PERFORMANCE COMPARISON OF THREAT CLASSIFICATION MODELS FOR CYBER-SITUATION AWARENESS

Conference Paper · September 2019

CITATIONS
0

READS
13

4 authors, including:

Temidayo Oluwatosin Omotehinwa
Kogi State University, Anyigba, Nigeria
9 PUBLICATIONS **8** CITATIONS

PERFORMANCE COMPARISON OF THREAT CLASSIFICATION MODELS FOR CYBER-SITUATION AWARENESS

S. S. Olofintuyi[1,*] T. O. Omotehinwa[1], O. H. Odukoya[2] and E. A. Olajubu[2]

[1]Department of Mathematical Sciences, Achievers University Owo, Ondo, Nigeria

[2]Department of Computer Science, Obafemi Awolowo University, Ile-Ife, Osun, Nigeria

*Email of Corresponding Author: olofintuyi.sundaysamuel@gmail.com

ABSTRACT

Cyber threats are becoming an issue and a great threat to organizations that work with data, and millions of dollars are being lost to hackers. Various machine learning algorithms have been used to detect threat at the first phase of situation awareness model. In this paper, we compare the performance of Support Vector Machine (SVM) and Artificial Neural Network (ANN) at the perception phase of situation awareness model. Feature selection was used to extract the most significant attributes and they are fed to ANN and SVM. Knowledge Discovery and Data Mining (KDD 99) dataset was used during the training of the two proposed algorithms. At the end of the simulation, ANN gives an accuracy of 0.978 while SVM gives an accuracy of 0.957. The results of the simulation showed that ANN is more accurate in comparison to SVM for threat detection on a computer network.

Keywords: Situation Awareness, Intrusion Detection System, Artificial Neural Network, Support Vector Machine, performance comparison.

INTRODUCTION

According to Endsley (1995) Situation Awareness (SA) is the act of detection of threat in the environment and relaying it back to the system administrator. Generally, the model for threat detection are classified into three sections which are the perception phase, comprehension phase and projection phase. The perception phase is solely responsible for detection of threat while the comprehension phase is connected to a trained database of various events of historical database that has been trained by the network administrator. Once the comprehension phase has finished judging whether such event is malicious or not, the projection phase then sends the feedback to the comprehension phase. A threat is a group of malicious programs that intrudes into one's program. Existing models for monitoring and protecting computer networks are unable to accurately detect modern threats and intrusions such as Denial of service (DOS), User to root, Root to local and probing. The need for an efficient classifier or predictive model for intrusion detection is on the increase as a result of the emergences of big data (Othman, *et al.,* 2018) and enterprise migrations to the cloud. Intruders are gaining more grounds due to the imbalances in the cyber security. This has negatively affected organization that keeps sensitive data, most organization have paid heavily for this and vital information has been lost to intruders. According to Dutt, *et al.,* 2012) they also worked on SA where an instance based learning theory was used for prediction of threat on a computer network. Furthermore, Mitchell, (1997) make use of Naïve Bayes Classifier for classifying whether a class is threat or non-threat on a computer network . Finally, Prahlad and Wenke (2006) make use of statistical approach for detecting threat on SA but it was observed that the approach cannot give accurate prediction to the administrator. Researcher has used various algorithms on the network for threat detection, but none has been able to obtain 100% accuracy. Feature selection is defined as the removal of redundant attributes from a given dataset (Yildirim, 2015). While on the other hand, machine learning is a branch of Artificial Intelligence that uses statistical and optimization techniques to create computers intelligent machines. This study is targeted at comparing two of the machine learning techniques that are widely used due to their attributes that have given them edge over other supervised machine learning algorithms.

Mehibs and Hashim, (2018) proposed an intrusion detection system based on back propagation neural network. The back propagation relies on the modification of weight to train the system; this is subsequently used to forecast the class label of the new input patterns. The authors proposed an algorithm for the classification of DOS, U2R, Probe and R2L and the developed algorithm was evaluated with Knowledge Discovery and Data Mining (KDD 99) dataset. The study obtained a detection rate of 0.99 and false alarm rate of 0.03 with a data size of 500. With

200% increase in data size, the results obtained were still in the range above for detection rate and false alarm rate. the algorithm is considered effective given the high detection and low false alarm rate. Zakrzewska and Ferragut (2011) in their work, presented a model for cyber conflict and an extended Petri-Net (PN) was adopted. Petri-Nets was used in modelling real-time conflicts. It was also noted that PN formalism is more expensive than other models such as attack graphs, for modelling cyber-conflict and that it is amenable to exploring cyber strategies.

Dutt, *et al.*, (2012) presents situation awareness in computer network defence which combat threat affecting the cyber infrastructure. Intrusion Detection System (IDS) was used in the model. The study validated the prediction given by the model.

Parveen, *et al.*, (2011) in their work presented a supervised learning insider threat detection model which employed stream mining technique. They deployed an ensemble-based insider threat where the continuous data was changed to chuck. The proposed model was tested with 1998 Lincoln laboratory intrusion dataset. After the experiment, it was observed that the proposed model performance was good but has just only one false negative and a few numbers of false positive.

Chintada and Udaykumar (2015) presented a novel approach to network security situation awareness method and model in which a security system was proposed which was capable of detecting threat. But at the end of their experiment, there is still high rate of false positive ratio which is as a result of wrong event judgement and malfunctioning of devices.

Megha and Amrita (2013) Presented performance analysis of different feature selection methods in intrusion detection. In their paper, six feature selection was adopted on Knowledge Discovery and Data Mining (KDD 99) dataset and the detection rate, root means square error and computational time was used as performance metric. It was also noted that the computational time of Naive Bayes was less compare to C4.5 algorithm.

Alocious, *et al.*, (2014) Presented intrusion detection framework for cyber-crimes in which Bayesian network was adopted because they are good for adaptive learning. KDD dataset Hettich and Bay, (1999) was used and after the experiment, the result signifies high accuracy in threat detection.

MATERIALS AND METHODS

Experimental Design

Generally, situation awareness model designed for computer network was designed for threat detection. Situation awareness was firstly introduced by (Endsley, 1995) in his work, in which the model has three major phases which are perception phase, comprehension phase and projection phase. The proposed situation awareness model has the following sub-models. Threat detection sub-model, designed as client-server architecture which consist of two levels:

i. Multilayer perception of ANN (First level detection)
ii. Support Vector Machine (Second level detection)

The model used in this work has three phases which are the perception phase, comprehension phase and projection phase. Furthermore, this work focused on the perception phase by introducing two supervised machine learning to the perception phase. Both machines are used as detector in the perception phase. One of the major onuses of the perception phase is to detect events in its environment and then classify them whether they are threat or not. Both machine were used simlatanouly to detect packet of data coming to the network and then classify them whether they are intrusion or not. Figure 1 shows how the two machines are placed in the situational awareness model and also used for threat detection.

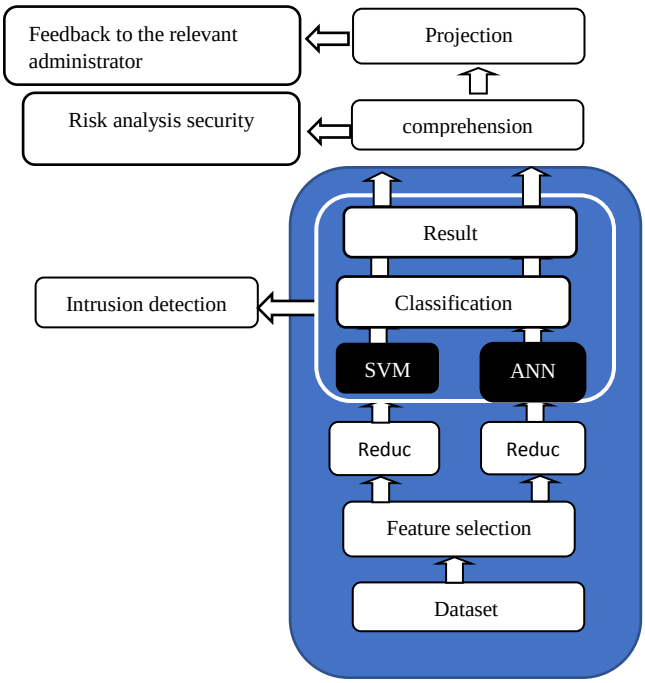

Figure 1 The Proposed Model for Threat Detection

KDD sDataset

Defence Advanced Research Projects Agency (DARPA) in the year 1998, created the first of its kind standard dataset for evaluating intrusion detection

system. The dataset supplied has a total of 24 training attacks with addition of 14 different test attack data. Finally, forty-one (41) attributes was given in KDD CUP 99 DATASET with their feature names but the most significant five features were selected after feature selection. The selected features are: Duration, protocol type, service, count, srv_ count.

There are different categories of intrusions, and they are classified into four:

Denial of Service (DOS): DOS is a group of attack, in which they keep the computing memory busy because of this, the memory no longer has time to attend to legitimate request. Example includes: Apache2, Mail bomb, Process table, Smurf, Udpstorm. Back, Land, Teardrop, Ping of death and SYN Flood.

User to root: These are group of attacks in which they approach a system as a normal or legitimate user of the system, meanwhile they are intruder. Once they get access to the system, they then explore the system vulnerabilities. Examples are Xterm, perl, loadmodule and fdformat.

Root to local: These are group of attacks in which they send packet of data to the network which they do not have access to. With this, they tend to gain access and explore the system vulnerabilities. Examples are FTP write, Imap, Xlock, Dictionary, Phf and Guest.

Probing: are also one of the categories of attack whereby an attacker approaches a system and then gain access to the system which later explore the vulnerabilities of the system. Examples are Saint, satan, Mscan, Ipsweep and Nmap.

Data Pre-processing: The dataset gotten ranges from different numbers, in this research, any number that is not zero (0) is been considered as one (1). Where 0 represents normal event and 1 is considered as malicious event. The dataset was inputted in excel in order to carry out the conversion. The dataset has forty-one attributes from the source but was reduced to most five significant attributes. This is done one after the other by deleting redundant and irrelevant attribute from the dataset. By doing these, the model is trained with the most significant features of the dataset in WEKA environment. The name of the attributes are duration, protocol, service,count and srv_count. The diagram below depict the dataset. Figure 2 depicts our dataset.

First Threat Detection Sub-phase (ANN): As used in this work, the ANN is trained with a set of data which is obtained from NSL- KDD 99 dataset. It has been used in various machine learning for threat detection that is why NSL- KDD 99 was put into consideration in this research work. This dataset consists of 49, 808 input sample and two-element target output. After the neural network has been created with WEKA neural network toolkit, it is then configured in a way that makes the network model compatible with the problem at hand, as defined by sample data. The tuning process for this model is referred to as training the network

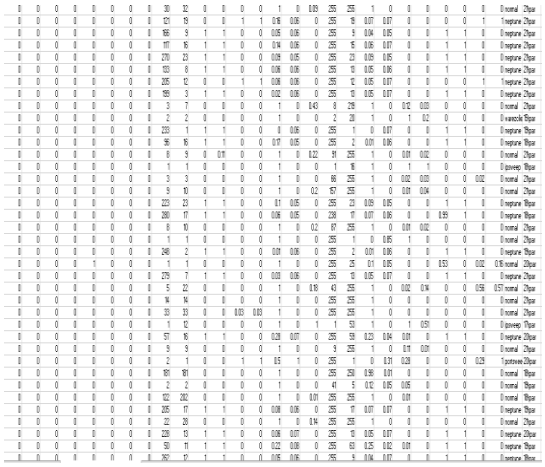

Figure 2 KDD 99 Dataset

At this stage, configuration and training require that the network be provided with example data which was uploaded. Also, in our method, all the attack groups were grouped into four sections and an output code were given to them to determine the group which they belong. Attacks under the denial of service were given 01000 output. Once the output is 01000, the model classifies it as DOS. Also, if the output is 00100, the model classifies it as Remote to local attack. And if the output is 00010, the attack is believed to be probes. Still in the same vein, if the output is given as 00001, the attack group is considered to be User to Root attack. Finally, if the output is given as 10000, then the event is taken to be normal by the ANN model.

Strength of Artificial Neural Network.

One of the advantages of using neural network is that it is an inherent parallel processor and it is also adaptive, meaning that it can be trained to take decision on its own. Neural network is proficient to give the better classification by nonlinear boundaries and also can easily overcome over fitting by some regularizes setting. ANN's are "universal approximators". With a sufficient amount of data and time, you should be able to approximate whatever function that generate the data with arbitrary amount of accuracy.

Second Threat Detection Sub-Phase Description

The second phase was detected using Support Vector Machine (SVM). SVM has shown superior performance in pattern recognition. An SVM is a model that is been represented by various points in space and each example of the point in space are separated by a hyper-plane. SVM has found its

usefulness in recognition and classification. The Sequential Minimal Optimization as used in WEKA environment was used in this research work. The missing binary value by default was normalized. To obtain the optimum hyperplane for a linearly separable classification Eq. 1.0 must be minimized subject to the constraints stated in Eq 2.0 and 3.0 respectively

$$min\frac{1}{2}\|w\|^2 \quad (1)$$

$(X_j, Y_j) \ldots (X_z, Y_z)$, $Y \epsilon \{1, 0\}$ Where $(X_j, Y_j) \ldots (Xz, Y_z)$ are a train data. z is the number of samples, Y belong to category of 0 or 1, W represents weight of the input, b represents bias while x represents input feature. The category formula is given as

$$(W.X) + b \geq Y_i \; if \; Y_i = 1 \quad (2)$$

$$(W.X) + b \leq Y_i \; if \; Y_i = 0 \quad (3)$$

Strength of Support Vector Machine

Ability of a machine to detect intrusion in real time is of great advantage to such machine. SVM detects intrusions in real time on a network of computers. Not only does SVM detects intrusions in real time it also has high speed of detection of threat and giving the administrator the feedback of any event coming to the network. Like other supervised machines, that follows the conventional empirical risk, SVM does not because it selects appropriate parameters. Finally, scalability is also one of the strengths of the proposed machine used in this model.

Performance Evaluation

The two proposed machines are supervised machine learning. As a result of that, the following metrics were used to evaluate their performance: True Positive (TP), False Positive (FP), False Negative (FN), and True Negative (TN). TP describes the event that are positive and are been classified as positive, TN also talks about the event that are negative and are been classified as negative. FN are events where the negative cases are not classified correctly and finally, FP are events where the positive events are not classified correctly.

Sensitivity/True positive rate/Recall: describes the event that are positive and are been classified as positive

$$Sensitivity = \frac{TP}{TP + FN} \quad (4)$$

Precision: talks about the event that are negative and are been classified as negative.

$$Specificity = \frac{TN}{FP + TN} \quad (5)$$

Accuracy: talks about the overall effectiveness of the proposed model**.**

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \quad (6)$$

Experimental Setup

WEKA, a simulation tool was used to simulate the proposed model. In the WEKA simulating environment, there are various classifier, but Support Vector Machine and Artificial Neural Network were selected for this work because they give better prediction above another classifier. NSL KDD dataset was used to test the functionality of the designed system. NSL KDD dataset is a dataset that has 41 features which was obtained from Defense Advance Research Project Agency (DARPA). However, best five significant features were used in this work which are the protocol type, duration, service, count and srv_count. Hybrid based feature selection method was used to remove irrelevant and redundant features. The data in the dataset was pre-processed and save in CSV format thereafter, it was saved and then reopen with a notepad. In this environment the data must be save in arff format for WEKA to recognize it. There are three sections in the notepad which are the title and it was denoted with @relation while the feature of the data was denoted with @ attribute while the data was denoted with @ data. This is the standard format for any arff format which is useable in the WEKA environment. All this process just describes how to prepare the dataset. Immediately after that, the software (WEKA) was opened and the data set was loaded into the software. After that, SVM module and ANN were selected from WEKA and all the proper parameter were keyed in.

RESULTS AND DISCUSSION

The simulation results showed that the false positive and true positive rates for SVM were 956 and 25,501 respectively out of 49,080. The result of the two supervised machine learning is stated in the Table 1.

The true negative and false negative rates were 22,306 and 1,045 respectively out of 48,080. The sensitivity for SVM was 0.961 while the specificity for SVM was 0.958. Finally, it was

observed that the accuracy for the SVM was 0.959 of the total actual selected features. On the other hand, it was observed that the true positive and false positive

Table 1 Result of classification by ANN and SVM.

Classifier	Number of instances	True Positive (TP)	True Negative (TN)	False Positive (FP)	False Negative (FN)	Sensitivity	Specificity	Accuracy
ANN	49,080	26116	22606	341	745	0.972	0.985	0.978
SVM	49,080	25501	22306	956	1045	0.961	0.958	0.959

for ANN were 26116 and 341 respectively out of 49,080. The true negative and false negative rates were 22,606 and 745 respectively out of 49,080. While the

sensitivity was 0.972 and the specificity by the model was 0.985. Finally, for the ANN, the accuracy was 0.978.

CONCLUSION

After the experiment, it was discovered that ANN shows more accuracy than SVM for threat detection on a computer network. However, the differences between the two machines for threat detection was minimal but can't be neglected. From this work, whenever a network administrator wants to build-up a system for awareness of intrusion on his network, ANN should be considered for accuracy in threat detection which also has a great advantage of speed in intrusion detection system.

REFERENCES

Alocious, C., Abouzakhar, N., Xiao, H., Christianson, B., Intrusion detection system using Bayesian network modeling. In proceedings of the 13th European conference on cyber warfare and security, 3(1): 223-230, 2014.

Chintada, S., Udaykumar, J., A novel approach to network security situation awareness method and model. International Journal of Engineering and Innovative Technology (IJEIT), 4(11): 103-107, 2015.

Dutt,V., Ahn,Y., Gonzalez, S., Cyber Situation Awareness: Modelling the Security Analyst in a Cyber-Attack Scenario through Instance-based Learning. In proceeding of Data and Applications Security and Privacy. Heidelberg, Germany, 2012.

Endsley, M. R., Toward a theory of situation awareness in dynamic system. In Human Factors Journal, 37(1): 32-64, 1995.

Hettich, S., Bay, S. D., KDD Cup 1999 Data. Retrieved from The UCI KDD Archive: http://kdd.ics.uci.edu, 1999.

Megha, A., Amrita, K., Performance analysis of different feature selection methods in intrusion detection. International Journal of Scientific and Technology Research, 2(6): 225-231, 2013.

Mehibs, M. S., Hashim, H. S., Proposed Network Intrusion Detection System In Cloud Environment Based on Back Propagation Neural Network. Journal of Babylon University, Pure and Applied Sciences, 26(1): 29-40, 2018.

Mitchell. T., Machine Learning, McGraw Hill.1997.

Othman, M. S., Ba-Alwi, M. F., Alsohybe, T. N., Al-Hashida, A. Y., Intrusion detection model using machine learning algorithm on Big Data environment. Journal of Big Data, 5(34): 250-261, 2018.

Parveen, P., Weger, Z. R., Thuraisingham, B., Hamlen, K., Khan, L. Supervised learning for insider threat detection using stream mining. In the proceedings of IEEE 23rd International conference on Tools with Artificial Intelligence ICTAI. Boca Raton, USA. 2011.

Prahlad, F., Wemke, L., Evaluating network anomaly detection systems: Formal seasoning and practical techniques. In Proceeding of the 15th USENIX Security Symposium, Vancouver, B.C., Canada, 2006.

Yildirim, P., Filter-Based Feature Selection Methods for Predicting of Risks in Hepatitis Disease. International Journal of Machine Learning and Computing, *5*(4): 258-263, 2015.

Zakrzewska, A., Ferragut, E., Modelling Cyber Conflicts using an Extended Petri net Formalism In: Computational Intelligence in Cyber Security. IEEE Symposium. Califonia, USA, 43-46, 2011.