

Accuracy and Efficiency in Intrusion Detection System

¹J.S.Narendra Kumar, ²T.Sudha Rani, ³M.Raja Babu

^{1,2,3}Dept. of CSE, ADITYA Engineering College, Surampalem, AP, India

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 and automatic pre defined user prompts. We demonstrate that high attack detection accuracy can be achieved by using Conditional Random Fields and high efficiency by implementing the Layered Approach and prompts. 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 Bayes. The improvement in attack detection accuracy is very high, particularly, for the U2R attacks (34.8 percent improvement) 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

Intrusion Detection, Layered Approach, Conditional Random Fields, Network Security, Decision Trees, Naive Bayes

I. Introduction

INTRUSION detection as defined by the SysAdmin, Audit, Networking, and Security (SANS) Institute is the art of detecting inappropriate, inaccurate, or anomalous activity [6]. 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 [4] and [24]. 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.

Intrusion detection started in around 1980s after the influential paper from Anderson [10]. Intrusion detection systems are classified as network based, host based, or application based depending on their mode of deployment and data used for analysis [11]. Additionally, intrusion detection systems can also be classified as signature based or anomaly based depending upon the attack detection method. The signature-based systems are trained by extracting specific patterns (or signatures) from previously known attacks while the anomaly-based systems learn from the normal data collected when there is no anomalous activity [11]. Another approach for detecting intrusions is to consider both the normal and the known

anomalous patterns for training a system and then performing classification on the test data. Such a system incorporates the advantages of both the signature-based and the anomaly-based systems and is known as the Hybrid System. Hybrid systems can be very efficient, subject to the classification method used, and can also be used to label unseen or new instances as they assign one of the known classes to every test instance. This is possible because during training the system learns features from all the classes. The only concern with the hybrid method is the availability of labeled data. However, data requirement is also a concern for the signature- and the anomaly-based systems as they require completely anomalous and attack free data, respectively, which are not easy to ensure.

II. Related Work

The field of intrusion detection and network security has been around since late 1980s. Since then, a number of proposed [1, 16]. We focus on social trust [8, 21, 24] that relies on user interests and collaboration behavior.

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. we discuss these techniques and frameworks[a]. To overcome the weakness of a single intrusion detection system, a number of frameworks have been proposed, which describe the collaborative use of network-based and host based systems [45]. Systems that employ both signature based and behavior-based techniques are discussed in [19] and [41]. In [32], the authors describe a data mining framework for building adaptive intrusion detection models. A distributed intrusion detection framework based on mobile agents is discussed in [12]. The most closely related work, to our work, is of Lee et al. [30-31], and [32]. 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 our work, we define features from the observations as well as from the observations and the previous labels and perform sequence labeling via the CRFs to label every feature in the observation. This setting is sufficient for modeling the correlation between different features of an observation. We also compare our work with [21], which describes the use of maximum entropy principle for detecting anomalies in the network traffic. The key difference between [21] and our work is that the authors in [21], use only the normal data during training and build a baseline system, i.e., a behavior-based system, while we train our system with both the normal and the anomalous data, i.e., we build a hybrid system. Second, the system in [21], fails to model long-range dependencies in the observations, which can be easily represented in our model. We also integrate the Layered Approach with the CRFs to gain the benefits of computational efficiency and high accuracy of detection in a single system. We compare the Layered Approach with the works in [18], [25], and [41]. The authors in [18], describe the combination of "strong" classifiers using stacking, where the decision trees, 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. In [25], 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. In [41], the authors apply a combination of anomaly and misuse detectors for better qualification of analyzed events. However, our work 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, our system is based upon serial layering of multiple hybrid detectors. From our experiments, we show that the Layered CRFs perform better than individual classifiers and they are more efficient and accurate than a system based on classifier combination. The results from individual classifiers at a layer are not combined at any later stage in the Layered Approach, and hence, an attack can be blocked 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 us the advantage of reduced processing when an attack is detected at the initial layers in the sequential model.

In this paper, we show the effectiveness of CRF using prompts for intrusion detection. Motivated by our results in [23], we perform detailed analysis and show that CRFs are a strong candidate for building robust intrusion detection systems. We then show that high efficiency can be achieved by implementing the Layered Approach using prompts. Finally, we integrate the Layered Approach and the CRFs to develop a system that is accurate and performs efficiently.

III. Proposed Model

A. Predefined User Prompts and Conditional Random Fields for Intrusion Detection

In intrusion detection system, prompting is the predefined technique which prompts the users while connects to the network and the system follow the previous approach of multi layered approach using conditional random fields for intrusion detection. In this proposed system the system basically prompts the user once logged into system, the system prompts the user for specific pre defined prompt then matches with the stored value. The unauthorized user who have entered into network will be automatically prompt ed. 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 [37], maximum entropy Markov models [34], and CRFs [29] 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 [27]. The simplest conditional classifier is the Maxent classifier based upon maximum entropy classification, which estimates the conditional distribution of every class given the observations [37]. The training data is used to constrain this conditional distribution while ensuring maximum entropy and hence maximum uniformity. We now give a brief description of

the CRFs, which is motivated from the work in [29].

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 $p(y,x)$, where as the CRF are discriminative models and directly model the conditional distribution $p(y|x)$, 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 $p(y|x)$. Second, inferring the conditional probability $p(y|x)$ from the modeled joint distribution, using the Bayes rule, requires the marginal distribution $p(y)$. 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 [40]. 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 [15]. CRFs also avoid the observation bias and the label bias problem, 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 [29]. 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, we explore the suitability of CRFs for intrusion detection.

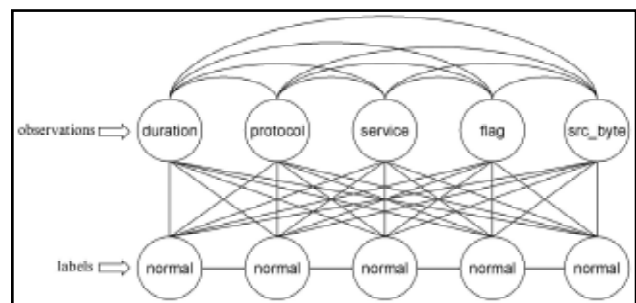


Fig. 1: Graphical Representation of a CRF

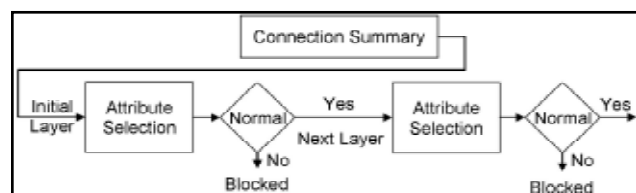


Fig. 2: Layered Representation

The data set used in our experiments represents features of every session in relational form with only one label for the entire record. In this case, using a conditional model would result in a simple maximum entropy classifier [40].

However, we represent the data in the form of a sequence and assign a label to every feature in the sequence using the first-order Markov assumption instead of assigning a single label to the entire observation. Though, this increases the complexity but it also increases the attack detection accuracy. Each record represents a separate connection, and hence, we consider every record as a separate sequence. We aim to model the relationships among features of individual connections using a CRF, as shown in fig. 1. In the fig. features such as duration, protocol, service, flag, and src_bytes take some possible value for every connection. During training, feature weights are learnt, and during testing, features are evaluated for the given observation, which is then labeled accordingly. As it is evident from the figure, every label is connected to every input feature, which indicates that all the features in an observation help in labeling, and thus, a CRF can model dependencies among the features in an observation. Present intrusion detection systems do not consider such relationships among the features in the observations. They either consider only one feature, such as in the case of system call modeling, or assume conditional independence among different features in the observation as in the case of a naive Bayes classifier. As we will show from our experimental results, the CRFs can effectively model such relationships among different features of an observation resulting in higher attack detection accuracy. Another advantage of using CRFs is that every element in the sequence is labeled such that the probability of the entire labeling is maximized, i.e., all the features in the observation collectively determine the final labels. Hence, even if some data is missing, the observation sequence can still be labeled with less number of features. Our first goal is to improve the attack detection accuracy. We first compare the accuracy of CRFs for detecting attacks with other methods [a].

B. Prompt Based Layered Approach for Intrusion Detection

The system first prompts the user for specific authenticated information once the user logged into the network. Once the user confirms the authenticated information and follows the layered approach for intrusion detection.

We now describe the Layer-based Intrusion Detection System (LIDS) in detail [a]. The LIDS draws its motivation from what we call as the Airport Security model, where a number of security checks are performed one after the other in a sequence. Similar to this model, the LIDS represents a sequential Layered Approach and is based on ensuring availability, confidentiality, and integrity of data and (or) services over a network. Fig. 3, gives a generic representation of the framework.

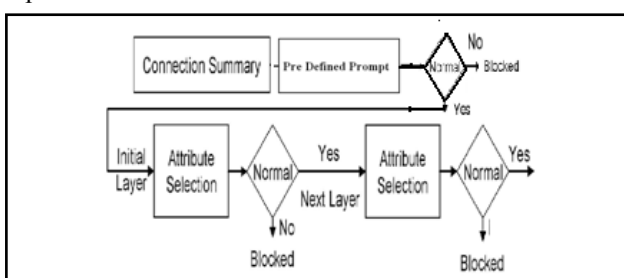


Fig. 3: Prompt and Layered Representation

C. Integrated Layered Approach with Conditionally Random Field

we discussed two main requirements for an intrusion detection system; accuracy of detection and efficiency in operation 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. Given the data, we first select four layers corresponding to the four attack groups (Probe, DoS, R2L, and U2R) and perform feature selection for each layer, which is described next.

IV. Experiments

In our experiments, we use 10 percent of the total training data and 10 percent of the test data (with corrected labels), which are provided separately. Each record in the data set represents a connection between two IP addresses, starting and ending at some well defined times with a well-defined protocol. Further, every record is represented by 41 different features. Each record represents a separate connection and is hence considered to be independent of any other record. The training data is either labeled as normal or as one of the 24 different kinds of attack. These 24 attacks can be grouped into four classes; Probing, DoS, R2L, and U2R.

Similarly, the test data is also labeled as either normal or as one of the attacks belonging to the four attack groups. It is important to note that the test data is not from the same probability distribution as the training data, and it includes specific attack types not present in the training data. This makes the intrusion detection task more realistic [3]. Table 1 gives the number of instances for each group of attack in the data set.

For our experiments with CRFs, we use the CRF toolkit, CRF++ [2]. We use the Weka tool [44], to perform experiments with the decision trees and the naive Bayes classifier. We develop python and shell scripts for data formatting and implementing the Layered Approach. For all our experiments, we perform hybrid detection, as discussed [a]

A. Comparison of Results

In this section, we compare our work with other well-known methods based on the anomaly intrusion detection principle. The anomaly-based systems primarily detect deviations from the learnt normal data by using statistical methods, machine learning, or data mining approaches. Standard techniques such as the decision trees and naive Bayes are known to perform well. However, our experiments show that the Layered CRFs perform far better than these techniques. The main reason for this is that the CRFs do not consider the observation features to be independent. In [38], the authors present a comparative study of various classifiers when applied to the KDD'99 data set, and in [13], the authors propose the use of Principle Component Analysis (PCA) before applying a machine learning algorithm. Use of support vector machines is discussed in [26]. We compare our results from the results presented in these papers in Table 14. The table represents the Probability of Detection (PD) and False Alarm Rate (FAR) in percent for various methods including the KDD '99 cup winners. From the table, we observe that the prompt based Layered CRFs perform significantly better than the previously reported results including the winner of the KDD '99 cup and various other methods applied to this data set. The most impressive part of the Layered CRFs is the margin of improvement as compared with other methods. Layered

CRFs have very high attack detection of 98.6 percent for Probes (5.8 percent improvement) and 97.40 percent detection for DoS. They outperform by a significant percentage for the R2L (34.5 percent improvement) and the U2R (34.8 percent improvement) attacks. From our experiments and the comparison in Table 14, we conclude that the prompt based Layered CRFs can be very effective in detecting the Probe, the U2R, and the R2L attacks as well as the DoS attacks we performed experiments with our integrated system by implementing a four-layer system. The four layers correspond to Probe, DoS, R2L, and U2R. For each layer, we then selected a set of features that is sufficient to detect attacks at that particular layer. Feature selection for each layer enhances the performance of the entire system

Table 1: Comparison of Result

		Probe	DoS	R2L	U2R
Prompt and Layered Conditional Random Fields	PD	99.00	97.90	30.000	90.4000
	FAR	0.91	0.07	0.360	0.0500
Layered Conditional Random Fields	PD	98.60	97.40	29.600	86.3000
	FAR	0.91	0.07	0.350	0.0500
KDD'99 Winner	PD	83.30	97.10	8.400	13.2000
	FAR	0.60	0.30	0.005	0.0030

The runtime (testing) performance of our model is comparable with other methods; however, the time required to train the model is slightly higher. We also observe that feature selection not only decreases the time required to test an instance, but it also increases the accuracy of attack detection. Our 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, we can increase or decrease the number of layers in the system depending upon the task requirement. Finally, our 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.

V. Conclusions and Futrue Work

References

- [1] D. Artz, Y. Gil, "A survey of trust in computer science and the semantic web", *J. Web Sem.*, 5(2), pp. 58–71, 2007.
- [2] D. Brabham, "Crowdsourcing as a model for problem solving: an introduction and cases", *Convergence*, 14(1), pp. 75, 2008.
- [3] D. Brickley, L. Miller, "Foaf vocabulary specification 0.98, 2010. [Online] Available: <http://www.xmlns.com/foaf/spec/>.
- [4] R. S. Burt, "Structural holes and good ideas", *American Journal of Sociology*, 110(2), pp. 349–399, Sept. 2004.
- [5] L. M. Camarinha-Matos, H. Afsarmanesh, "Collaborative networks", In *PROLAMAT*, pp. 26–40, 2006.
- [6] C. Dwyer, S. R. Hiltz, K. Passerini, "Trust and privacy concern within social networking sites", In *AMCIS*, 2007.
- [7] M. Ford et al., "Web Services Human Task (WS-HumanTask)", Version 1.0., 2007.
- [8] J. Golbeck, "Trust and nuanced profile similarity in online social networks", *TWEB*, 3(4), 2009.
- [9] T. Grandison, M. Sloman, "A survey of trust in internet applications", *IEEE Communications Surveys and Tutorials*, 3(4), 2000.
- [10] L. Juszczak, S. Dustdar, "Script-based generation of dynamic testbeds for soa", In *ICWS*, pp. 195–202, 2010.
- [11] J. Kleinberg, "The convergence of social and technological networks", *Commun. ACM*, 51(11), pp. 66–72, 2008.

- [12] J. Kleinberg, S. Suri, E. Tardos, T. Wexler, "Strategic network formation with structural holes", *ACM Conference on Electronic Commerce*, 7(3), pp. 1–4, 2008.
- [13] P. J. Macdonald, E. Almaas, A. L. Barabási, "Minimum spanning trees of weighted scale-free networks", *Europhys. Lett.*, 72(2), pp. 308–314, 2005.
- [14] M. J. Metzger, "Privacy, trust, and disclosure: Exploring barriers to electronic commerce", *J. Computer-Mediated Communication*, 9(4), 2004.
- [15] T. P. Moran, A. Cozzi, and S. P. Farrell, "Unified activity management: Supporting people in e-business", *Com. of the ACM*, 48(12), pp. 67–70, 2005.
- [16] L. Mui, M. Mohtashemi, A. Halberstadt, "A computational model of trust and reputation for e-businesses", In *HICSS*, pp. 188, 2002.
- [17] C. Petrie, "Plenty of room outside the firm", *IEEE Internet Computing*, 14, 2010.
- [18] R. Ronen and O. Shmueli, "Soql: A language for querying and creating data in social networks", In *ICDE*, pp. 1595–1602, 2009.
- [19] D. Schall, S. Dustdar, "Dynamic context-sensitive pagerank for expertise mining", In *Social Informatics*, Vol. 6430 of *LNCS*, pp. 160–175. Springer, 2010.
- [20] D. Schall, H.-L. Truong, S. Dustdar, "Unifying human and software services in web-scale collaborations", *Internet Comp.*, 12(3), pp. 62–68, 2008.
- [21] F. Skopik, D. Schall, S. Dustdar, "Modeling and mining of dynamic trust in complex service-oriented systems", *Information Systems*, pp. 735–757, 2010.
- [22] W. Tsai, "Social capital, strategic relatedness, and the formation of intra-organizational strategic linkages", *Strategic Management Journal*, (21), pp. 925–939, 2000.
- [23] W3C, "Sparql query language for rdf", 2008, [Online] Available: <http://www.w3.org/TR/rdf-sparql-query/>.
- [24] C.-N. Ziegler, J. Golbeck, "Investigating interactions of trust and interest similarity", *Decision Support Systems*, 43(2), pp. 460–475, 2007.



MR.M.RAJABABU is a well known Author and excellent teacher Received M.tech from affiliated college of JNTU university. He is presently working as a Sr.Asst.Professor in Aditya Engineering college in CSE department, surampalem. His area of interest in Networking, Data Mining, Information security and other advances in computers.



Mr.J.S.Narendra Kumar is a student of ADITYA Engineering college. Surampalem. Presently he is pursuing his M.TECH from this college and He received his graduation from Swarnandhra college of Engineering and technology in 2010.



Ms. T.SUDHA RANI well known Author and excellent teacher Received her graduation and M.TECH from the affiliated college of JNTU university. she is working as Associate Professor in Computer science Engineering in ADITYA Engineering college. Surampalem. Her area of Interest includes Data Warehouse and Data Mining, information security, flavors of Unix Operating systems and other

advances in computer Applications.