International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 5, May - 2013

Intrusion Detection System Based On Conditional Random Fields

Deepa V. Guleria[1], Chavan M. K[2]
[1]PG Scholar, VPCOE Baramati

[2]Asstt Prof, VPCOE Baramati

Abstract

An intrusion detection system is used to monitor network traffic, check for suspicious activities and notifies the network administrator or the system. To operate in high speed networks, present network intrusion detection systems are either signature based or anomaly based system. These systems are inefficient and suffer from a large number of false alarms. Some of the common attacks such as DoS,R2L ,Probe and U2R affect the network resources. Intrusion detection system has challenges to detect malicious activities reliably and should able to perform efficiently with large amount of network traffic.

We address in this paper two major issues of Accuracy and Efficiency by introducing a probabilistic approach Conditional Random Fields and Sequential Layered Approach. It is demonstrated that using Conditional Random Fields high attack detection accuracy can be achieved and using the Sequential Layered Approach high efficiency. Our experimental results on the benchmark KDD 1999 intrusion data set show improvement in attack detection accuracy is very high for Probe, Denial of Service, U2R and R2L attacks.

Keywords: *Intrusion Detection, Conditional Random Fields, Network Security, Decision tree*

1. Introduction

Intrusion Detection Systems (IDS) refers to a program used to detect an intrusion when it happens and to prevent a system from being compromised. An intrusion detection system monitors the activities of a given environment and detects inaccurate and inappropriate and anomalous activity as defined by the Sysadmin, Audit, Networking, and Security (SANS) institute [1]. Detecting intrusions in networks and applications has become one of the most critical tasks to prevent their misuse by attackers. Attackers try the newer and more advanced methods to defeat the installed security system. Denial of Service, Probing, Remote to Local, User to Root and others are some diverse type of attacks that creates a challenge for any intrusion detection system to detect different types of attacks with very minimum false alarms [2]. Therefore its a challenge to build a system which has broad attack detection coverage and which gives very few false alarms. The system must also be efficient to cope with large amount of audit data. There are three types of IDS depending on their mode of deployment, Network Based, Host Based and Application Based .Network based IDS monitors the packets from the network identifies intrusion by examining the network traffic and multiple hosts. Host based IDS analyze the audit patterns at the kernel level of the system which include system access logs and the error logs. It alerts the user or administrator when suspicious activity is detected. Intrusion detection systems can also be classified as signature based or anomaly based depending upon the attack detection method. Signature based IDS relies on identifying known signatures while the anomaly based systems depends on the pattern of computer usage and trained from the normal data. The Signature based systems have very high detection accuracy but they fail when an attack is previously unseen. On the other hand, anomaly based may have the ability to detect new unseen attacks but have the problem of low detection accuracy [4].

Hybrid approach is another technique for intrusion detection which is trained with both the normal and the known anomalous patterns. Hybrid systems are efficient and perform classification on test data. They can be use d to label unseen or new instances because during training they assign one of the known classes to every test instance. The disadvantage of a single system is that they cannot detect a different type of attacks reliably and has limited attack detection coverage. We introduce hybrid intrusion detection systems based on conditional random fields which can detect a wide variety of attacks and gives very few false alarms. We then integrate the layered framework with conditional random fields to improve the efficiency of the system. The proposed hybrid system is based on both the normal and the anomalous patterns.

2. Conditional Random Fields

Conditional Random Fields are discriminative probabilistic models that are used to model the conditional distribution over a set of random variables. Model).CRF was firstly proposed by Lafferty and his colleagues in 2001, whose model idea mainly came from MEMM (Maximum Entropy Markov Model)[5][9]. CRF is a sequence modeling framework that has all the advantages of MEMMs but also solves the label bias problem in a principled way. The critical difference between CRFs and MEMMs is that a MEMM uses per-state exponential models for the conditional probabilities of next states given the current state, while a CRF has a single exponential model for the joint probability of the entire sequence of labels given the observation sequence .A conditional random field is simply a conditional distribution p(y|x) with an associated graphical structure[8]. The model is conditional, dependencies among the input variables x do not need to be explicitly represented, affording the use of rich, global features of the input. Conditional models having better framework and they also do not make any unwarranted assumptions on the observations. They used to model rich overlapping features among the visible observations. Such models have been used in the natural language processing tasks. Lafferty and his colleagues in 2001 firstly proposed CRF.

Lafferty, McCallum and Pereira define a CRF on observations X and random variables Y. Let X be the random variable over data sequence to be labeled and Y the corresponding label sequence. In addition, let $G = (V, E)$ be a graph such that Y is indexed by the vertices of G. Then, $(X, Y)$is a CRF, when conditioned on X, the random variables Y_v obey the Markov property with respect to the graph: $p(Y_v|X, Y_{w,} w \neq v) = p(Y_v|X, Y_{w,} w{\sim}v)$where $w{\sim}v$ means that w and v are neighbors in G, i.e., a CRF is a random field globally conditioned on X. For a simple sequence (or chain) modeling, as in our case, the joint distribution over the label sequence Y given X has the following form:

$$p_\theta(y|x) \propto exp\left(\sum_{e\in E,k} \lambda_k f_k(e, y|_e, x + \sum_{v\in V,k} \mu_k g_k(v, y|_v, x\right), \quad (1)$$

where x is the data sequence, y is a label sequence, and $Y|_s$ is the set of components of y associated with the vertices or edges in subgraph S.

In addition, the features f_k and g_k are assumed to be given and fixed. In addition, the features f_k and g_k are assumed to be given and fixed. For example, a Boolean edge feature f_k might be true if the observation X_i is "protocol= tcp," tag Y_{i-1} is "normal," and tag Y_i is "normal". Similarly, a Boolean vertex feature g_k might be true if the observation X_i is "service= ftp" and tag Y_i is "attack." Further, the parameter estimation problem is to find the parameters $\theta = (\lambda_1, \lambda_2, \ldots; \mu_1, \mu_2, \ldots)$from the training data $D = (x^i, y^i)_{i=1}^N)$ with the empirical distribution$\tilde{p}(y|x)$.

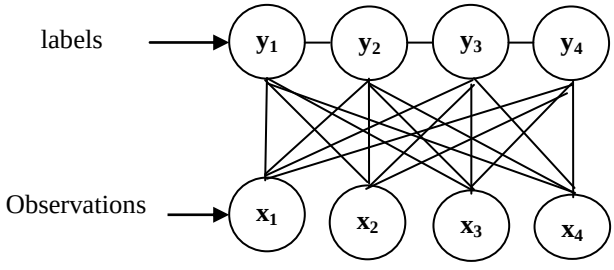

Figure1. Graphical Representation of a CRF

The graphical structure of a conditional random field is represented in Figure1 where $x1, x2, x3, x4$ represents an observed sequence of length four and every event in the sequence is correspondingly labeled as *y*1, *y*2, *y*3, *y*4. Conditional Random Fields predict the label sequence y given the observation sequence x. They model the arbitrary relationship among different features in an observation [6].

3. Description of KDD'99 data set

Benchmark KDD cup 99 Intrusion Detection data set is used for experiments [3]. The dataset was a collection of simulated raw TCP dump data on a local area network. The KDD 99 data set contains about 5 million connection records of the training data and about 2 million connection records of the test data. In our experiments, we use the ten percent of the total training data and ten percent of the test data (with corrected labels) which are provided separately. This leads to 494,020 training and 311, 029 test instances as shown in Table 1.

	Training Set	Test Set
Normal	97,277	60,593
Probe	4,107	4,166
DoS	391,458	229,853
R2L	1,126	16,349
U2R	52	68
Total	494,020	311,029

Table 1

The training data and testing data is made up of 22 different types of attacks out of the 39 present in the test data. There are some additional attacks in the KDD test dataset which are not available in the training data sets. This makes the task of intrusion detection more realistic. The attacks types are grouped into four categories as Probe, Denial of service (DoS), unauthorized access from a remote machine or Remote to Local (R2L) and unauthorized access to root or User to Root (U2R).The training dataset consisted of 494,021 records among which 97,277 (19.69%) were normal, 391,458 (79.24%) DOS, 4,107 (0.83%) Probe, 1,126 (0.23%) R2L and 52 (0.01%) U2R connections. Each TCP/IP connection is described by 41 features and labeled as either the normal or as an attack.

4. Sequential Layered Approach integrated with Conditional Random Fields

We are building an efficient and an effective hybrid network IDS by integrating the layered framework with the conditional random fields. Layered Approach is based on ensuring confidentiality, availability and integrity of data over a network [6][7]. Depending on the four different attack classes in the KDD 1999 data and other attacks in test data five layer system is implemented where every layer corresponds to a single attack class. In the system, the layers are trained separately with the normal patterns and with the attack patterns belonging to a single attack class. Every layers are then arranged one after the other in a sequence as shown in Figure 2. The layered approach reduces overall time required the compute and to detect the anomalous connections.

The layers are independent to each other and self-sufficient to block an attack without any need of a central decision-maker. During testing, all the unknown audit patterns irrespective of their attack class are passed into the system starting from the first layer. If the layer detects the instance as an attack, the system labels the instance as a Probe attack and initiates the response mechanism otherwise it passes the instance to the next layer.

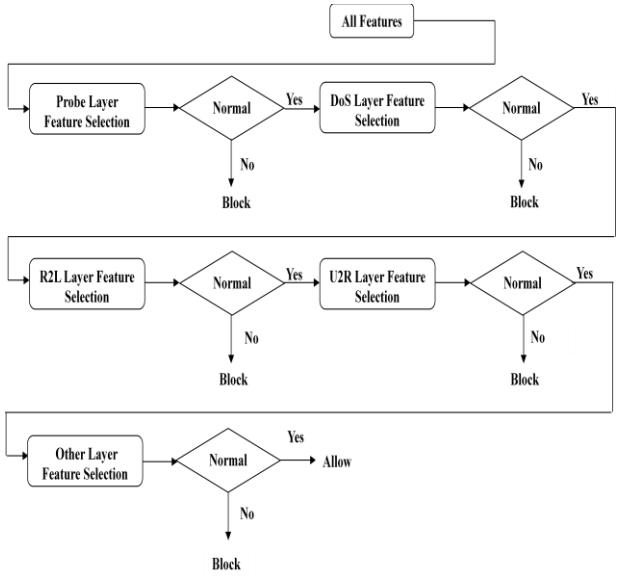

Figure 2. Integrating Layered Approach with Conditional Random Fields

The same process is repeated at every layer until either an instance is detected as an attack or it reaches the last layer where the instance is labeled as normal if no attack is detected.

4.1 Feature Selection

Corresponding to the four attack groups (Probe, DoS,R2L, and U2R) and other attacks given in the KDD 99 Data Set we select different features for different layers based upon the type of attack the layer is trained to detect. Hence we have a four independent modules corresponding to the four attack groups and fifth module is trained for other attacks not present in four attack groups in the training data set. We are selecting different features to train different layers in our framework. Hence, we use domain knowledge to select features for all the four attack classes. We now describe why some features were chosen over others in every layer in layered framework

1) Probing Attack:

It is an attempt of an attacker to scan the network to gather information about a network of computers or find known vulnerabilities for the apparent purpose of circumventing its security controls. e.g. portsweep, satan, ipsweep, nmap.

2) Denial of Service Attack (DoS):

It is a class in which the attacker makes some computing or memory resource too busy or too full to handle legitimate requests, or denies legitimate users

access to a machine. e. g. smurf, teardrop, land, back, neptune, pod.

3) Remote to Local Attack (R2L):

It occurs when an attacker who does not have an account on a remote machine sends packets to that machine over a network and exploits some vulnerability to gain local access as a user of that machine. e.g. spy, warezclient, warezmaster, ftp write, guess passwd.

4) User to Root Attack (U2R):

It is a class of exploit in which the attacker starts out with access to a normal user account and is able to exploit some vulnerability to gain root access to the system. e.g. perl,rootkit,buffer_overflow.

5) Other attacks:

These are attacks not present in above four classes. e.g, snmpgetattack, mailbomb, snmpguess ,mscan.

The list of features used for all the five layers described in Appendix.

5. Results and Discussion

The Benchmark KDD' 99 intrusion data set is used for experiments [3]. We use 10 percent of the total training data and 10 percent of the test data (with corrected labels), which are provided separately for system. For our results, we give the Precision, Recall, and F-Value. They are defined as follows:

$$Precision = \frac{number\ of\ True\ Positives}{number\ of\ True\ Positives + number\ of\ False\ Positives}$$

$$Recall = \frac{number\ of\ True\ Positives}{number\ of\ True\ Positives + number\ \ of\ False\ Negatives}$$

$$F - Measure = \frac{(1+\beta^2) * Recall * Precision}{\beta^2 * (Recall + Precision)}$$

where TP, FP, and FN are the number of True Positives, False Positives, and False Negatives, respectively, and corresponds to the relative importance of precision versus recall and is usually set to 1. We divide the training and testing data into different groups; Normal, Probe, DoS, R2L, and U2R. We perform experiments separately for all the five attack classes by randomly selecting data corresponding to that particular attack class and normal data only. Hence, for five attack classes we formed five independent models, separately, with feature selection.

5.1. Detecting Probe Attacks with Feature Selection

For detecting probe attack 5 significant features are selected out of 41 features shown in appendix. After selecting these 5 features, we have formed the probe patterns by using CRF coding in Java programming language. For this purpose, we used the records from 10 percent KDD train data set which is of type 'Normal + Probe' .After that it is tested with two labeled datasets, 10 percent corrected KDD test data and old KDD test data. Figure 3 shows the Probe attack result.

Normal and Probe (with Feature Selection)

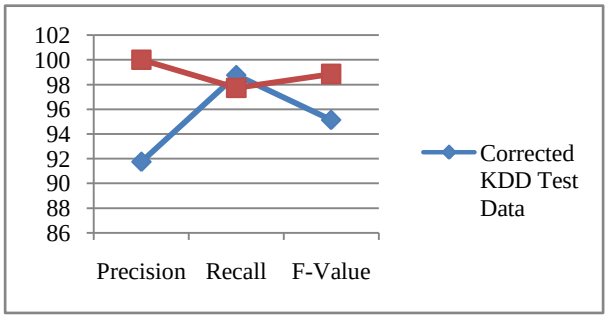

Figure 3. Probe Attack Result

5.2. Detecting DOS Attacks with Feature Selection

For detecting DoS attack 9 significant features are selected from appendix and formed the DoS patterns. For this purpose, we used the records from 10 percent KDD train data set which is of type 'Normal + DoS'. We do not add the probe, R2L and U2R data when detecting DOS. This allows the system to better learn the features for DOS and normal events. After that, we tested it with 10 percent corrected KDD test data and old test data. Figure 4 shows the DoS attack result.

Normal and DoS (with Feature Selection)

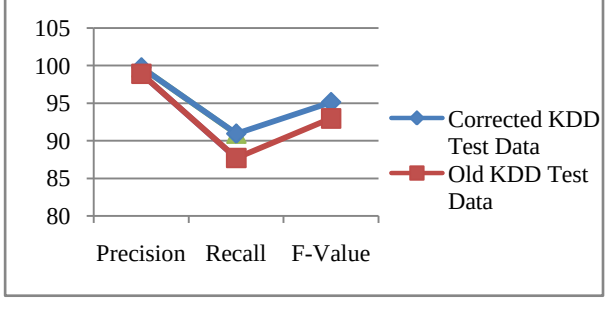

Figure 4. DoS Attack Result

5.3. Detecting R2L Attacks with Feature Selection

For detecting R2L attack 14 significant features are selected out of 41 features shown in appendix. After selecting these 14 features, we have formed the R2L

patterns. For this purpose, we used the records from 10 percent KDD train data which is of type 'Normal +R2L'. After that, we tested it with 10 percent corrected KDD test data and old test data. Figure 5 shows the R2L attack result.

Normal and R2L (with Feature Selection)

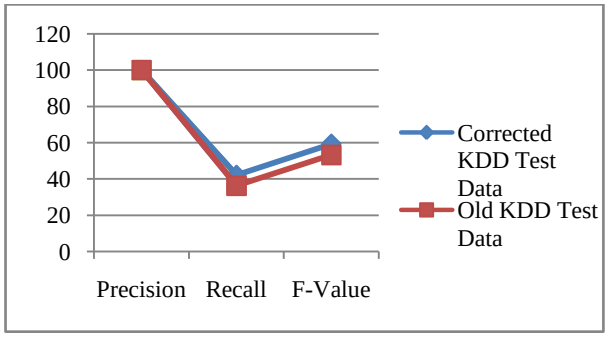

Figure 5. R2L Attack Result

5.4. Detecting U2R Attacks with Feature Selection

For detecting U2R attack we have selected 8 significant features out of 41 features shown in appendix. After selecting these 8 features, we have formed the U2R patterns. For this purpose, we used the records from 10 percent KDD train data which is of type 'Normal + U2R'.After that, we tested it with 10 percent corrected KDD test data and old test data. Figure 6 shows U2R attack result.

Normal and U2R (with Feature Selection)

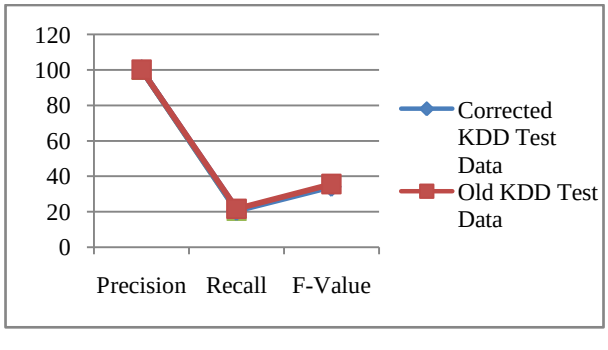

Figure 6. U2R Attack Result

5.5. Detecting Other Attacks

For Other attacks, we selected features such as 'duration', 'protocol' and 'service requested', while we ignored features such as 'number of file creations'. After selecting these 3 features, we have formed the Other attack patterns. For this purpose, we used the records which is of type 'Normal + other'. For example, to detect Other attacks, we train and test the system with other and normal data only. This allows the system to better learn the features for Other and normal events. Figure 7 shows Other attack result.

Normal and Other Attacks (with Feature Selection)

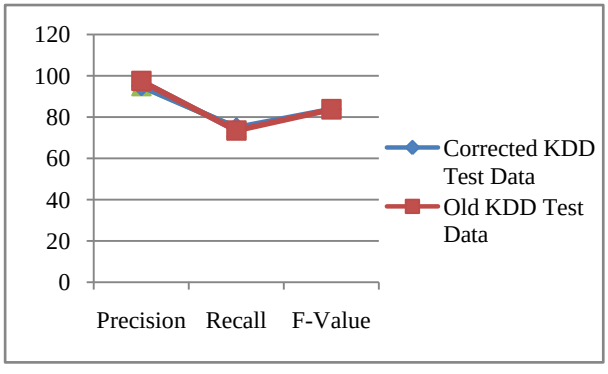

Figure7. Other Attack Result

5.6. Integrated System with Feature Selection

We integrate the five models with feature selection to develop the final system. In this experiment, the data in the test set is relabeled either as normal or as attack and all the data from the test set is passed though the system starting from the first layer. Figure 8 shows the Integrated System result.

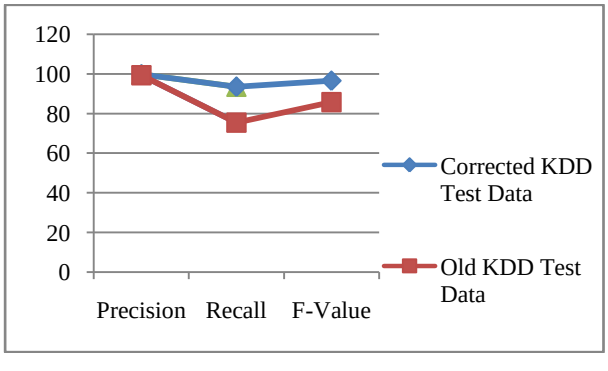

Figure 8. Integrated System Result

4.7. Comparison Results with Other Approaches

Figures show the comparison between Layered Approach using Conditional Random Fields, Layered Navie Bayes and Layered Decision Trees with feature selection. The results shows in Figure 9, Figure 10, Figure 11, Figure 12 that Layered Conditional Random

Fields with Feature Selection outperform well for detecting R2L and U2R attacks than other methods such as Layered Navie Bayes and Layered Decision Trees.

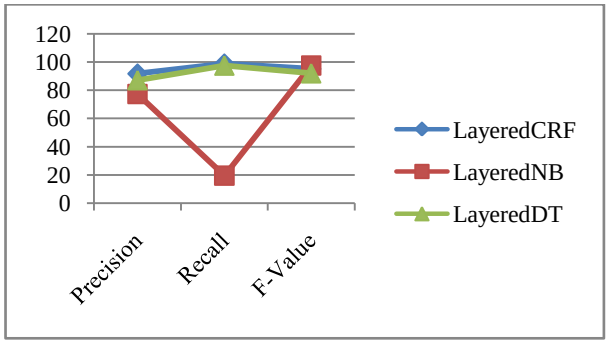

Figure 9. Normal and Probe (Feature Selection)

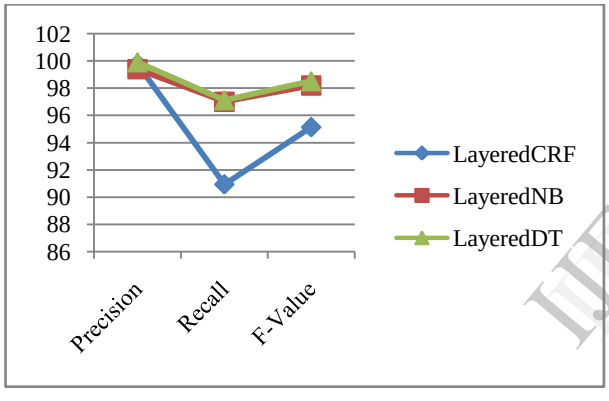

Figure 10. Normal and DoS (Feature Selection)

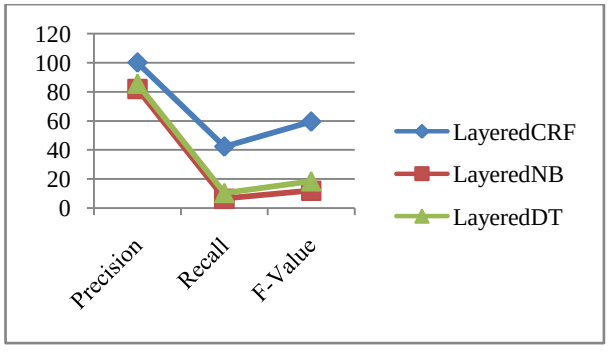

Figure 11. Normal and R2L (Feature Selection)

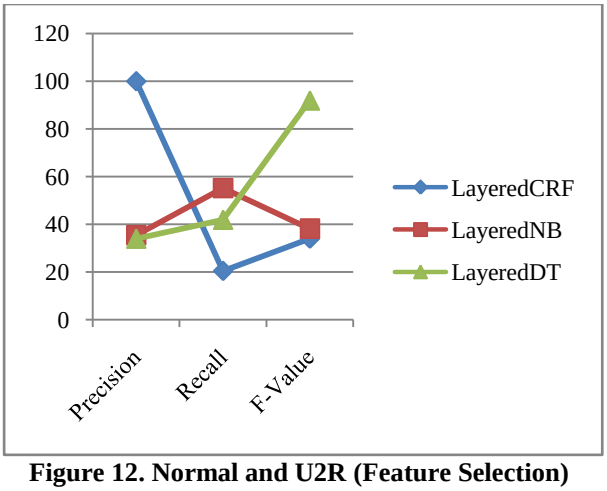

Figure 12. Normal and U2R (Feature Selection)

6. Conclusion

The hybrid system, addresses the problem of Accuracy and Efficiency for building accurate and efficient intrusion detection system. Implementing the sequential Layered Approach and feature selection reduce the time required to train and test the model. The experimental results in section 5 show that Conditional Random Fields very effectively improve the attack detection rate and decrease the false alarm rate. Conditional Random Fields which is a sequence labeling method can be very effective in detecting attacks. System can be implemented to detect a variety of attacks including the DoS, Probe, R2L and the U2R. Other type of attacks can also be detected by adding new layers in the system, making our system highly scalable.

The proposed approach is compared with some well known methods for intrusion detection such as naïve Bayes and decision trees. These methods cannot detect the Remote to Local and the User to Root attacks effectively, while the proposed integrated system can efficiently and effectively detect such attacks. The proposed system identify an attack once it is detected at a particular layer and gives a quick response to an attack, thus minimize the impact of an attack. The number of layers in the system can be increased or decreased which a major advantage of the system.

References

[1] SANS Institute—Intrusion Detection FAQ, http://www.sans.org/ resources/idfaq/, 2010.
[2] Autonomous Agents for Intrusion Detection, http://www.cerias.purdue.edu/research/aafid/, 2010.
[3] Overview of Attack Trends, http://www.cert.org/archive/pdf/ attack_trends.pdf, 2002.

[4] KDD Cup 1999 Intrusion Detection Data, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html , 2010.
[5] J. Lafferty, A. McCallum, and F. Pereira, "Conditional Random Fields: Probabilistic Models for Segmenting and labeling Sequence Data", Proc. 18th Int'l Conf. Machine Learning (ICML '01), pp. 282- 289, 2001.
6] 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.
7] Kapil Kumar Gupta, Baikunth Nath, Ramamohanarao Kotagiri, "Layered Approach Using Conditional Random Fields for Intrusion Detection," IEEE Transactions on Dependable and Secure Computing (vol. 7 no. 1),pp. 35-49,2010.
[8] C. Sutton and A. McCallum, "An Introduction to Conditional Random Fields for Relational Learning," Introduction to Statistical Relational Learning, 2006
[9] A. McCallum, D. Freitag, and F. Pereira, "Maximum Entropy Markov Models for Information Extraction and Segmentation," Proc. 17th Int'l Conf. Machine Learning (ICML '00), pp. 591-598, 2000.

Appendix

Following tables shows the Feature Selection for Network Intrusion Detection:

Feature Selected for Probe Layer

Feature Number	Feature Name
1	duration
2	protocol_type
3	service
4	flag
5	src_bytes

Feature Selected for R2L Layer

Feature Number	Feature Name
1	duration
2	protocol_type
3	Service
4	flag
5	src_bytes
10	hot
11	num_failed_logins
12	logged_in
13	num_compromised
17	num_file_creation
18	num_shells
19	num_access_files
21	is_host_login
22	is_guest_login

Feature Selected for Other Layer

Feature Number	Feature Name
1	duration
2	protocol_type
3	service

Feature Selected for DoS Layer

Feature Number	Feature Name
1	duration
2	protocol_type
4	flag
5	src_bytes
23	count
34	dst_host_same_srv_rate
38	dst_host_serror_rate
39	dst_host_srv_serror_rate
40	dst_host_rerror_rate

Feature Selected for U2R Layer

Feature Number	Feature Name
10	hot
13	num_compromised
14	root_shell
16	num_root
17	num_file_creation
18	num_shells
19	num_access_files
21	is_host_login