Development of a Layered Conditional Random Field Based Network Intrusion Detection System

Ele, B. I.[1], Mbam, B.C.E. [2]

[1]Department of Computer Science, University of Calabar, Calabar
Cross River State – Nigeria. mydays2020@gmail.com

[2]Department of Computer Science, Michael Okpara Federal University of Agriculture, Umudike
Abia State – Nigeria. quicksuccessng@yahoo.com

Abstract

The rapid proliferation of network systems and mobile computing applications has changed the landscape of network security. The recent denial of service attacks on major Internet sites has shown that no open computer network is immune from intrusions. The inefficiency, inaccuracy and high false alarm rate of existing network security systems posed serious problems to network users, network administrators and security professionals and needs urgent redress. The traditional way of protecting network systems with firewalls and encryption software is no longer sufficient and effective, and there is an urgent need for new architecture and mechanism to protect network systems and mobile computing applications. Therefore, the purpose of this study is to develop an efficient model of network intrusion detection system using layered framework with conditional random fields that is capable of overcoming the apparent shortcomings of the present network intrusion detection systems. In this paper, the security system was developed using the structured system analysis and design methodology (SSADM). Furthermore, a simple, scalable, customizable and intelligent layered conditional random field based network intrusion detection system (LCRFNIDS) for detecting network based attacks was successfully implemented. This system will play a key role in controlling intruders' activities by detecting network based attacks reliably and efficiently. Specifically, in this system: an automated network monitoring system was implemented for monitoring packet broadcast from unauthorized internet protocol (IP) addresses, usual packet size, unauthorized packet transmission and packet broadcast to unauthorized IP addresses In general, the developed system was tested and found to be very effective for detecting and alerting intruder's activities in the network systems in order to establish a secured network system that will enhance business continuity and preserve organizations' vital and sensitive information. The result of this study will help to proactively address potential security vulnerabilities by detecting attacks and security policy violations reliably and efficiently in network systems.

Keywords: layered framework, conditional random fields, layered conditional random fields, network intrusion detection system, intrusion detection techniques, security vulnerabilities, intrusion detection system, network security system

1. Introduction

Network security system has been a major concern since computer networks evolved. Since the evolution of the internet, there has been an increasing need for effective network security systems. Hazem and Nikod stated that one important type of security software that has emerged since the evolution of the internet is intrusion detection system (IDS) in [1]. They further asserted that network intrusion detection systems (NIDSs) are the most efficient way of defending against network-based attacks aimed at computer systems. In [2], the authors asserted that network intrusion detection systems are used in almost all large-scale information technology infrastructures.

According to the authors in [3], the problem of detecting intrusions, anomalies, and other forms of computer abuses can be viewed as finding non-permitted deviations or security violations of the characteristic properties in the monitored network systems. This assumption is based on the fact that intruders' activities must be different in some ways from the normal users' activities. However, in most situations, it is very difficult to realize and detect such differences before any damage occurs during break-ins.

The widespread use of information stored and processed on network-based systems in most businesses and their associated vulnerabilities have increased the necessity for protecting these systems, and most businesses are constantly experiencing new threats and vulnerabilities in their applications. Therefore, trying to keep up with emerging threats, applying patches against known vulnerabilities, updating antivirus software, updating firewall rules and all of the other security measures can have a network or security administrator working 24 hours a day, 7 days a week, 365 days a year with no vacation [4]. Thus, there is a crucial need to address security issues that affect networks. It is equally vital to be able to carefully examine the mountains of potential threats and determine which ones truly affect the network so that time and resources can be put to the most efficient use.

However, Intrusion Detection Systems (IDSs) are now an essential component in the overall network and information security arsenal. An intrusion detection system (IDS) is a device or software application that monitors network and system activities for malicious activities or policy violations and produce reports to a management station [5]. Detecting intrusions in networks and applications has become one of the most critical tasks to prevent their misuse by attackers. The cost involved in protecting these valuable resources is often negligible when compared with the actual cost of a successful intrusion, which strengthens the need to develop more powerful network intrusion detection system. Intrusion detection started in 1980's and since then a number of approaches have been introduced to build intrusion detection systems [6] and [7]. According to Kapil, Baikunth, Kotagiri, and Ashraf [8], intrusion detection is still at its infancy and naive attackers can launch powerful attacks which can bring down an entire network. They further noted that the rapid advancement in the network technologies including higher bandwidths and ease of connectivity of wireless and mobile devices has changed the focus of intrusion detection from simple signature matching approaches to detecting attacks based on analyzing contextual information which can be specific to individual networks and applications. As a result, anomaly and hybrid intrusion detection approaches have gained significance, however, present anomaly and hybrid detection approaches suffer three major setbacks; limited attack detection coverage, large number of false alarms and inefficiency in operation. Therefore, the purpose of this paper is to develop an efficient model of network intrusion detection system using layered approach with conditional random fields that is capable of overcoming the apparent shortcomings of the present anomaly and hybrid network intrusion detection systems.

2. Problem Definition

There exist various problems that induce the complexity of detection systems such as low detection accuracy, unbalanced detection rates for different attack types and high false alarms.

Present networks and applications are drastically faced with three significant factors which severely restrict the utility of present anomaly and hybrid intrusion detection systems. The three factors are; limited attack detection coverage, large number of false alarms and inefficiency in operation.

Present anomaly and hybrid intrusion detection systems have limited attack detection capability, suffer from a large number of false alarms and cannot be deployed in high speed networks and applications without dropping audit patterns. Hence, most existing network intrusion detection systems such as Bro, Snort and others are developed using knowledge engineering approaches where domain experts can build focused and optimized pattern matching models [6].

It is true that such systems result in very few false alarms, but are specific in attack detection and often tend to be incomplete. As a result, their effectiveness is limited. Furthermore, due to their manual development process, signature based systems are expensive and slow to build. Thus, this paper addresses these apparent shortcomings and develops a better model of network intrusion detection system using layered conditional random fields, which is accurate in attack detection, efficient in operation and has wide attack detection coverage.

3. Intrusion Detection System (IDS) Overview

An intrusion is when anyone, usually a hacker, attempts to break into or misuse a computer system. An Intrusion Detection System (IDS) is a system for detecting such intrusions. A network IDS will continually monitor packets on a network wire and attempt to discover whether a break into the system has been attempted. The IDS can also try to determine other intrusions such as an attempt to cause a 'denial of service' attack to freeze the ability of the network to handle data traffic. In some cases, IDS may be able to respond to anomalous or malicious traffic by taking action, such as reconfiguring a remote firewall in order to block a user's IP address or port from gaining access into a network.

SANS Institute [9] defined intrusion detection as the act of detecting inappropriate, inaccurate or anomalous activity. The mechanism responsible for this task is known as intrusion detection system.

Intrusion can be defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. Intrusion leads to violations of the security policies of a computer system, such as unauthorized access to private information, malicious break-in into a computer system, or rendering a system unreliable or unusable [10].

IDS can run on the target machine watching its own traffic (host-based), usually integrated with the stack and services themselves. Only packets from the device are monitored and they will provide alerts when suspicious activity is detected. Alternatively, IDS can run on an independent machine promiscuously watching all network traffic (network-based). The IDSs are placed at strategic points within the network to provide maximum monitoring of all inbound and outbound traffic. There are IDSs that detect intrusions based on specific signatures of known malicious threats - similar to how most antivirus software protect against malware. On the other hand, there are IDSs that detect intrusion based on comparing traffic patterns against a baseline and looking for anomalies. The baseline will identify what can be considered "normal" for that network, and that includes protocols, services, ports and IPs used. This type of IDS will alert against traffic that are anomalous, or significantly different, from the established baseline [11]. Additionally, there are passive IDSs and reactive IDSs. Passive IDS simply detects intrusion and alerts the appropriate personnel, who will decide which actions to take next. Reactive IDS will not only detect suspicious network traffic, but will also take pre-defined proactive actions as a response to the detected intrusion. Typically, this reaction involves blocking any further network traffic from the IP address or user of the network connection.

Best practices for securing a network include a need to implement IDS in order to monitor inbound and outbound traffic in the network. IDS can identify suspicious and malicious traffic which has somehow managed to bypass the firewall. In addition, IDS will be able to detect intrusion that originates from inside the network.

A full-blown network security system should include the following subsystems:

- **Intrusion Detection Subsystem:** Distinguishes a potential intrusion from a valid network operation.
- **Protection Subsystem:** Protects the network and security system itself from being compromised by the network intrusions.
- **Reaction Subsystem:** This part either traces down the origin of an intrusion or fights back the hackers.

The focus of this paper is on the intrusion detection subsystem, which constitutes the first line of defense for a computer network system. There are a number of approaches in this field. Most of them fall into three primary categories: anomaly detection, misuse detection and hybrid detection.

The anomaly detection approach is based on a model of normal activities in the system. This model can either be predefined or established through techniques such as machine learning. Once there is a significant deviation from this model, an anomaly will be reported. By contrast, a misuse detection approach defines specific user actions that constitute a misuse and uses rules for encoding and detecting known intrusions [12]. The hybrid detection approach uses a combination of anomaly and misuse detection techniques.

Intrusion detection system is a critical component in the network security arsenal. Security is often implemented as a multilayer infrastructure and different approaches for providing security can be categorized into the following six areas [13]:

i) 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. However, it requires strong evidence against the attacker in case an attack was launched. Research in this area focuses on methods such as those discussed in [14] which can effectively trace the true source of attack as very often the attacks are launched with spoofed source IP address.

ii) 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 [15].

iii) 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 made to reveal the attack. Research in this area focuses on attack deflection systems such as the honey pots [4].

iv) 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 [16].

Encrypting data renders the data useless to the attacker, thus, avoiding possible threat.

v) 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.

vi) **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 intrusion detection systems. However, the difference between intrusion prevention and intrusion detection is slowly diminishing as the present intrusion detection systems increasingly focus on real-time attack detection and blocking an attack before it reaches the target. Such systems are better known as Intrusion Prevention Systems.

4. Review of Related Work

The field of intrusion detection and network security has been around since late 1980s. Since then, a number of methods and frameworks have been proposed and many systems have been built to detect intrusions. Various techniques such as association rules, clustering, naive Bayes classifier, support vector machines, genetic algorithms, artificial neural networks, and others have been applied to detect intrusions. In this section, these techniques and frameworks are briefly discussed.

Lee et al introduced data mining approaches for detecting intrusions in [17], [18] and [19]. Data mining approaches for intrusion detection include association rules and frequent episodes, which are based on building classifiers by discovering relevant patterns of program and user behavior. Association rules and frequent episodes are used to learn the record patterns that describe user behavior [20]. These methods can deal with symbolic data, and the features can be defined in the form of packet and connection details. However, mining of features is limited to entry level of the packet and requires the number of records to be large and sparsely populated; otherwise, they tend to produce a large number of rules that increase the complexity of the system [21].

Data clustering methods such as the k-means and the fuzzy c-means have been applied extensively for intrusion detection in [22] and [23]. One of the main drawbacks of the clustering technique is that it is based on calculating numeric distance between the observations, and hence, the observations must be numeric. Observations with symbolic features cannot be easily used for clustering, resulting in inaccuracy. In addition, the clustering methods consider the features independently and are unable to capture the relationship between different features of a single record, which further degrades attack detection accuracy.

Naive Bayes classifiers have been used for intrusion detection in [24]. However, Naive Bayes classifiers make strict independence assumption between the features in an observation resulting in lower attack detection accuracy when the features are correlated, which is often the case for intrusion detection.

Bayesian network can also be used for intrusion detection in [25]. However, Bayesian network for intrusion detection tend to be attack specific and build a decision network based on special characteristics of individual attacks. Thus, the size of a Bayesian network increases rapidly as the number of features and the type of attacks modeled by a Bayesian network increases. Hidden Markov Models (HMMs) have been applied to detect anomalous traces of system calls in privileged processes [26]. However, modeling the system calls alone does not always provide accurate classification and in such cases, various connection level features are ignored. Furthermore, HMMs are generative systems and fail to model long-range dependencies between the observations [27].

In [24], decision trees are used for building intrusion detection system. The decision trees select the best features for each decision node during the construction of the tree based on some well-defined criteria. One such criterion is to use the information gain ratio, which is used in C4.5. Decision trees generally have very high speed of operation and high attack detection accuracy.

In [28] and [29], the used of artificial neural networks for network intrusion detection are discussed. Though the neural networks can work effectively with noisy data, they require large amount of data for training and it is often hard to select the best possible architecture for a neural network. Also, support vector machines are used for detecting intrusions [29]. Support vector machines map real valued input feature vector to a higher dimensional feature space through nonlinear mapping and can provide real-time detection capability, deal with large dimensionality of data, and can be used for binary-class as well as multiclass classification. Other approaches for detecting intrusion include the use of genetic algorithm and autonomous and probabilistic agents for intrusion detection. These methods are generally aimed at developing a distributed intrusion detection system.

In [30], a framework known as Collaborative Intrusion Detection System (CIDS) which describe the collaborative use of network-based and host-based systems to overcome the weakness of a single intrusion detection system was proposed. Tombini, et al discussed intrusion detection systems that employ both signature-based and behavior-based techniques known as hybrid intrusion detection systems in [31]. In [19], the authors describe a data mining framework for building adaptive intrusion detection models. In [32], the authors discussed distributed intrusion detection framework based on mobile agents.

The most closely related work, to this study, is that of [17], [18] and [19]. They, however, consider a data mining approach for mining association rules and finding frequent episodes in order to calculate the support and confidence of the rules separately. Instead, in this study, features are selected from the observations as well as from the previous labels and sequence labeling performed via the conditional random fields to label every feature in the observation. This setting is sufficient for modeling the correlation between different features of an observation.

This study was also compared with that of [33], in their research titled “Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation,” which describes the use of maximum entropy principle for detecting anomalies in the network traffic. The key difference between study in [33] and this study is the high rate of false alarms generated by the system in [33], while the system developed in this study drastically reduced the false alarms to the least minimum, if not completely eliminated. Second, the system developed in [33] fails to model long-range dependencies in the observations, which can be easily represented in the model developed in this study. The study also integrates the Layered Approach with the Conditional Random Fields to gain the benefits of computational efficiency and high accuracy of detection in a single system.

In this study the Layered Approach will be compared with the studies in [31], [34] and [35]. In [31], the authors apply a combination of anomaly and misuse detectors for better qualification of analyzed events. In [34], the authors use a combination of “weak” classifiers. The individual classification power of weak classifiers is slightly better than random guessing. The authors show that a number of such classifiers when combined using simple majority voting mechanism, provide good classification. The authors in [35] describe the combination of “strong” classifiers using stacking, where the decision tress, naive Bayes, and a number of other classification methods are used as base classifiers. The authors show that the output from these classifiers can be combined to generate a better classifier rather than selecting the best one. However, this study is not based upon classifier combination. Combination of classifiers is expensive with regard to the processing time and decision making. The purpose of classifier combination is to improve accuracy. Rather, this system is based upon serial layering of multiple detectors. The results from individual classifiers at a layer are not combines at any later stage in the Layered Approach, and hence, an attack can be alerted at the layer where it is detected. There is no communication overhead among the layers and the central decision-maker. In addition, since the layers are independent they can be trained separately and deployed at critical locations in a network depending upon the specific requirements of a network. Using a stacked system will not give the advantage of reduced processing when an attack is detected at the initial layers in the sequential model.

This review shows the effectiveness of Conditional Random Fields (CRFs) and layered framework for building robust network intrusion detection system that is accurate in attack detection and performs efficiently.

5. Layered Framework For Intrusion Detection

The Layered Network Intrusion Detection System (LNIDS) draws its motivation from the Airport Security model, where a number of security checks are performed one after the other in a sequence. Similar to this model, the LNIDS represents a sequential Layered Approach and is based on ensuring availability, confidentiality, and integrity of data and services over a network. Figure 1 below gives a generic representation of the framework

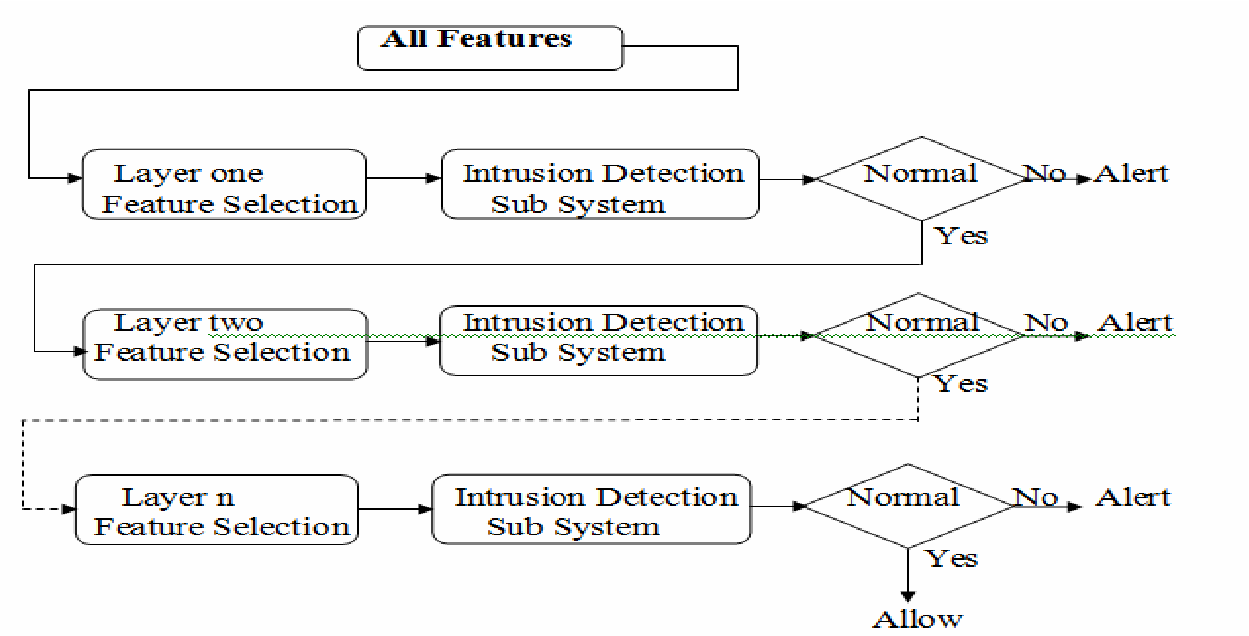

Figure 1: Generic Representation of Layered Network Intrusion Detection System

The goal of using a layered model is to reduce computational complexity 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 alert and block an attack without the need of a central decision-maker. Every layer in the LNIDS framework is trained separately and then deployed sequentially. In this paper, three layers are defined that corresponds to the three attack groups. They are DoS layer, R2L layer, and U2R layer. Each layer is then separately trained with a small set of relevant features. This implies that feature selection is very significant for the Layered Approach. In order to make the layers independent, some features may be present in more than one layer. The layers essentially act as filters that alert and block any anomalous connection, thereby eliminating the need of further processing at subsequent layers enabling quick response to intrusion. The effect of such a sequence of layers is that the anomalous events are identified and alerted as soon as they are detected. The second goal of the layered approach is to improve the speed of operation of the system. 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. Methods such as naive Bayes assume independence among the observed data. This certainly increases system efficiency, but it may severely affect the accuracy. To balance this trade-off, the Conditional Random Fields that are more accurate, though expensive are used, while implementing the Layered Approach to improve overall system performance.

6. Conditional Random Fields for Intrusion Detection

Conditional models are probabilistic systems that are used to model the conditional distribution over a set of random variables. Such models have been extensively used in the natural language processing tasks. 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 [36], maximum entropy Markov models [37], and CRFs [27], are such conditional models. The advantage of CRFs is that they are undirected and are, thus, free from the Label Bias and the Observation Bias [38]. The simplest conditional classifier is the Maxent classifier based upon maximum entropy classification, which estimates the conditional distribution of every class given the observations [36]. The training data is used to constrain this conditional distribution while ensuring maximum entropy and hence maximum uniformity.

CRFs are undirected graphical models used for sequence tagging. The prime difference between CRF and other graphical models such as the HMM is that the HMM, being generative, models the joint distribution, whereas the CRF are discriminative models and directly model the conditional distribution, which is the distribution of interest for the task of classification and sequence labeling.

Similar to HMM, the naive Bayes is also generative and models the joint distribution. Modeling the joint distribution has two disadvantages. First, it is not the distribution of interest, since the observations are completely visible and the interest is in finding the correct class for the observations, which is the conditional distribution. Second, inferring the conditional probability from the modeled joint distribution, using the Bayes rule, requires the marginal distribution. To estimate this marginal distribution is difficult since the amount of training data is often limited and the observation x contains highly dependent features that are difficult to model and therefore strong independence assumptions are made among the features of an observation.

This results in reduced accuracy [39]. CRFs, however, predict the label sequence y given the observation sequence x. This allows them to model arbitrary relationship among different features in an observation x [40]. CRFs also avoid the observation bias and the label bias problems, which are present in other discriminative models, such as the maximum entropy Markov models. This is because the maximum entropy Markov models have a per-state exponential model for the conditional probabilities of the next state given the current state and the observation, whereas the CRFs have a single exponential model for the joint probability of the entire sequence of labels given the observation sequence [27].

The task of intrusion detection can be compared to many problems in machine learning, natural language processing, and bioinformatics. The CRFs have proven to be very successful in such tasks, as they do not make any unwarranted assumptions about the data. Hence, the CRFs are strong candidates for intrusion detection. See figure 2 below for graphical representation of a Conditional Random Field.

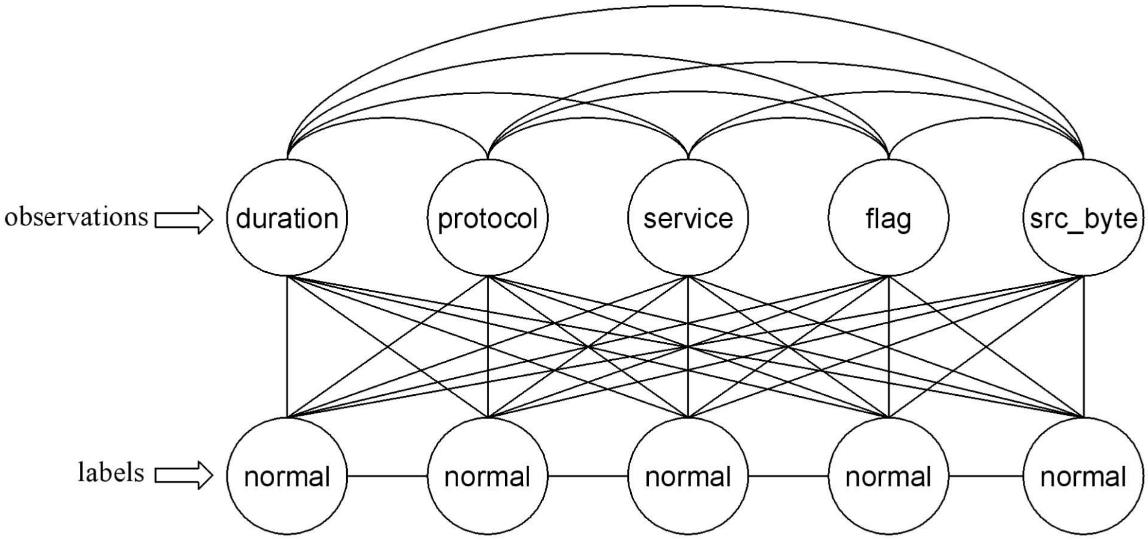

Figure 2: Graphical Representation of a Conditional Random Field

7. Integrating Layered Framework with Conditional Random Field

The two main requirements for an intrusion detection system include accuracy of detection and efficiency in operation. As discussed in Sections 5 and 6, respectively, the Layered framework can be implemented to improve the overall system efficiency, while the CRFs are effective in improving the attack detection accuracy by reducing the number of false alarms. Hence, a natural choice is to integrate the layered framework and conditional random fields to build a single system known as Layered Conditional Random Fields Based Network Intrusion Detection System (LCRFNIDS) that is accurate in detecting network based attacks and efficient in operation.

8. Development Methodology

The methodology adopted for the study and development of this system follows the internationally acceptable standards and ethics of software application development.

In this paper, the structured system analysis and design methodology (SSADM) was adopted for the design of the proposed system. The proposed system was designed using layered framework and conditional random fields, that is, integrating the layered framework with conditional random fields to form layered conditional random fields based network intrusion detection system. In the layered framework, a number of separately trained and sequentially arranged sub-systems are used in order to decrease the number of false alarms and increase the attack detection coverage. The layered framework enhances the building of hybrid network intrusion detection system, which can operates efficiently in high speed networks and can accurately detect a variety of attacks.

The layered conditional random fields will be used to capture the correlations among different features in the data and hence perform better when compared with other methods such as decision trees and naive bayes. This approach enhances the development of an efficient network intrusion detection system

.

9. User Interface Design Of The Proposed System

The user interface design for the proposed system is as shown in figure 3 below:

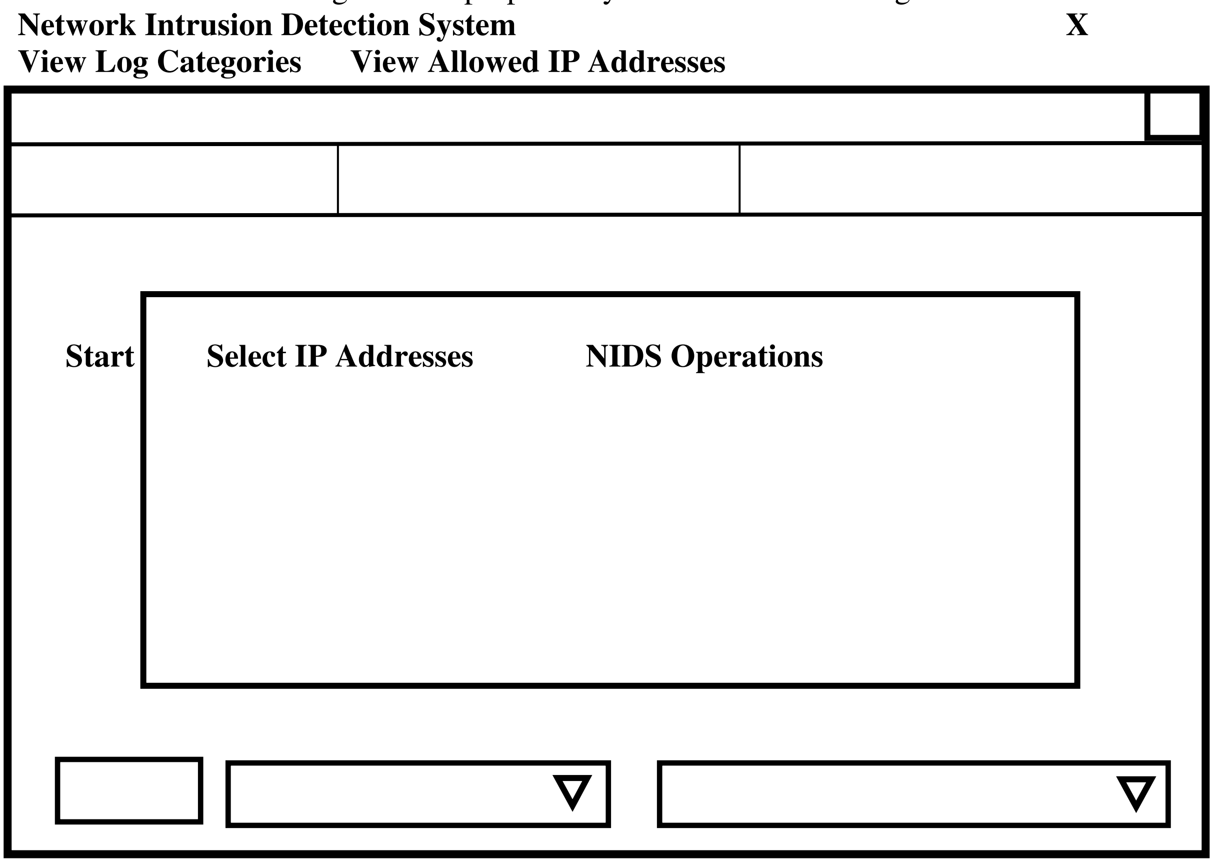

Figure 3: User Interface Design of the Proposed System

The user interface or main window consists of the title of the application (Network Intrusion Detection System) and the close button (X), View Log Categories, View Allowed IP Addresses, Start/Stop, Select IP Addresses, NIDS Operations and the work space. The title of the application is Network Intrusion Detection System. The close button (X) is used to terminate the system if the user or operator is authorized to do so. The View Log Categories consist of the normal traffic log and attack log. All normal network traffics are stored on the traffic log and all attacks detected are stored on the attack log. The start option is used to initiate the system. The Select IP Addresses option is used to select the required IP address or addresses. The NIDS operation option is used to choose NIDS operation to be performed at any point in time and to categorize the nature and type of network attacks, that is, there is an option to select the NIDS operation by simply clicking on the look down triangle in the NIDS operation windows. The operations include monitoring packet broadcast from unauthorized internet protocol (IP) addresses, monitoring unusual packet size, monitoring unauthorized packet transmission and monitoring packet broadcast to unauthorized IP addresses.

10a. Data Flow Diagram of the Proposed Network Security System

Figure 4 below is a level one data flow diagram of the proposed network security system.

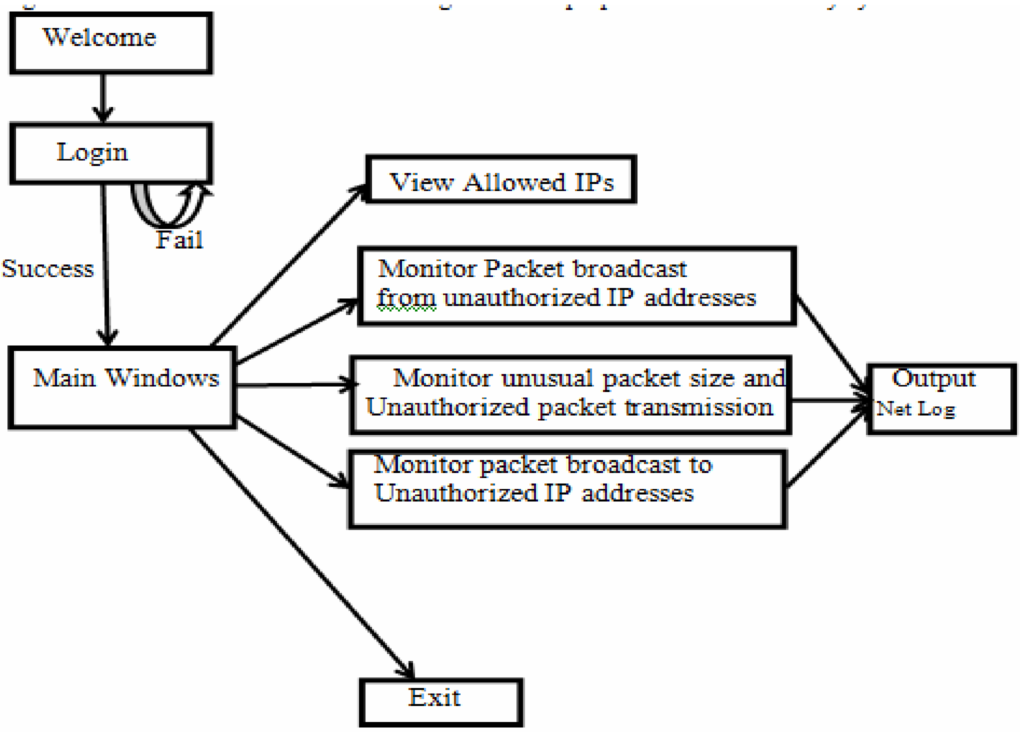
Welcome
Login
Fail
Success
Main Windows
View Allowed IPs
Monitor Packet broadcast from unauthorized IP addresses
Monitor unusual packet size and Unauthorized packet transmission
Monitor packet broadcast to Unauthorized IP addresses
Output
Net Log
Exit

Figure 4: Data Flow Diagram of the Proposed Security System

10b. Data Flow Diagram Demonstrating the Flexibility in Utilizing the Proposed LCRFNIDS

Figure 5 is a data flow diagram demonstrating the flexibility in utilizing the proposed Layered Conditional Random Fields Based Network Intrusion Detection System (LCRFNIDS).

Figure 5: Data Flow Diagram Demonstrating the Flexibility in Utilizing the Proposed LCRFNIDS

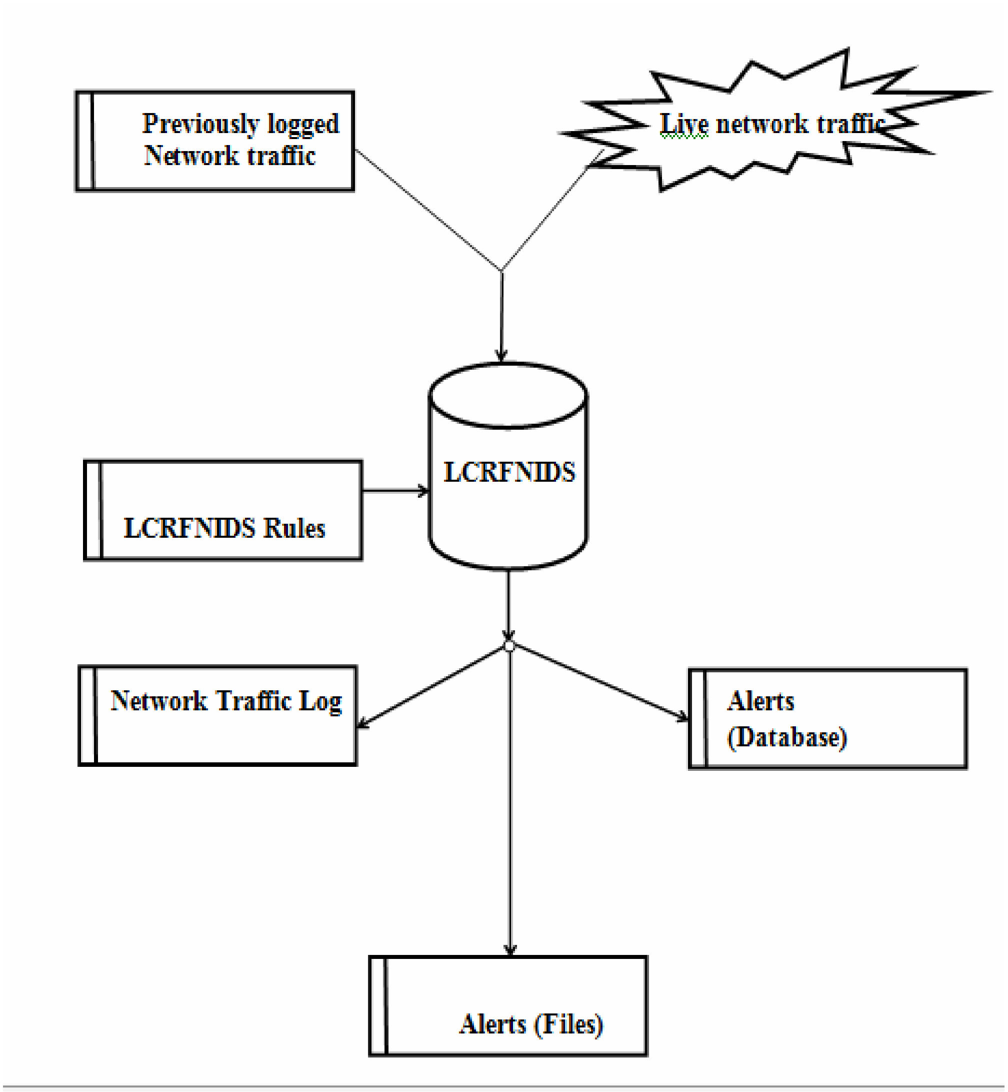

Figure 5: Data Flow Diagram Demonstrating the Flexibility in Utilizing the Proposed LCRFNIDS

11. Flowchart for the Proposed Network Security System

Figure 6 below is a flowchart for the proposed network security system

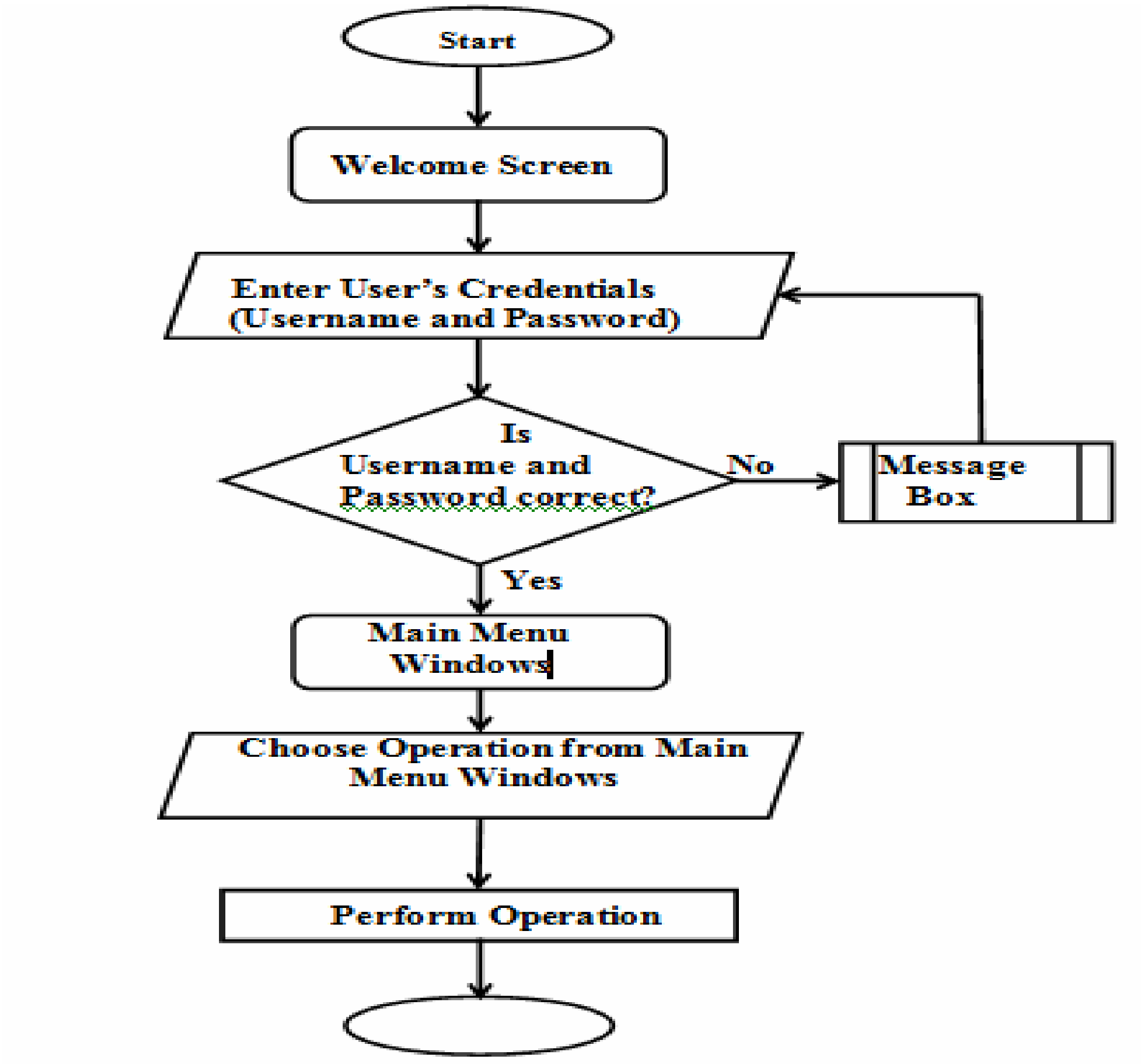
Start
Welcome Screen
Enter User's Credentials (Username and Password)
Is Username and Password correct?
No
Message Box
Yes
Main Menu Windows
Choose Operation from Main Menu Windows
Perform Operation

Figure 6: Flowchart for the Proposed Network Security System

12. Result and Discussion

The result of this study shows that the Layered Conditional Random Fields Based Network Intrusion Detection System (LCRFNIDS) can be very effective in detecting the DoS, the U2R, and the R2L attacks. Feature selection for each layer enhances the performance of the entire system. The runtime performance of the model is comparable with other methods; however, the time required to train the model is slightly higher. It is also observed that feature selection not only decreases the time required to test an instance, but it also increases the accuracy of attack detection. This is because using more features than required can generate superfluous rules often resulting in fitting irregularities in the data, which can misguide classification. From the findings of the study, it was observed that the main strength of the method lies in detecting the DoS, the R2L and the U2R attacks, which are not satisfactorily detected by other methods.

The prime reason for better detection accuracy for the CRFs is that they do not consider the observation features to be independent. CRFs evaluate all the rules together, which are applicable for a given observation. This results in capturing the correlation among different features of the observation resulting in higher accuracy. Considering both the accuracy and the time required for testing, the system scores better. The integrated system also has the advantage that any method can be used in the layers of the system. This gives flexibility to the user to decide between the time and accuracy trade-off. Furthermore, it is possible to increase or decrease the number of layers in the system depending upon the task requirement. Finally, the system can be used for performing analysis on attacks because the attack category can be inferred from the layer at which the attack is detected and thus, the Layered CRFs are a strong candidate for building robust and efficient network intrusion detection systems.

13. Conclusion

This study focused on the development of layered conditional random fields based network intrusion detection system (LCRFNIDS). In this study, the suitability of conditional random fields and layered framework for building robust and efficient model of intrusion detection system for network systems was examined. In particular, layered framework was introduced and a layered conditional random fields based network intrusion detection model was developed which addresses three critical factors that severely affect the large scale deployment of present anomaly and hybrid intrusion detection systems in high speed networks. The three factors are:

i. Limited attack detection coverage;
ii. Large number of false alarms and
iii. Inefficiency in operation.

The study observed that 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, hence, specific intrusion response mechanism can be initiated which helps to minimize the impact of the attack.

The study also observed that conditional random fields are a strong candidate for building robust and efficient network 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 a moderate false alarms and thus, the attacks can be detected with very high accuracy.

This study has addressed the dual problem of **accuracy** and **efficiency** for building robust and efficient network intrusion detection systems. In this study, the layered conditional random fields approach was compared with some well-known methods and found that most of the present methods for intrusion detection fail to reliably detect denial of service attacks, root to local attacks and user to root attacks, while the integrated system developed in this study can effectively and efficiently detect such attacks. The developed system can help in identifying an attack once it is detected at a particular layer, which expedites the intrusion response mechanism, thus minimizing the impact of an attack. Finally, the developed system has the advantage that the number of layers can be increased or decreased depending upon the environment in which the system is deployed, giving flexibility to the network administrators and security professionals

.

References

[1] Hazem, M. E. and Nikos, M. A, (2008). "Real-Time Intrusion Detection Algorithm for Network Security. WSEAS Transactions on communications, 12(7).

[2] Allen.J, Christie.A, Fithen.W, McHugh.J, Pickel.J, Stoner.E, (2000) "State of the practice of Intrusion Detection Technologies" Technical Report CMU/SEI-99TR- 028, Carnegie-Mellon University - Software Engineering Institute.

[3] Kabiri, P. and Ghorbani, A. A. (2005). Research in Intrusion Detection and Response – A Survey. International Journal of Network Security. 1(2): 84–102.

[4] Bace, R. and Mell, P. (2001). Intrusion Detection Systems. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

[5] Scarfone, K. and Mell, P. (2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)". Computer Security Resource Centre (National Institute of Standards and Technology), (94-100).

[6] Axelsson, S. (1998). Research in Intrusion-Detection Systems: A Survey. Technical Report, Department of Computer Engineering, Chalmers University of Technology, (56-66).

[7] Anita K. J. and Robert S. S. (1999). Computer System Intrusion Detection: A Survey. Technical report, Department of Computer Science, University of Virginia. Retrieved: June 10, 2012. http://www.cs.virginia.edu/˜jones/IDS-research/Documents/jones-sielken- survey-v11.pdf.

[8] Kapil, K. G., Baikunth, N., Kotagiri, R., and Ashraf, K. (2006). Attacking Confidentiality: An Agent Based Approach. In *Proceedings of IEEE International Conference on Intelligence and Security Informatics*, Lecture Notes in Computer Science, Springer Verlag, (3975), (285–296).

[9] SANS Institute (2006). Intrusion Detection FAQ, http://www.sans.org/resources/idfaq/.

[10] Heady, R.; Luger, G.; Maccabe, A. and Mukherjee, B. (1991) A Method To Detect Intrusive Activity in a Networked Environment. In *Proceedings of the 14th National Computer Security Conference*, pages (362-371).[11] Altaf, A., Javed, M.Y. and Ahmed, A. (2008). Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005. Proceedings of the 9th ACIS International Conference of Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Aug. 6-8, IEEE., (335-339).

[12] Abdelaziz, M. (1997). Languages and Tools for Rule-Based Distributed Intrusion Detection, Ph.D. Thesis, Faculty University, Belgium.

[13] Christopher, K.; Fredrik V. and Giovanni V. (2005). Intrusion Detection and Correlation: Challenges and Solutions. Springer.

[14] Tao, P.; Christopher, L. and Kotagiri, R. (2002). Adjusted Probabilistic Packet Marking for IP Traceback. In Proceedings of the Second IFIP Networking Conference, Springer, (697–708).

[15] William R. C. and Steven M. B. (1994). Firewalls and Internet Security. Addison-Wesley.

[16] Schneier, B. (1996). Applied Cryptography. John Wiley & Sons.

[17] Lee, W. and Stolfo, S. (1998). Data Mining Approaches for Intrusion Detection. Proceedings of Seventh USENIX Security Symposium. (79-94).

[18] Lee, W. and Stolfo, S. and Mok, K, (1998). Mining Audit Data to Build Intrusion Detection Models. Proceedings of Fourth International Conference on Knowledge Discovery and Data Mining (KDD '98), (66-72).

[19] Lee, W. and Stolfo, S. and Mok, K, (1999). A Data Mining Framework for Building Intrusion Detection Model. Proceedings of IEEE Symposium, Security and Privacy

(SP ’99), (120-132).

[20] Agrawal, R. Imielinski, T. and Swami, A. (1993). Mining Association Rules between Sets of Items in Large Databases. Proceedings of ACM SIGMOD, 22(2), (207-216).

[21] Abraham, T. (2008). IDDM: Intrusion Detection Using Data Mining Techniques. http://www.dsto.defence./gov.au/publications/2345/DSTO-GD-0286.pdf. Retrieved August 4th 2012.

[22] Portnoy, L., Eskin, E. and Stolfo, S. (2001). Intrusion Detection with Unlabeled Data Using Clustering. Proceedings of ACM Workshop on Data Mining Applied to Security (DMSA), 2001.

[23] Shah, H., Undercoffer, J. and Joshi, A. (2003). Fuzzy Clustering for Intrusion Detection. Proceedings of 12th IEEE International Conference on Fuzzy Systems (FUZZ-IEEE ’03), 2, (1274-1278).

[24] Amor, N.B. Benferhat, S. and Elouedi, Z. (2004). Naive Bayes vs. Decision Trees in Intrusion Detection Systems. Proceedings of ACM Symposium on Applied Computing (SAC ’04), (420-424).

[25] Kruegel, C. Mutz, D. Robertson, W. and Valeur, F. (2003). Bayesian Event Classification for Intrusion Detection. Proceedings of 19th Annual Computer Security Applications Conference (ACSAC ’03), (14-23).

[26] Du, Y., Wang, H. and Pang, Y. (2004) “A Hidden Markov Models-Based Anomaly Intrusion Detection Method,” Proceedings of Fifth World Congress on Intelligent Control and Automation (WCICA ’04), 5, (4348-4351).

[27] Lafferty, J., McCallum, A. and Pereira, F. (2001). “Conditional Random Fields: Probabilistic Models for Segmenting and Labeling Sequence Data,” Proceedings of. 18th International Conference on Machine Learning (ICML ’01), (282-289).

[28] Debar, H., Becke, M. and Siboni, D. (1992) “A Neural Network Component for an Intrusion Detection System,” Proceedings of IEEE Symposium Research in Security and Privacy (RSP ’92), (240-250).

[29] Kim, D. S. and Park, J. S. (2003). “Network-Based Intrusion Detection with Support Vector Machines,” Proceedings of Information Networking, Networking Technologies for Enhanced Internet Services International Conference on Information Networking (ICOIN ’03), (747-756).

[30] Wu, Y. S., Foo, B. Mei, Y. and Bagchi, S. (2003). “Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS. Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC ’03), (234-244).

[31] Tombini, E., Debar, H. Me, L. and Ducasse, M. (2004). A Serial Combination of Anomaly and Misuse IDSs Applied to HTTP Traffic. Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC ’04), (428-437).

[32] Boughaci, D. Drias, H. Bendib, A. Bouznit, Y. and Benhamou, B.(2006). Distributed Intrusion Detection Framework Based on Mobile Agents. Proceedings of International Conference on Dependability of Computer Systems (DepCoS-RELCOMEX ’06), (248-255).

[33] Gu, Y., McCallum, A. and Towsley, D. (2005). “Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation,” Proceedings of Internet Measurement Conference (IMC ’05), USENIX Association, (345-350).

[34] Ji, C. and Ma, S. (1997). Combinations of Weak Classifiers. IEEE Transactions on Neural Networks, 8(1), (32-42).

[35] Dzeroski, S. and Zenko, B. (2002). Is Combining Classifiers Better than Selecting the Best One. Proceedings of the 19th International Conference on Machine Learning (ICML ’02), (123-129).

[36] Ratnaparkhi, A. (1996). A Maximum Entropy Model for Part-of-Speech Tagging,

Proceedings Conference on Empirical Methods in Natural Language Processing (EMNLP '96), Association for Computational Linguistics, (133-142).

[37] McCallum, A.; Freitag, D. and Pereira, F. (2000). "Maximum Entropy Markov Models for Information Extraction and Segmentation," Proceedings of 17th International Conference on Machine Learning (ICML '00), (591-598).

[38] Klein, D. and Manning, C. D. (2002). "Conditional Structure versus Conditional Estimation in NLP Models," Proc. ACL Conf. Empirical Methods in Natural Language Processing (EMNLP '02), Association for Computational Linguistics, 10, (9-16).

[39] Sutton, C. and McCallum, A (2006). "An Introduction to Conditional Random Fields for Relational Learning," Introduction to Statistical Relational Learning.

[40] Dietterich, T. G. (2002). Machine Learning for Sequential Data: A Review. Proceedings Of Joint IAPR International Workshop Structural, Syntactic, and Statistical Pattern Recognition (SSPR/SPR '02), LNCS 2396, (15-30) .