Machine Learning based Anomaly Detection Techniques for Network Intrusion Detection Systems

Pritika Mehra
PG Dept. of Computer Science
Khalsa College for Women
Amritsar, India
mehra_priti@yahoo.com

Sumit Chabbra
PG Dept. of Computer Science
Khalsa College for Women
Amritsar, India
sumitchabbra_12@yahoo.co.in

***Abstract*-Intrusion detection systems (IDSs) are an important component of defensive measures protecting computer systems and networks from abuse. Due to the rising complexity and volume of the attacks in the network, Network Intrusion detection systems are preferred over Host based Intrusion detection systems. NIDS are categorized as misuse network intrusion detection and anomaly detection. Misuse detection systems deal with threats already known in beforehand. On the other hand, anomaly detection systems are more ambitious and try to discover new unknown threats. This paper focuses on anomaly based network intrusion detection systems. Such systems can detect intrusions by using various techniques such as statistical, knowledge based or machine learning. This paper describes a contemporary overview of the machine learning techniques for anomaly based network intrusion detection system.**

***Keywords*: Intrusion detection, Anomaly detection, Machine learning, Bayesian network, Neural Networks**

I. INTRODUCTION

An intrusion is defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. Intrusion Detection Systems (IDS) are security tools that, like other measures such as antivirus software, firewalls and access control schemes, are intended to strengthen the security of information and communication systems. Intrusion Detection Systems can be classified into two categories: Network Intrusion Detection System and Host based Intrusion detection system.

Network intrusion detection system (NIDS) identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. A host-based intrusion detection system (HIDS) consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files) and other host activities and state. A network intrusion by malicious or unauthorized users can cause severe disruption to networks. Therefore the development of a robust and reliable network intrusion detection system (IDS) is increasingly important.

II. Network Intrusion Detection System

Network Intrusion detection systems are classified as either misuse-based or anomaly-based. Misuse intrusion detection uses well-defined patterns of the attack that exploit weaknesses in system and application software to identify the intrusions. These patterns are encoded in advance and used to match against the user behavior to detect intrusion. Anomaly intrusion detection uses the normal usage behavior patterns to identify the intrusion. The normal usage patterns are constructed by using any of the techniques such as statistical, knowledge based, data mining and machine learning. The behavior of the user is observed and any deviation from the constructed normal behavior is detected as intrusion.

However, misuse based methods suffer from their inability to detect new types of attacks. Further-more the database of the signatures is growing as new types of attacks are being detected, which may affect the efficiency of the detection. An anomaly-based IDS examines ongoing traffic, activity, transactions, or behavior for anomalies on networks or systems that may indicate attack. Anomaly based IDS can detect new types of attacks.

Due to the promising capabilities of anomaly-based network intrusion detection systems, this approach is presently a main focus of research and development in the field of intrusion detection

III. Anomaly based NIDS

An anomaly detection technique generally consists of two different steps: the first step is called training phase wherein a normal traffic profile is generated; the second phase is called anomaly detection, wherein the learned profile is applied to the current traffic to look for any deviations. A number of anomaly detection mechanisms have been proposed recently to detect such deviations, which cam be categorized into statistical methods, knowledge based, data-mining methods and machine learning based methods.

In statistical-based techniques, the network traffic activity is captured and a profile representing its stochastic behaviour is created. Statistical anomaly detection has no intelligent learning model which may lead to a high rate of false alarms or may not detect attacks reliably. In knowledge based techniques prior knowledge of usage behaviour is required. Knowledge based Intrusion detection systems encode an expert's knowledge of known patterns of attack and system vulnerabilities as if-then rules. The acquisition of these rules is a tedious and error-prone process. The various problems with statistical and knowledge based methods, has generated a great deal of interest in the application of machine learning techniques to automate the process of learning the patterns. Examples include the Time-based Inductive Machine (TIM) for intrusion detection that learns sequential patterns and neural network-based intrusion detection systems

IV. Machine Learning

Machine learning is an algorithmic method wherein an application automatically learns from the input and the feedbacks to improve its performance over time. Unlike statistical methods, which aims at determining the deviations in traffic features, machine learning based methods aims at detecting anomalies using some mechanism, and then based upon false positive or not, improving the mechanism.

Machine learning, a branch of artificial intelligence, is a scientific discipline concerned with the design and development of algorithms that allow computers to evolve behaviors based on empirical data, such as from sensor data or databases.A major focus of machine learning research is to automatically learn to recognize complex patterns and make intelligent decisions based on data.

V. Machine Learning techniques to implement Anomaly based NIDS

Here we discuss four machine learning techniques that can be used for anomaly detection: Bayesian network, Inductive learning, instance based learning, neural network.

a. Bayesian network

A Bayesian network (BN) is used to build an automatic intrusion detection model and signal an intrusion when a suspicious activity is noticed. They are probabilistic models very helpful when facing problems that require predicting the outcome of a system consisting of a high number of interrelated variables. After a training period, the Bayesian network *learns* the behaviour of the model and, thereafter it is able to foresee its outcome.

A Bayesian network is a graphic representation of the joint probability distribution function over a set of variables. The network structure is represented as a Directed Acyclic Graph (DAG) in which each node corresponds to a random variable and each edge indicates a dependent relationship between connected variables. Each variable (node) in a BN is associated with a Conditional Probability Table (CPT), which enumerates the conditional probabilities for this variable given all the combinations of its parents' values [6]. Therefore, for a BN, the DAG captures causal relationships among random variables, and CPTs quantify these relationships. Since individual events in an attack can be represented as nodes and the causal relations between events can be modeled as edges in Bayesian networks, we use a BN as our inference model. A BN model is capable of learning causal relationships from an existing dataset and predicting the consequences of an intervention in the problem domain.A BN is an ideal model for combining prior knowledge with new data and inferring posterior knowledge.

Formally, let a Bayesian Network *B* be defined as a pair, *B* = (*D*, *P*), where *D* is a directed acyclic graph;

$$P = \{p(x_1|\Psi_2), ..., p(x_n|\Psi_n)\}$$

is the set composed of *n* conditional probability functions (one for each variable); and Ψ_i is the set of parent nodes of the node *Xi* in *D*. The set *P* is defined as the *joint probability density function[5]:*

$$P(x) = \prod_{i=1}^{n} p(x_i|\Psi_i)$$

This is based on the Baye's Theorem which adjusts the probabilities as new information on evidences appears. According to its classical formulation, given two events A and B, the conditional probability *P*(*A*|*B*) that A occurs if B occurs can be obtained if we know the probability that A occurs, P(A), the probability that B occurs, *P*(*B*), and the conditional probability of B given A, *P*(*B*|*A*) (as shown in equation below):

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$$

The main problem of using bayeisan network in IDS is the computational difficulty of exploring a previously unknown network. To calculate the probability of any branch of the network, all branches must be calculated. The advantage of Bayesian networks is that they improve the aggregation of different model outputs and allow one to effortlessly incorporate additional information into an already existing model. Johansen et al. [7] believe that a Bayesian system provides a solid Mathematics foundation to simplify a seemingly difficult and monstrous problem that today's IDS implementations fail to solve. They added that Bayesian network IDS differentiate between attacks and the normal network activity by comparing metrics of each network traffic sample.

b. Inductive learning

Inductive learning is an approach to machine learning in which concepts are learned from examples and counterexamples. One requirement for inductive learning is an explicit representation of the characteristics that determine whether an object is an example or counterexample [9]. Time based Inductive Machine (TIM) is an example of inductive learning proposed by Teng, Chen and Lu (1990) [4].TIM discovers temporal sequential patterns in a sequence of events. The temporal patterns represent highly repetitive activities. Rulebase is generated to store the patterns in the form of rules and the rules are modified from the input data using a logical inference called inductive generalization. When applied to intrusion detection, the rules describe the behaviour patterns of either a user or a group of users based on past audit history. Each rule describes a sequential event pattern that predicts the next event from a given sequence of events. An example of a simplified rule produced in TIM is

$$E1 - E2 - E3 \rightarrow (E4 = 95\%; E5 = 5\%),$$

where E1,E2,E3,E4 and E5 are security events. This rule states that if E1 is followed by E2, and E2 is followed by E3, then there is 95% chance (based on previous observation) that E4 will follow and a 5% chance that E5 will follow.

The limitation of TIM is that it only considers the immediately followed relationship between the observed events. The main advantage of this approach is that it has potential of detecting masqueraders based on deviations from the known sequential patterns of a user.

c. Instance based learning

In machine learning, instance-based learning or memory-based learning is a family of learning algorithms that, instead of performing explicit generalization, compare new problem instances with instances seen in training, which have been stored in memory. Instance-based learning is a kind of lazy learning. In artificial intelligence, lazy learning is a learning method in which generalization beyond the training data is delayed until a query is made to the system, as opposed to in eager learning, where the system tries to generalize the training data before receiving queries.It is called instance-based because it constructs hypotheses directly from the training instances themselves.This means that the hypothesis complexity can grow with the data in the worst case, a hypothesis is a list of *n* training items and classification takes *O*(*n*). One advantage that instance-based learning has over other methods of machine learning is its ability to adapt its model to previously unseen data. Where other methods generally require the entire set of training data to be re-examined when one instance is changed, instance-based learners may simply store a new instance or throw an old instance away.A simple example of an instance-based learning algorithm is the k-nearest neighbor algorithm.

d. Neural networks

Neural network (NN) is an information processing system that is inspired by the way biological nervous systems, such as the brain, process information. It is composed of a large number of highly interconnected processing elements (neurons) working with each other to solve specific problems. Each processing element (neuron) is basically a summing element followed by an activation function. The output of each neuron (after applying the weight parameter associated with the connection) is fed as the input to all of the neurons in the next layer. The learning process is essentially an optimization process in which the parameters of the best set of connection coefficients (weighs) for solving a problem are found and includes the following basic steps :

- Present the neural network with a number of inputs (vectors each representing a pattern)

- Check how closely the actual output generated for a specific input matches the desired output.

- Change the neural network parameters (weights) to better approximate the outputs.

Some IDS designers exploit NN as a pattern recognition technique. Pattern recognition can be implemented by using a feed-forward neural network that has been trained accordingly. During training, the neural network parameters are optimized to associate outputs (each output represents a class of computer network connections, like normal and attack) with corresponding input patterns (every input pattern is represented by a feature vector extracted from the characteristics of the network connection record). When the neural network is used, it identifies the input pattern and tries to output the corresponding class. When a connection record that has no output associated with it is given as an input, the neural network gives the output that corresponds to a taught input pattern that is least different from the given pattern [10].

The advantage of neural network technique for NIDS is that it can be trained rapidly, can be trained incrementally, and once trained, can perform fast and accurate classification of its input.

CONCLUSION

Anomaly based Network intrusion detection systems can be benefited by using Bayesian networks for learning and storing the behaviour patterns of the network. The most promising technique is the neural network for anomaly detection and the research on applying neural networks to anomaly detection is in preliminary stage and more work is needed to confine the potentials of neural networks for intrusion detection systems.

REFERENCES

[1] Crina Gro¸san, Ajith Abraham and Sang Yong Han, MEPIDS: Multi-Expression Programming for Intrusion Detection System

[2] http://www.ids-sax2.com/articles/IntrusionDetectionSystem.htm

[3] http://www1.cse.wustl.edu/~jain/cse571-07/ftp/ids/index.html

[4] H. Teng, K. Chen, and S. Lu, Adaptive real-time anomaly detection using inductively generated sequential patterns, in Proc. IEEE Computer Society Symposium. Research in Security and Privacy, Oakland, CA, May 1990.

[5] Pablo G. Bringas and Igor Santos, Bayesian Networks for Network Intrusion Detection

[6] Alma Cemerlic, Li Yang, Joseph M. Kizza, Network Intrusion Detection Based on Bayesian Networks

[7] K. Johansen, S. Lee. Network Security: Bayesian Network Intrusion Detection (BINDS) May, 2003.

[8] Sailesh Kumar, Survey of Current Network Intrusion Detection Techniques

[9] James P. Callan, Knowledge_Based Feature Generation for Inductive Learning, Ph.D thesis 1993

[10] Mehdi Moradi and Mohammad Zulkernine, A Neural Network Based System for Intrusion Detection and Classification of Attacks

UACEE
Globalize The Research
Localize The World