International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org || PP. 49-54

Layered Approach Using Conditional Random Fields for Intrusion Detection

C.ELAVARASI
Assistant Professor
(Department of Computer Science/ Thiruvalluvar College of Arts and Science,Kurunjipadi)

Abstract: *Intrusion detection faces a number of challenges; an intrusion detection system must reliably detect malicious activities in a network and must perform efficiently to cope with the large amount of network traffic. In this paper, we address these two issues of Accuracy and Efficiency using Conditional Random Fields and Layered Approach. We demonstrate that high attack detection accuracy can be achieved by using Conditional Random Fields and high efficiency by implementing the Layered Approach. Experimental results on the benchmark KDD '99 intrusion data set show that our proposed system based on Layered Conditional Random Fields outperforms other well-known methods such as the decision trees and the naive Bays. The improvement in attack detection accuracy is very high, particularly, for the U2R attacks and the R2L attacks (34.5 percent improvement). Statistical Tests also demonstrate higher confidence in detection accuracy for our method. Finally, we show that our system is robust and is able to handle noisy data without compromising performance.*

Keywords: *Detection, Intrusion, Layered Approach, Random Fields U2R, R2L.*

I. Introduction

Intrusion detection as defined by the Sys Admin, Audit, Networking, and Security (SANS) Institute is the art of detecting inappropriate, inaccurate, or anomalous activity. Today, intrusion detection is one of the high priority and challenging tasks for network administrators and security professionals. More sophisticated security tools mean that the attackers come up with newer and more advanced penetration methods to defeat the installed security systems and. Thus, there is a need to safeguard the networks from known vulnerabilities and at the same time take steps to detect new and unseen, but possible, system abuses by developing more reliable and efficient intrusion detection systems.

Any intrusion detection system has some inherent requirements. Its prime purpose is to detect as many attacks as possible with minimum number of false alarms, i.e., the system must be accurate in detecting attacks. However, an accurate system that cannot handle large amount of network traffic and is slow in decision making will not fulfill the purpose of an intrusion detection system. We desire a system that detects most of the attacks, gives very few false alarms, copes with large amount of data, and is fast enough to make real-time decisions.

II. Literature Review

Conditional models are probabilistic systems which are used to model the conditional distribution over a set of random variables. Such models have been extensively used in natural language processing tasks and computational biology. Conditional models offer a better framework as they do not make any unwarranted assumptions on the observations and can be used to model rich overlapping features among the visible observations. Maxent classifiers, maximum entropy Markov models, and conditional random fields are such conditional models.The simplest conditional classifier is the Maxent classifier based upon maximum entropy classification which estimates the conditional distribution of every class given the observations[1].

Intrusion Detection Systems (IDSs) are proliferating throughout corporate, government, and academic computer network .Intrusion detection is not an emerging research field. It is a well-established commercial area with several large competitors like Cisco and network associates. Admittedly, IDS products themselves produce many false positives and do not detect all known attacks. However, the development of IDS product is likely to parallel the past development anti-virus software. Original anti-virus software created an alarm every time user created new files. The anti-virus software is running and they have confidence that it detects all known viruses [2].

Attack tool developers are using more advanced techniques them previously. Attack tool signatures are more difficult to discover through analysis and more difficult to detect through signature-based systems such as antivirus software and intrusion detection systems [3].

A distributed intrusion detection system (IDS), based on mobile agents, that detects intrusion from outside the network segment as well as from inside. Remote sniffers are controlled by the IDS via mobile agents, which gather intrusion detection data send back to the main station for analysis. The system shows a superior performance compared to central sniffing IDSs that activate too many sniffers causing bottlenecks in the network [4].

The prospect of maintaining a single system which can be used to detect network wide attacks make network monitoring a preferred option as opposed to monitoring individual hosts in a large network. A number of techniques such as association rules, clustering, naive Bays classifier, support vector machines, genetic algorithms, artificial neural networks and others have been applied to detect intrusions at network level. It is important to note that different methods are based on specific assumptions and analyze different properties in the audit patterns, resulting in different attack detection capabilities [5].

Data mining and machine learning methods focus on analyzing the properties of the audit patterns rather than identifying the process which generated. These methods include approaches for mining association rules, classification and cluster analysis. Classification methods are one of the most researched and include methods like the decision trees, Bayesian classifiers, artificial neural networks, k-nearest neighbor classification, support vector machines and many others. Clustering – Clustering of data has been applied extensively for intrusion detection using a number of methods such as k-means, fuzzy c-means and others. Clustering methods are based upon calculating the numeric distance of a test point from different cluster centre's and then adding the point to the closest cluster. One of the main drawbacks of clustering technique is that since a numeric distance measure is used, the observations must be numeric. Observations with symbolic features cannot be readily used for clustering which results in inaccuracy [6].

Artificial Neural Networks – Neural networks have been used extensively to build network. Intrusion detection systems . Though, the neural networks can work effectively with noisy data, like other methods, they require large amount of data for training and it is often hard to select the best possible architecture for the neural network [7].

III. Layered Framework For Intrusion Detection

Layered Framework was introduced for building intrusion detection systems which can be used, for example, as a network intrusion detection system and can detect a wide variety of attacks reliably and efficiently when compared to the traditional network intrusion detection systems. The layered framework, use a number of separately trained and sequentially arranged sub systems in order to decrease the number of false alarms and increase the attack detection coverage. In particular the layered framework has the following advantages:

- The framework is customizable and domain specific knowledge can be easily incorporated to build individual layers which help to improve accuracy.
- Individual intrusion detection sub systems are light weight and can be trained separately.
- Different anomaly and hybrid intrusion detectors can be incorporated in our framework.
- The framework not only helps to detect an attack but it also helps to identify the type of attack. As a result, specific intrusion response mechanisms can be initiated automatically reducing the impact of an attack.
- The framework is scalable and the number of layers can be increased (or decreased) in the overall framework.

IV. Layered Conditional Random Fields For Network Intrusion Detection

Network monitoring is one of the common and widely applied methods for detecting malicious activities in an entire network. However, real-time monitoring of every single event even in a moderate size network may not be feasible, simply due to the large amount of network traffic. As a result, it is only possible to perform pattern matching using attack signatures which may at best detect only previously known attacks. Anomaly based systems result in dropping audit data when they are used to analyze every event. As a result, network monitoring often involves analyzing only the summary statistics from the audit data. The summary statistics may include features of a single TCP session between two IP addresses or may include network level features such as the load on sever, number of incoming connections per unit time and others. Such statistics are represented in the KDD 1999 data set The Layered Conditional Random Fields which can be used to build accurate anomaly intrusion detection systems which can operate efficiently in high speed networks. In particular, the system has the following advantages:

- The attack detection accuracy improves for individual sub systems when using conditional random fields.
- The overall system has wide attack detection coverage, where every sub system is trained to detect attacks belonging to a single attack class.
- Attacks can be detected efficiently in high speed networks.
- The system is robust to noise and performs better than any other compared system.

V. Intrusion Detection And Intrusion Detection System

The intrusion detection systems are a critical component in the network security arsenal. Security is often implemented as a multi layer infrastructure and different approaches for providing security can be categorized into the following six areas

1. Attack Deterrence – Attack deterrence refers to persuading an attacker not to launch an attack by increasing the perceived risk of negative consequences for the attacker. Having a strong legal system may be helpful in attack deterrence.. Spoofing refers to sending IP packets with modified source IP address so that the true sender of the packet cannot be traced.)
2. Attack Prevention – Attack prevention aims to prevent an attack by blocking it before an attack can reach the target. However, it is very difficult to prevent all attacks. This is because to prevent an attack, the system requires complete knowledge of all possible attacks as well as the complete knowledge of all the allowed normal activities which is not always available. An example of attack prevention system is a firewall.
3. Attack Deflection – Attack deflection refers to tricking an attacker by making the attacker believe that the attack was successful though, in reality, the attacker was trapped by the system and deliberately mad e to reveal the attack. Research in this area focuses on attack deflection systems such as the honey pots.
4. Attack Avoidance – Attack avoidance aims to make the resource unusable by an attacker even though the attacker is able to illegitimately access that resource. An example of security mechanism for attack avoidance is the use of cryptography. Encrypting data renders the data useless to the attacker, thus, avoiding possible threat.
5. Attack Detection – Attack detection refers to detecting an attack while the attack is still in Progress or to detect an attack which has already occurred in the past. Detecting an attack is significant for two reasons; first the system must recover from the damage caused by the attack and second, it allows the system to take measures to prevent similar attacks in future. Research in this area focuses on building intrusion detection systems.
6. Attack Reaction and Recovery – Once an attack is detected, the system must react to an attack and perform the recovery mechanisms as defined in the security policy. Tools available to perform attack detection followed by reaction and recovery are known as the intrusion detection systems.

Components of Intrusion Detection Systems

An intrusion detection system typically consists of three sub systems or components:

1. Data Preprocessor – Data preprocessor is responsible for collecting and providing the audit data (in a specified form) that will be used by the next component (analyzer) to make a decision. Data preprocessor is concerned with collecting the data from the desired source and converting it into a format that is comprehensible by the analyzer. Background Data used for detecting intrusions range from user access patterns (for example, the sequence of commands issued at the terminal and the resources requested) to network packet level features (such as the source and destination IP addresses, type of packets and rate of occurrence of packets) to application and system level behavior (such as the sequence of system calls generated by a process.) We refer to this data as the audit patterns.

2. Analyzer (Intrusion Detector) – The analyzer or the intrusion detector is the core component which analyzes the audit patterns to detect attacks. This is a critical component and one of the most researched. Various pattern matching, machine learning, data mining and Statistical techniques can be used as intrusion detectors. The capability of the analyzer to detect an attack often determines the strength of the overall system.

3. Response Engine – The response engine controls the reaction mechanism and determines how to respond when the analyzer detects an attack. The system may decide either to raise an alert without taking any action against the source or may decide to block the source for a predefined period of time. Such an action depends upon the predefined security policy of the network. The authors define the Common Intrusion Detection Framework (CIDF) which recognizes a common architecture for intrusion detection systems. The CIDF defines four components that are common to any intrusion detection system. The four components are; Event generators (Eboxes), event Analyzers (A-boxes), event Databases (D-boxes) and the Response units (R-boxes). The additional component, called the D-boxes, is optional and can be used for later analysis.

A. Layered Approach For Intrusion Detection

The goal of using a layered model is to reduce computation and the overall time required to detect anomalous events. The time required to detect an intrusive event is significant and can be reduced by eliminating the communication overhead among different layers. This can be achieved by making the layers autonomous and self-sufficient to block an attack without the need of a central decision-maker. Every layer in the LIDS framework is trained separately and then deployed sequentially.

Each layer is then separately trained with a small set of relevant features. Feature selection is significant for Layered Approach and discussed in the next section. In order to make the layers independent, some features may be present in more than one layer. The layers essentially act as filters that block any

One Day National Conference On "Internet Of Things - The Current Trend In Connected World" NCIOT-2018 51 | Page

anomalous connection, thereby eliminating the need of further processing at subsequent layers enabling quick. Our second goal is to improve the speed of operation of the system. Hence, we implement the LIDS and select a small set of features for every layer rather than using all the 41 features. This results in significant performance improvement during both the training and the testing of the system. In many situations, there is a trade-off between efficiency and accuracy of the system and there can be various avenues to improve system performance.

The CRFs that are more accurate, though expensive, but we implement the Layered Approach to improve overall system performance. The performance of our proposed system, Layered CRFs, is comparable to that of the decision trees and the naive Bayes, and our system has higher attack detection accuracy.

B. Integrating Layered Approach With Conditional Random Field

The CRFs can be effective in improving the attack detection accuracy by reducing the number of false alarms, while the Layered Approach can be implemented to improve the overall system efficiency. Hence, a natural choice is to integrate them to build a single system that is accurate in detecting attacks and efficient in operation.

Feature Selection:

Probe Layer

- The probe attacks are aimed at acquiring information about the target network from a source that is often external to the network. Hence, basic connection level features such as the “duration of connection” and “source bytes” are significant while features like “number of files creations” and “number of files accessed” are not expected to provide information for detecting probes.

DoS Layer

The DoS attacks are meant to force the target to stop the service(s) that is (are) provided by flooding it with the DoS layer, traffic features such as the “percentage of connections having same destination host and same service” and packet level features such as the “source bytes” and “percentage of packets with errors” are significant. To detect DoS attacks, it may not be important to know whether a user is “logged in or not.”

R2L Layer

The R2L attacks are one of the most difficult to detect as they involve the network level and the host level features. We therefore selected both the network level features such as the “duration of connection” and “service requested” and the host level features such as the “number of failed login attempts” among others for detecting R2L attacks.

U2R Layer

The U2R attacks involve the semantic details that are very difficult to capture at an early stage. Such attacks are often content based and target an application. Hence, for U2R attacks, we selected features such as “number of file creations” and “number of shell prompts invoked,” while we ignored features such as “protocol” and “source bytes.”

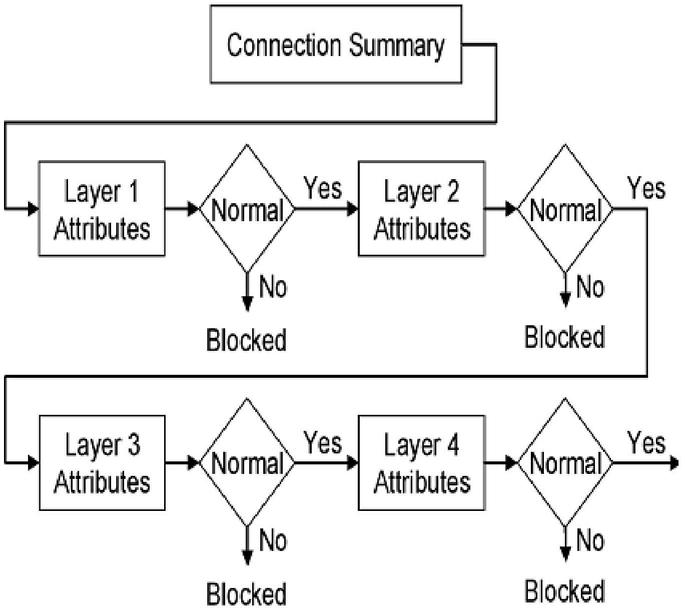

Fig 1: Integrating Layered Approach

Each layer is then separately trained with a small set of relevant features. Feature selection is significant for Layered Approach and discussed in the next section. In order to make the layers independent, some features may be present in more than one layer. The layers essentially act as filters that block any anomalous connection, thereby eliminating the need of further processing at subsequent layers enabling quick.

VI. Conclusion

In this thesis, explored the suitability of conditional random fields for intrusion detection systems which can operate, both, at the network and at the application level. In particular, we introduced novel frameworks and developed models which address three critical issues that severely affect the large scale deployment of present anomaly and hybrid intrusion detection systems in high speed networks. The three issues are:
1. Limited attack detection coverage
2. Large number of false alarms and
3. Inefficiency in operation

Other issues such as the scalability and ease of system customization, robustness of the system to noise in the training data, availability of training data, and the ability of the system to detect disguised attacks were also addressed. As a result of this research, we conclude that:

1. Layered framework can be used to build efficient intrusion detection systems. In addition, the framework offers ease of scalability for detecting different variety of attacks as well as ease of customization by incorporating domain specific knowledge. The framework also identifies the type of attack and, hence, specific intrusion response mechanism can be initiated which helps to minimize the impact of the attack.
2. Conditional random fields are a strong candidate for building robust and efficient intrusion detection systems. Integrating the layered framework with the conditional random fields can be used to build effective and efficient network intrusion detection systems. Using conditional random fields as intrusion detectors result in very few false alarms and, thus, the attacks can be detected with very high accuracy.

Directions For Future Research

The critical nature of the task of detecting intrusions in networks and applications leaves no margin for errors. The effective cost of a successful intrusion overshadows the cost of developing intrusion detection systems and hence, it becomes critical to identify the best possible approach for developing better intrusion detection systems.

Every network and application is custom designed and it becomes extremely difficult to develop a single solution which can work for every network and application. In this thesis, proposed novel frameworks and developed methods which perform better than previously known approaches. However, in order to improve the overall performance of our system we used the domain knowledge for selecting better features for training our models. This is justified because of the critical nature of the task of intrusion detection.

References

[1] K.K. Gupta, B. Nath, and R. Kotagiri," Conditional Random Fields for Intrusion Detection," Proc.21st Int'l Conf. Advanced Information Networking and Applications Workshops (AINAW'07), PP.203-208, 2007.

[2] K.K .Gupta, B. Nath, and R. Kotagiri, "Network Security Framework," Int'l J. Computer Science and Network Security,vol.6,no.7B,PP.151-157,2006.

[3] R. Bace and P. Mell, Intrusion Detection Systems, Computer Security Division, Information Technology Laboratory, Nat'l Inst.of Standards and Technology, 2001.

[4] C.Kruegel, D.Mutz, w.Robertson, and F.Valeur,"Bayesian Event Classification for Intrusion Detection,"Proc.19th Ann.Computer Security Applications Conf. (ACSAC'03), pp.14-23, 2003.

[5] T. Abraham, IDDM: Intrusion Detection Using Data Mining Techniques, http://www.dsto.defence./gov.au/publications/2345/DSTO-GD-0286.pdf, 2008.

[6] N.B. Amor, S. Benferhat, and Z. Elouedi, "Naive Bayes vs. Decision Trees in Intrusion Detection Systems," Proc. ACM Symp. Applied Computing (SAC '04), pp. 420-424, 2004.

[7] D. Boughaci, H. Drias, A. Bendib, Y. Bouznit, and B. Benhamou, "Distributed Intrusion Detection Framework Based on Mobile Agents," Proc. Int'l Conf. Dependability of Computer Systems (DepCoS-RELCOMEX '06), pp. 248-255, 2006.

[8] K.K.Gupta, B.Nath, R.Kotagiri,and A.Kazi,"Attacking Confedentiality:An Agent Based Approach,"Proc.IEEE Int'l Conf.Intelligence and Security Informatics(ISI'06),2006.. (8)

[9] P.O. Bishop, Neurophysiology of binocular vision, in J.Houseman (Ed.), *Handbook of physiology*, 4 (New York: Springer-Verlag, 1970) 342-366.