is developed to increase a grid security level by the advanced methods of intrusion detection. The behavior-based method dictates how to compare recent user actions to his usual behavior. In this particular case, we need to recognize expected behavior (legitimate use) or a severe deviation of behavior. We focus on identifying user behavioral patterns and deviations from it. With this strategy, we are able to cover a wider range of unknown attacks.

IDS Service analyzes data captured by the auditor and applies detection techniques based on user behavior and knowledge of previous attacks.

The audited data is sent (i) to the IDSService core which starts the behavior analysis task (ii). This task uses artificial intelligence tricks to detect user behavior deviations. With the help of a profile history database (iii), the analyzer is able to determine the distance between

this behavior and the usual one and (iv) communicates this to the IDSService. The rules analyzer receives audit packages (v) and verifies with the policies if any rule in the database (vi) is being broken. The result is returned to the IDSService core (vii). With these responses (iv, vii), the IDS calculates the probability that the action represents an attack. The other nodes are alerted if the probability is high enough.

Event Auditor: To perform analysis for intrusion detection, audit data describing the state of the environment and the messages being exchanged is needed. The event auditor allows the monitoring of data being accessed by the analyzers. The first component monitors message exchange between nodes.

All the requests received by a node and their corresponding responses and other messages are captured by the communication auditor. The capturing of this data is fundamental for behavior analysis.

For each action performed by a node a log entry is generated to register the methods and parameters invoked during the action.

In the experiments with the Behavior-based Intrusion Detection System we considered the use of audit data from a log and a communication system, but the data from a log system, with the exception of the message element, has a limited set of values with little variation. The evaluation of the behavior-based technique was performed with artificial intelligence enabled by a feed forward neural network. In the simulation environment we have considered 5 users as intruders and 5 users as legitimate ones.

The neural network training initiated with a data set representing 10 days of usage simulation. Using this data resulted in a high number of false negatives, besides a high level of uncertainty. As the sample period was increased in the learning phase, also the outputs got nearer the expected results.

Result Analysis

Topology Creation: Fig.3 shows the creation of nodes (topology generation) in a distributed grid environment.

Signal Transmission: Fig.4 shows how data and signals are transferred between nodes in a distributed grid environment.

Conclusion and Future Work:

Conclusion: In this work we have described a grid computing intrusion detection system capable of identifying unknown attacks, such as malicious usage through behavior deviation and known attacks, with the help of a rule database that defines typical attacks. Our solution is an IDS service that captures audit data from a log and a communication part of a middleware increasing the level of security in each node, as well as the entire environment. Behavior-based intrusion detection was achieved with a feed-forward artificial neural network to recognize patterns of user behavior and indicate abnormal activity. The prototype implementing this solution was demonstrably accurate, with a low rate of false positives and false negatives.

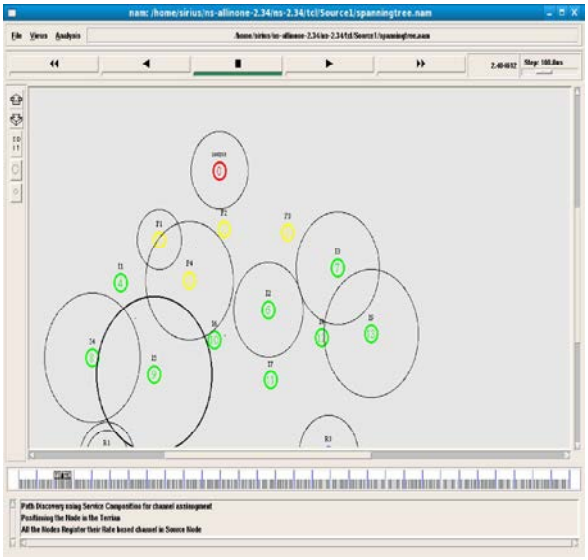

Fig 3: Generation of nodes

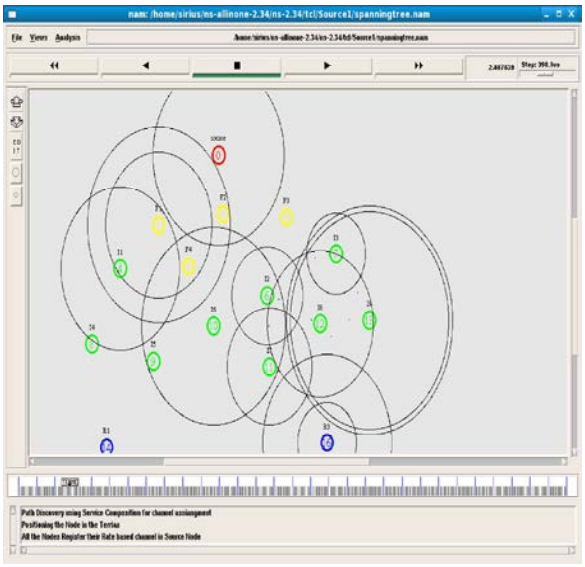

Fig 4: Signal transmission between nodes

Future work: In this phase, topology for nodes in a distributed grid environment is generated and signals and data are made to be passed between them. In the next phase, the intrusion between nodes in grid environment will be detected and protocols such as AODV and DSDV would be implemented to improve the throughput, energy and packet delivery ratio between nodes in a grid environment.

REFERENCES

1. Debar, H., M. Dacier and A. Wespi, 1999. "Towards a taxonomy of intrusion detection systems," Int. J. Computer and Telecommunications Networking, 31(9): 805-822.
2. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing. April, 2009. http://www.cloudsecurityalliance.org/
3. Foster, I., C. Kesselman, G. Tsudik and S. Tuecke, 1998. A Security Architecture for Computational Grids. Proc. 5th ACM Conference on Computer and Communications Security Conference, pp: 83-92.
4. Axelsson, S., 1999. Research in Intrusion-Detection Systems: A Survey. Technical Report TR-98-17, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden, pp: 93.
5. Fang-Yie, L., *et al.*, 2005. Integrating Grid with Intrusion Detection. In: International Conference On Advanced Information Networking And Applications (AINA), 19., 2005, Taipei, Taiwan. IEEE Computer Society, 1: 304-309.
6. Kenny, S. and B. Coghlan, 2005. "Towards a grid-wide intrusion detection system," in Proc. European Grid Conference (EGC2005), Amsterdam, The Netherlands, pp: 275-284.
7. Feng, G., X. Dong, L. Weizhe, L. Chu and J. Li, 2006. GHIDS: Defending Computational Grids against Misusing of Shared Resource. In: Asia- Pacific Conference on Services Computing (APSCC'06).
8. Tolba, M., *et al.*, 2005. Distributed Intrusion Detection System for Computational Grids. In: International Conference On Intelligent Computing And Information Systems, 2., 2005, Cairo, Egypt. ACM.
9. Schulter, A., K. Vieira, Kleber, C.B. Westphall, C.M. Westphall and A. Sekkaki, 0000. Intrusion Dectection for Computational Grids.
10. Franke, H., F. Koch, C. Rolim, C.B. Westphall and D. Balen, 0000. Grid-M: Middleware to Integrate Mobile Devices, Sensors and Grid Computing.