The 4th International Conference on Digital Arts, Media and Technology
and 2nd ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering

A Machine Learning Approach for Detecting Distributed Denial of Service Attacks

Tanaphon Roempluk *† and Olarik Surinta *
* *Multi-agent Intelligent Simulation Laboratory (MISL)*
Department of Information Technology, Faculty of Informatics
Mahasarakham University
Maha Sarakham, Thailand
{tanaphon.roe, olarik.s}@msu.ac.th
†*Master student*

***Abstract*—This research aims to present the method for identifying distributed denial of service (DDoS) attacks. Two benchmark dataset, including KDD CUP 1999 and NSL-KDD, were used. The dataset were checked and deleted duplicate data. After the process, the amount of records of KDD Cup 1999 dataset were decreased from 4,898,431 records to 529,655 records, and the amount of records of NSL-KDD dataset were decreased from 125,373 to only 12,354 records. The reduction of the records always happened because of the characteristics of DDoS attacks which send repeated data to the victims' server. The researchers converted alphabet data to numeric data, then training by K-nearest neighbor (KNN), multi-layer perceptron and support vector machine. The result showed that KNN was the best method to identify the DDoS attacks.**

***Index Terms*—Distributed denial of service (DDoS) attack, K-nearest neighbor (KNN), Multi-layer percetron (MLP), Support vector machine (SVM)**

I. Introduction

Nowadays, security concerns from the use of the internet and computer system is one of problems. The security has been attacked in different ways. Distributed Denial of Service (DDoS) [1] is one of the most common attacks on the internet due to the limitation on the attacked device such as memory or bandwidth. The victims require to open the system to allow users to connect. The cyber attackers use these channels to make the victims' resources reach their peak until they cannot be used. Then, the victim' devices are out of service and cannot serve the users. Classification o f abnormalities in computer network can be classified b y u sing computer network traffic l ogs, w hich i nclude n ormal d ata a nd various network attack data. In each attack features, there are different characteristics which can be used to detect abnormalities when occurring in the system. In [2]–[5] artificial n eural network (ANN) were used in order to classify attack data. The accuracy is higher than 90%.

Related work: In the research [2], researchers specified the numbers of hidden layers of the network from 30-55 layers in order to to classify the DDoS attack data from 4,986 records. Records were classified i nto 4 g roups i ncluding, D NS DDoS attack, CharGen DDoS attack, UDP DDoS attack and Normal. The result found that ANN with total 50 hidden layers can identify the DDoS data with a 95.6% accuracy rate. While Hsieh and Chan [3] used neural network and Apache Spark framework, which has been used to manage large-scale data (Big Data) and work as a cluster for DDos detection. In the experiment of series ARPA 2000 LLDOS 1.0 which has 7 special features including, Number of Packets, Average of Packet Size, Time Interval Variance, Packet Size Variance, Number of Bytes, Packet Rate, and Bit Rate. All data were classified into two categories: normal data and attack data. There were 51,040 normal data and 74,480 attack data. All data samples were separated into 2 parts, 30% for the learning series, and another 70% for the test Data. It was found 94% accuracy rate.

In the research of Devaraju and Ramakrishnan [4] tested three artificial neural networks including 3 methods. There were feed forward neural network (FFNN), probabilistic neural network (PNN) and radial basis neural network (RBNN). The methods has been used to test the effectiveness of the Intrusion Detection System by tested with the KDD Cup 1999 dataset [6], containing 41 special features. There are four types of attacks including, 1) Denial of Service (DoS) containing back, land, neptune, pod, smurf and teardrop, 2) Remote to Local (R2L), containing ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient and warezmaster, 3) User-to-Root (U2R), containing buffer_overflow, loadmodule, perl and rootkit, 4) probing, containing ipsweep, nmap, portsweep and satan. The data were divided into 7 classes. There were normal class, smurf class, neptune class, saint class, mail bomb class, Apache class and satan class. The experiment was divided into training set and test set. Each set contains 700 data. The experimental data showed that the PNN network was the best. The PNN, FFNN and RBNN neural networks performed accuracy rate at 97.5%, 94.3% and 65%, respectively.

Researchers also use different machine learning techniques e.g. In [5], they classified network attack information by using ANN, SVM, and ANN+SVM techniques and using dataset NSL KDD [7] . In this experiment, the attack were divided into 2 classes including, 58,630 attack class and 67,343 normal classes. The accuracy rate were 79.56, 79.27 and 79.71%, respectively.

In [8] offers intrusion detection method by using decision

978-1-5386-8072-8/19/$31.00 ©2019 IEEE

tree ID3 in order to reduce the number of special features. From the KDD Cup 1999 dataset which reduced 41 attributes to 18 attributes. The information used in this test were divided into four intrusion categories. There are Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R) and Probe. The 26,167 data sets are divided into two equal parts for training and testing. Special feature information were trained through K-nearest neighbor and genetic algorithm (KNN-GA) techniques in order to categorize the information and compare to KNN methods and support vector machine (SVM). The experiments showed that the KNN-GA method was the most accurate. The accuracy rate was 98%.

In [9] presented a method for improving the detection and classification process using naïve bayes, bayesian networks (NB-Tree) and AD-Tree which tested with NSL-KDD 99 dataset. The test data values were converted to the rage 0-1 by min-max normalization method. Then, the special features were selected from the data by correlation-based feature selection (CFS). The results showed that NB-Tree had the best performance. NB-Tree, AD-Tree and naïve bayes are effective at 99.87%, 98.49% and 90.38%, consequently.

Kushwaha et al. [10] presented a method for selecting the best special features with the Mutual Information (MI) for detecting abnormalities. 10% of KDD Cup 1999 data were tested. The data contains 494,021 training data and 311,029 test data. The data were divided into 2 classes including, attack data and normal data. When using MI, 30 special features were selected and applied to further training with naïve, random forest, OneR, SVM, Adaboost, Bagging, KNN (k=5), KNN (k=10) and SVM+Nave Bayes. The accuracy rates were 92.73%, 99.89%, 95.58%, 99.91%, 95.05%, 99.79%, 99.77%, 99.69%, and 60.40% respectively. The results showed that the SVM performs the best accuracy rate at 99.91%. In [11] presented the method for identifying abnormal data in computer networks. The KDD Cup 1999 and NSD-KDD dataset were tested with J48 graft and naïve bayes method. Cross validation were conducted as an effective evaluator. Given $K = 10$, from the test, the J48 graft method has 99.435% accuracy rate. the J48 got the best effectiveness. The naïve bayes method got 92.715% accuracy rate.

Contribution: This research presents a method for classifying DDoS attack data by using computer network security information with machine learning. The KNN, SVM and MLP method are introduced. The grid search method are used for finding the suitable parameters for the KDD Cup 1999 and NSL-KDD dataset in order to make a performance comparison.

Paper outline: The remaining parts of the paper is organized as follows: In Section II, the machine learning approaches are described. In Section III data processing is presented. In Section IV experimental settings and the results are presented. Finally, a conclusion and future work is given in Section V.

II. Machine Learning Approaches

A. K-Nearest Neighbors Algorithm (KNN)

KNN which is the method to find the nearest member in dataset. It is a technique of machine learning that does not require modeling for data classification, but all data will be calculated to find distance value in order to compare the distance between the data that need to be classified y and all data X_i [12]. Therefore, the data with the smallest distance, the amount of data is k , is taken to be considered. In the total k, if any of members in the group C_i has the highest values of k, that data which needs to be categorized y will be categorized at that group. Therefore, given $k = 3$ means 3 values with minimum distance value will be taken into the account. If three data, containing the distance value, are in the group $d = (C_1, C_1, C_3)$, the data which need to be categorized will be set as C_1 because there are the most appearances. Euclidean distance calculations can be calculated as Eq. 1.

$$d(x, y) = \sqrt{\sum_{i=1}^{N}(x_i - y_i)^2} \tag{1}$$

where N is the number of special features (Dimensions) of the data. x, y is the data in the training set, and y is the data which needs to be classified. Then, calculate all the distance values $d(x, y)$ for voting by majority vote method. Therefore, C_k dataset which most appears is determined as the result of KNN.

B. Support Vector Machine (SVM)

SVM [13], [14] is the powerful and accurate categorization method, so researchers always use in classifcation problems. The SVM algorithm find the optimal hyperplane with the maximum margin between training point and hyperplane. The training point that approach the hyperplane line are called *support vectors*. Initially, SVM was designed to work with the special two-class classification, using a linear equation for segmenting feature vector data (Eq. 2).

$$f(x) = sign(w^T x + b) \tag{2}$$

where w is weight vector and B is bias.

C. Multi-Layer Perceptron (MLP)

MLP is artificial neural network with a multi-layer structure [15]. It consists of an input layer and passes from one layer to another hidden layer. It has a function for calculating when receiving an output from the node in the previous layer. The function called *activation function*. Each layer does not need to be the same function. The function converts incoming data to distinguish using a single line called *linearly separable*. Before the data has been sent to the output layer, it is sometimes necessary to use more than one hidden layer in order to convert the data into Linearly Separable until it reach the output layer.

III. Data Processing

A. Data Analysis

KDD CUP 1999 dataset and NSL-KDD dataset were divided into normal class and 4 features of attack class including,

1) *Denial of Service (DOS)* attacks is an attack that send a large number of packets to the target victims which cause the service to become failed.
2) *Remote to Local (R2L)* attacks is an attempt to access the targeted system without permission to access.
3) *User to Root (U2R)* attacks is an attempt to access unauthorized function in order to reach the Supper-user (root).
4) *Probing* attacks are the data validation on the network.

Then, trying to find the vulnerability of the target in order to use in the attacks. The example of common types are Nmap or port scanning. In the dataset of this research, there are 41 special features which are selected only normal data and DDos attacks.

B. Data Pre-Processing

The KDD CUP 1999 dataset and NSL-KDD dataset are composed of duplicate data, numbers, and alphabets. Before sending the data to machine learning, the data required to be processed as follows.

1) Removed the DDos data which is duplicate data. A lot of duplicate data were sent to the system during attacks. Deleting the duplicate data result as the data could be different in one row. Deleting method is done by diagnosis the duplicate special attributes and classes (Class).
2) Convert the alphabet values of the special feature to numeric values.
3) From normal dataset and DDoS dataset (Total 526,655 record), the dataset were divided into 3 series which different classes as follows:
   a) *Series 1* has 2 classes: normal data and DDoS attack which converted from 6 classes to 1 class which is attacks.
   b) *Series 2* has 6 classes: the dataset that get rid of normal data. The remaining data are DDoS attacks. There are Neptune, Pod, Smurf, Teardrop, Land and Back.
   c) *Series 3* has 7 classes: the dataset contains Neptune, Pod, Smurf, Teardrop, Land, Back and Normal.

IV. Experimental Setting and Results

This research is a research on the security of computer networks for identifying DDoS attacks using the 4,898,431 KDD Cup 1999 dataset and 125,373 NSL-KDD dataset. Those dataset are normal data and computer network intrusion data.

A. Parameter Tuning

Classification on information of machine learning were conducted by modeling both sets of data for DDoS attacks classification and identification. Training data and testing data were divided by cross validation method (given, $k = 2$). Then, both dataset were classified by MLP, SVM and KNN. The Parameter Tuning were as follows:

1) *KNN* is the identification of information by distance detection K position which get majority vote or nearest distance value. Given $K = 1, 3, 5, 7, 9$ to find the parameter for the test that aim to give the highest accuracy.
2) *SVM* [12,13] is a discriminative classifier formally defined by a separating hyperplane. The data classification which presented in this research apply grid search method to find suitable parameter for SVM. The testing parameter were as follows. Kernel function were set as RBF and linear. Gamma γ were set as between $1e-3$ and 1000. C were set as between $1e-3$ and 1000 to calculate the best parameter.
3) *MLP* applying grid search method to find the parameter. The test were set hidden layer as 10, 50, 100, 150, 200, 500, 1000. alpha were set as 1e-05, 1000, ... , 0.0001, 0.00001 and use the same methods as Adam [16] which works great when the data is large.

B. Experimental Results

There are three machine learning methods of classifying DDoS attacks in this research including, 1) K-Nearest Neighbor (KNN), 2) Support Vector Machine (SVM), and 3) Multi-Layer Perceptron (MLP). The accuracy equation [16] is as follows.

$$ACC = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{3}$$

where True Positive (TP): refer to predictions is true and confirm that is true.

True Negative (TN): refer to predictions is not true and confirm that is not true.

False Positive (FP): refer to predictions is true and confirm that is not true.

False Negative (FN): refer to predictions is not true and confirm that is true.

TABLE I: Accuracy Results of the KDD Dataset

Methods	Parameters Setting	Accuracy (%)
KDD 2-Class+SVM	rbf kernel, $C = 8, \gamma = 16$	98.946± 0.022
KDD 2-Class+KNN	$K = 3$	**99.983± 0.003**
KDD 2-Class+MLP	Hidden layer = 150	98.833± 0.131
KDD 6-Class+SVM	rbf kernel, $C = 8, \gamma = 32$	98.781± 0.020
KDD 6-Class+KNN	$K = 3$	**99.998± 0.002**
KDD 6-Class+MLP	Hidden layer = 20	99.981± 0.131
KDD 7-Class+SVM	rbf kernel, $C = 4, \gamma = 32$	99.096± 0.027
KDD 7-Class+KNN	$K = 3$	**99.984± 0.002**
KDD 7-Class+MLP	Hidden layer = 500	99.944± 0.019

TABLE II: Accuracy Results of the NSL-KDD Dataset

Methods	Parameters Setting	Accuracy (%)
NSL-KDD 2-Class+SVM	rbf kernel, $C = 1, \gamma = 32$	91.171± 0.194
NSL-KDD 2-Class+KNN	$K = 3$	**99.191± 0.044**
NSL-KDD 2-Class+MLP	Hidden layer = 200	98.091± 0.265
NSL-KDD 6-Class+SVM	rbf kernel, $C = 4, \gamma = 16$	95.364± 0.603
NSL-KDD 6-Class+KNN	$K = 3$	**99.951± 0.026**
NSL-KDD 6-Class+MLP	Hidden layer = 150	98.730± 1.200
NSL-KDD 7-Class+SVM	rbf kernel, $C = 1, \gamma = 16$	91.182± 0.183
NSL-KDD 7-Class+KNN	$K = 3$	**99.087± 0.076**
NSL-KDD 7-Class+MLP	Hidden layer = 100	98.066± 0.137

The accuracy results of the DDoS attack classification test with KDD CUP 1999 dataset and NSL-KDD dataset are showed at Table I and Table II, respectively.

In this paper, the data divided by cross validation method. The data were divided into two parts ($k = 2$) and tested 10 iterations. Starting with the KDD CUP 1999 dataset, the results found KNN had the best performance for all three subsets (2 Classes, 6 Classes, and 7 Classes). The accuracy rate were 99.98%, 99.99% and 99.98%, respectively which is very effective when compared to SVM and MLP. Then, testing with the NSL-KDD dataset which were also divided into three subsets. The results found that the KNN method had better performance than MLP and SVM with the three subsets data. The accuracy rate were 99.19% for NSL-KDD (2 Classes), 99.95% for NSL-KDD (6 Classes), and 99.08% for NSL-KDD (7 Classes).

V. Conclusion

In this research, machine Learning including; KNN, MLP and SVM were used to identify DDoS attacks. Two benchmark dataset which is 529,655 records of KDD CUP 1999 dataset and 12,354 records of NSL-KDD dataset. Those two dataset were divided into three subordinate dataset. There are 2, 6 and 7 classes for accuracy test of classification of DDoS attacks. When testing were conducted for 10 iterations, the result showed that KKN method obtained the best performance when compare with MLP and SVM with the accuracy rate 99.99%. In the future, researchers have planned to find a special feature that could possible to reduce the number of features. At the same time, it must not reduce the accuracy rate. Then, experiment with other types of attacks.

Acknowledgment

This research was supported by the Rajamanjala University of Technology Isan, Surin Campus, Thailand.

References

[1] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," in *Systems, Man, and Cybernetics (ICSMC), IEEE International Conference on*, vol. 3, Oct 2000, pp. 2275–2280 vol.3.

[2] D. Peraković, M. Periša, I. Cvitić, and S. Husnjak, "Artificial neuron network implementation in detection and classification of DDoS traffic," in *24th Telecommunications Forum (TELFOR)*, Nov 2016, pp. 1–4.

[3] C. Hsieh and T. Chan, "Detection DDoS attacks based on neural-network using apache spark," in *Applied System Innovation (ICASI), International Conference on*, May 2016, pp. 1–4.

[4] S. Devaraju and S. Ramakrishnan, "Performance analysis of intrusion detection system using various neural network classifiers," in *Recent Trends in Information Technology (ICRTIT, International Conference on)*, Jun 2011, pp. 1033–1038.

[5] T. Omrani, A. Dallali, B. C. Rhaimi, and J. Fattahi, "Fusion of ANN and SVM classifiers for network attack detection," *CoRR*, vol. abs/1801.02746, pp. 1–5, Jan 2018. [Online]. Available: http://arxiv.org/abs/1801.02746

[6] Information and Computer Science, "KDD cup 1999 data," Oct 1999. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[7] S. Yuanyuan, W. Yongming, G. Lili, M. Zhongsong, and J. Shan, "The comparison of optimizing SVM by GA and grid search," in *Electronic Measurement Instruments (ICEMI), 13th IEEE International Conference on*, Oct 2017, pp. 354–360.

[8] P. Singh and A. Tiwari, "An efficient approach for intrusion detection in reduced features of KDD99 using ID3 and classification with KNNGA," in *Advances in Computing and Communication Engineering ICACCE, 2nd International Conference on*, May 2015, pp. 445–452.

[9] D. H. Deshmukh, T. Ghorpade, and P. Padiya, "Intrusion detection system by improved preprocessing methods and naïve bayes classifier using NSL-KDD 99 dataset," in *Electronics and Communication Systems (ICECS), International Conference on*, Feb 2014, pp. 1–7.

[10] P. Kushwaha, H. Buckchash, and B. Raman, "Anomaly based intrusion detection using filter based feature selection on KDD-CUP 99," in *IEEE Region 10 Conference TENCON*, Nov 2017, pp. 839–844.

[11] G. Meena and R. R. Choudhary, "A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA," in *Computer, Communications and Electronics (Comptelix), International Conference on*, Jul 2017, pp. 553–558.

[12] O. Surinta, M. F. Karaaba, L. R. Schomaker, and M. A. Wiering, "Recognition of handwritten characters using local gradient feature descriptors," *Engineering Applications of Artificial Intelligence*, vol. 45, pp. 405 – 414, 2015.

[13] V. N. Vapnik, *Statistical Learning Theory*. Wiley, 1998.

[14] A. G. Gedam and S. G. Shikalpure, "Direct kernel method for machine learning with support vector machine," in *Intelligent Computing, Instrumentation and Control Technologies (ICICICT), International Conference on*, Jul 2017, pp. 1772–1775.

[15] J. Wu, X. Wang, X. Lee, and B. Yan, "Detecting DDoS attack towards DNS server using a neural network classifier," in *Artificial Neural Networks (ICANN), 20th International Conference on*, K. Diamantaras, W. Duch, and L. S. Iliadis, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 118–123.

[16] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*. Elsevier, 2011.