International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 7 392 – 394

Intrusion detection with Parameterized Methods for Wireless Sensor Networks

Safi Yadahalli
Computer Networks
KJ College of engineering and Management Research of,
Pune, India.
sysafisafi@gmail.com

Prof. Mininath N Nighot
Computer Networks
KJ College of engineering and Management Research of,
Pune, India.
imaheshnighot@gmail.com

Abstract: Current network intrusion detection systems lack adaptability to the frequently changing network environments. Furthermore, intrusion detection in the new distributed architectures is now a major requirement. In this paper, we propose two Adaboost based intrusion detection algorithms. In the first algorithm, a traditional online Adaboost process is used where decision stumps are used as weak classifiers. In the second algorithm, an improved online Adaboost process is proposed, and online Gaussian mixture models (GMMs) are used as weak classifiers. We further propose a distributed intrusion detection framework, in which a local parameterized detection model is constructed in each node using the online Adaboost algorithm. A global detection model is constructed in each node by combining the local parametric models using a small number of samples in the node. This combination is achieved using an algorithm based on particle swarm optimization (PSO) and support vector machines. The global model in each node is used to detect intrusions. Experimental results show that the improved online Adaboost process with GMMs obtains a higher detection rate and a lower false alarm rate than the traditional online Adaboost process that uses decision stumps. Both the algorithms outperform existing intrusion detection algorithms. It is also shown that our PSO, and SVM-based algorithm effectively combines the local detection models into the global model in each node; the global model in a node can handle the intrusion types that are found in other nodes, without sharing the samples of these intrusion types.

Index Terms:- *Dynamic distributed detection, network intrusions, Adaboost learning, parameterized model*.

*****

I. INTRODUCTION

Statistics based methods construct statistical models of network connections to determine whether a new connection is an attack. For instance, Denning [8] construct statistical profiles for normal behaviors. The profiles are used to detect anomalous behaviors that are treated as attacks. Caberera et al. [9] adopt the Kolmogorov- Smirnov test to compare observation network signals with normal behavior signals, assuming that the number of observed events in a time segment obeys the Poisson distribution. Li and Manikopoulos extract several representative parameters of network flows, and model these parameters using a hyperbolic distribution. Peng et al. use a nonparametric cumulative sum algorithm to analyze the statistics of network data, and further detect anomalies on the network. 2) Data mining-based methods mine rules that are used to determine whether a new connection is an attack. For instance, Lee et al. [10] characterize normal network behaviors using association rules and frequent episode rules.Intrusions on the network is indicated by these deviation rules. To automatically build patterns of attackset alZhang et al. use the random forest algorithm. [11] propose an algorithm for mining frequent itemsets (groups of attribute value pairs) to combine categorical and continuous attributes of data. To handle dynamic and streaming datasets this algorithm is extended. Unsupervised clustering is first used byZanero and Savaresi to reduce the network packet payload to a tractable size, andto intrusion detection then a traditional anomaly detection algorithm is applied.Using genetic network programmingMabu et al. detect intrusions by mining fuzzy class association rules. Using fuzzy logic Panigrahi and Sural detect intrusions, which from a user's current and past behaviorscombines evidence.

II. RELATED WORK

1) Data Preprocessing:, Three groups of features for each network connectionare extracted that are commonly used for intrusion detection:For transmission control protocol (TCP) connections basic features of individual, Assuggested by domain knowledge content features within a connection, and using a two-second time window traffic features computed. x = (x1, x2, . . . ,xD) This is the vector fored from the extracted feature values from a network connection, here number of feature components is denoted by D. , and of the feature'svalue ranges may differ greatly from each other of continuous and categorical features. A set of data which is labeled for training purposes contains the framework for constructing these features. Depending on the attack type there are many types of attacks on the Internet. +1labeledsamples are the normal samples whereas −1, −2, ...,.are the attack samples.

2) Local Models: The design of weak classifiers and Adaboostbased training is included in the construction of a local detection model at each node. Each individual feature component corresponds to a weak classifier. In this way,full use of the information is possible by naturally handling the mixed attribute data for the network connections in each feature. Using only the local training samples the Adaboost training is implemented at each node. A parametric model

consisting of the parameters of the weak classifiers and the ensemble weights is contained in each node after training.

3) Global Models: In each node,using the PSO and SVM-based algorithm a global model is constructed by sharing all the local parametric models. The information learned from all the local nodes is fused by the global model in each using a small number of training samples in the node. The input to the global classifier is Feature vectors of new network connections to the node, which classified as either normal or attacks. The local model in the node is updated using results of the global model in the node which is then shared by other nodes.

III. LITERATURE SURVEY

In the paper [1] using online Ada boost based approach combined with weak classifiersIDS for distributed environment is proposed and implemented. This paper maintaining highest detection rate and accuracy.intrusionovercomes the difficulty of handling multi attribute network connectiondata with To do better than the decision tree algorithm without feature selection detection with feature selection was accomplished. The classification capabilities of the decision tree is possible with this establishment filtering in a shorter time [2]. Out of selected three features filter algorithm, it was found that than ReliefF when KDD data set was takenChi square and Information Gain was giving a better performance. By considering the four major attacks in the KDD data set the work can be further extended. S.Vijayarani, M.Divyaanalysed the performance of the three classification rule algorithms, Part algorithm seems better than the other two algorithms as far as time factor & number of rules generation are concernedfor Breast Cancer Dataset and Heart Disease dataset as far as experimental results are concerned. [4] The performance of three well known data mining classifier algorithms ie ID3, J48 and Naïve Bayes were evaluated by Mrutyunjaya Panda, ManasRanjanPatra basedon the 10-fold cross validation test. KDDCup'99 experimental results IDS data set conveys that Naïve Bayes is one of the most valuable inductive learning algorithms; As far as the detection of new attacks is concerneddecision trees are more remarkable. Some researchers predictable apriori algorithm [5] which scans the dataset only twice and builds FP-tree once while it still requests to generate candidate item sets. FPGrowth algorithm [6], which contains two methods for competently foretelling an FP-tree-the core operation of the FP-growth algorithm whose implementation is described by Christian Borgelt.The implementation clearly outperforms Apriori and Éclat, even in highly optimized versions is proved from the experimental results.Using online Adaboost based approach combined with weak classifiers and implantation of IDS for a dessiminated environment [7] defeat the complexity of handling multi attribute network connection data with maintaining highest detection rate and accuracy of different types of attacks.

The remainder of this paper is organized as follows. Introduces the intrusion detection framework i.e. proposed system is described in Section III. The system analysis of intrusion detection models is described in Section IV. The experimental results are in Section V. conclusion of the paper is in Section VI.

IV. PROPOSED SYSTEM

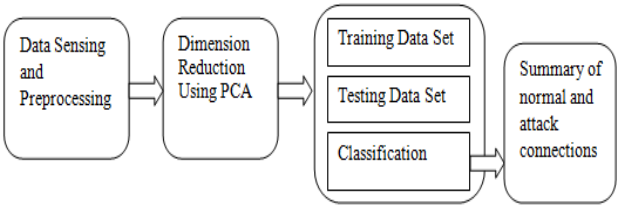

Fig 1. System Architecture

Offline Adaboost algorithms are constructed in one step andAdaboostalgorithm is updated one by one., The sample weights are updated simultaneously in the offline Adaboost algorithm while, the sample weights are updated one by one in the Adaboostalgorithm.Thenumber of weak classifiers so fixed in the offline Adaboost algorithm while the number of weak classifiers is fixed,inoffline Adaboost algorithm, and equal to the dimension of the feature vectors.

Let t be initial weight of each training sample,

$$t = \begin{cases} \dfrac{(M_{normal} + M_{intrusion}) * r}{M_{normal}} & \text{for normal connection} \end{cases}$$

V. RESULT TABLE

Algorithm	Total Test file	Malicious file	Normal file	Detection rate	False alarm rate
PSO	106	46	60	93.48	5
SVM	106	46	60	95.65	3.33
KNN	73	33	40	87.88	12.5
PSO+ SVM	300	30	270	95.00	3.00

Table I: Result analysis value for another algorithm

We in our work aim to achieve results that are more efficient than the above mentioned algorithms both in detection rate and at false alarm rate, we aim to achieve the detection rate as possible and close to 97% and the reduce the flase alarm rate to 3.

VI. CONCLUSION

A new Intusion detection system is proposed using some of the old teechiniques with advanced adaboost algorithm which increases the efficiency of detection of attacks and reduction of the false alarm rates.

REFERENCES

[1] Weiming Hu, Jun Gao, Yanguo Wang, Ou Wu, and Stephen Maybank," Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection", IEEE Transactions on Cybernetics 2013.

[2] Luigi Coppolino, Salvatore D'Antonio, AlessiaGarofalo, Luigi Romano," Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks", 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing.

[3] Vikas Sharma, AditiNema," Innovative Genetic approach For Intrusion Detection by Using Decision Tree", 2013 International Conference on Communication Systems and Network Technologies.

[4] Dr. T. Subbulakshmi, Ms. A. Farah Afroze," Multiple Learning based Classifiers using Layered Approach and Feature Selection for Attack Detection", 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013).

[5] P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo," Real-Time Intrusion Detection with Fuzzy Genetic Algorithm", 978-1- 4799-0545-4/13/$31.00, IEEE

[6] Manish Kumar, Dr. M. Hanumanthappa, Dr. T. V. Suresh Kumar," Intrusion Detection System Using Decision Tree Algorithm", proceeding for IEEE, 2012.

[7] Jinhua Huang and Jiqing Liu," Intrusion Detection System Based on Improved BP Neural Network and Decision Tree", 2012 IEEE fifth International Conference on Advanced Computational Intelligence (ICACI).

[8] D. Denning, "An intrusion detection model," IEEE Trans. Softw. Eng., vol. SE-13, no. 2, pp. 222 232, Feb. 1987.

[9] J. B. D. Caberera, B. Ravichandran, and R. K. Mehra, "Statistical traffic modeling for network intrusion detection," in Proc. Modeling, Anal. Simul.Comput.Telecommun. Syst., 2000, pp. 466–473.

[10] Prof RiyazJamadar"Enhanced Detection Rate through PCA and Radial SVM in Wireless Sensor Networks".