CLASSIFICATION DENIAL OF SERVICE (DOS) ATTACK USING ARTIFICIAL NEURAL NETWORK LEARNING VECTOR QUANTIZATION (LVQ)

Reza Firsandaya Malik
Computer Engineering Department
Faculty of Computer Science, Sriwijaya University
Palembang, Indonesia
reza.firsandaya@gmail.com

Verlly Puspita
Computer Engineering Department
Faculty of Computer Science, Sriwijaya University
Palembang, Indonesia
verlly.droger@gmail.com

***Abstract*— Network security is an important aspect in computer network defense. There are many threats find vulnerabilities and exploits for launching attacks. Threats that purpose to prevent users get the service of the system is Denial of Service (DoS). One of software application that can detect intrusion on is an Intrusion Detection System (IDS). IDS is a defense system to detect suspicious activity on the network. IDS has ability to categorize the various types of attack and not attack. In this research, Learning Vector Quantization (LVQ) neural network is used to classify the type of attacks. LVQ is a method to study the competitive supervised layer. If two input vectors approximately equal, then the competitive layers will put both the input vector into the same class. The results show IDS able to classify PING and UDP Floods are 100%.**

Keywords: Network Security, Denial of Service (DoS) , IDS , Learning Vector Quantization (LVQ).

I. INTRODUCTION

The development of computer technology brings many aspects to human. One is a DoS (Denial of Service) against a computer system connected to the Internet. As a consequence, many computer systems or networks disrupted even be damaged. To overcome this, we need a security system that can cope and prevent activities that may attack the system network. Conventional technologies commonly used *signature base* method to detect a type of attack, the weakness of this method cannot detect new types of attacks that the signature is not found in the database, so that when the attacker used another type of attack that have been modified from previous attacks, it is possible that the attack will succeed and is not detected by the system. One method that can be used to detect new attack patterns is by using artificial neural networks, for example Learning Vector Quantization (LVQ). LVQ is a prototype based classification supervise algorithms. The purpose of this algorithm is to approximate the distribution of the vector class in minimize of errors when classification.

II. DENIAL OF SERVICE AND LEARNING VECTOR QUANTIZATION (LVQ)

A. Denial of Service (DoS)

A Denial of Service attack is commonly characterized as an event in which a legitimate user or organization is deprived of certain services, like web, email or network connectivity, that they would normally expect to have. DDoS is basically a resource overloading problem. The resource can be bandwidth, memory, CPU cycles, file descriptors, buffers etc. The attackers bombard scare resource, either by flood of packets or a single logic packet which can activate a series of processes to exhaust the limited resource [1].

DoS attack may target on a specific component of a computer, entire computer system, certain networking infrastructure, or even entire Internet infrastructure. Attacks can be either by exploits the natural weakness of a system, which is known as logical attacks or overloading the victim with high volume of traffic, which is called flooding attacks. The main problem is that there are still many insecure machines over the Internet that can be compromised to launch large-scale coordinated DoS attack. One promising direction is to develop a comprehensive solution that encompasses several defense activities to trap variations of DoS attack. If one level of defense fails, the others still have the possibility to defend against attack [2].

A logic DoS attack is based on an intelligent exploitation of vulnerabilities in target. For example, a skillfully constructed fragmented IP datagram may crash a system due to a serious fault in the operation system (OS) software. Another example of a logic attack is to exploit missing authentication requirements by injecting bogus routing

information to prevent traffic from reaching the victim's network [3].

B. Learning Vector Quantization

LVQ network has three layers, is an input layer, a Kohonen layer, and output layers. An LVQ network has a first competitive layer and a second linear layer. The competitive layer learns to classify input vectors in much the same way as the competitive layers of Self-Organizing Feature Maps. The linear layer transforms the competitive layer's classes into target classifications defined by the user. The classes learned by the competitive layer are referred to as subclasses and the classes of the linear layer as target classes [4].

Prototype network is given by W = (w (i), ... w (n))). It will change the weights of the network to classify the data correctly. For each data point, the prototype (neurons) that is closest to the specified (called the winner neuron). Connection weights are then adapted to the neurons, which are made more close if classification of data is correct or if the classification is made less close one. One advantage of LVQ is to create a prototype that is easy to interpret the experts in certain fields.

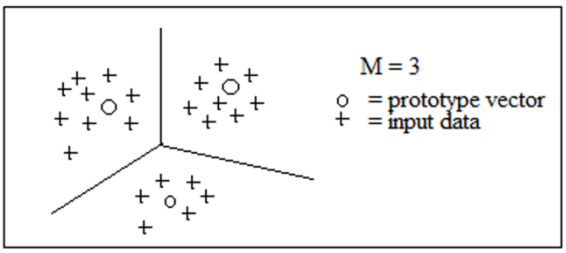

Fig. 1. Vector Quantitation

We assume that the codebook is defined by a set of prototype vector M (M selected by the user and any initial vector chosen prototype). Input will always be included in the cluster I if I is the index of the nearest prototype (Euclidean Distance) [5].

In terms of neural networks a LVQ is a feedforward net with one hidden layer of neurons, fully connected to the input layer. A codebook Vector (CV) can be seen as a hidden neuron ('Kohonen neuron') or a weight vector of the weights between all input neurons and the regarded Kohonen neuron respectively [6].

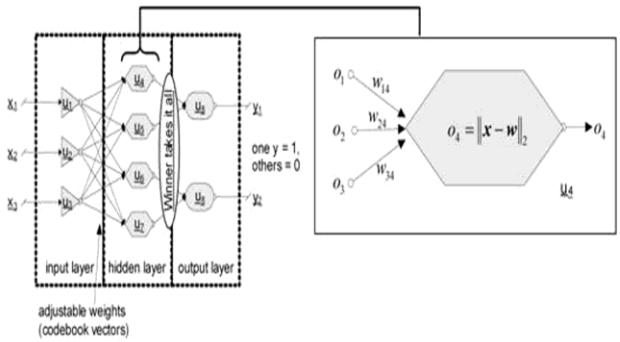

Fig. 2. LVQ Concept

Learning means modifying the weights in accordance with adapting rules and, therefore, changing the position of a CV in the input space. Since class boundaries are built piecewise-linearly as segments of the mid-planes between CVs of neighboring classes, the class boundaries are adjusted during the learning process. The tessellation induced by the set of CVs is optimal if all data within one cell indeed belong to the same class.

III. Related Works

One of the researches about classification type of attacks using artificial neural network, Self Organizing Maps (SOM) is work done by Bambang Tutuko, Siti Nurmaini and Dearby Suganda [7]. Based on the results using SOM learning that has been done, the success rate for normal conditions by 80%, UDP flood 100%, and ping flood 90%. While the research conducted by Mehdu Muradi and Mohammad Zulkernine [8] using an artificial neural network Multi Layer Perceptron (MLP), can classify the data with an accuracy of 91% for two and 87% hidden layer with only one hidden layer. Besides that, Abdulkader A. Alfantookh [9] also have research about Denial of Service Intelligent Detection (DoSID). The type of Neural Network used to implement DoSID is feed forward, which uses the backpropagation learning algorithm. The data used in training and testing are the data collected by Lincoln Labs at MIT for an intrusion detection system evaluation sponsored by the U.S. Results show that normal traffic and know the attacks are discovered 91% and 100% respectively. Identifying DoS attack using data pattern analysis, such as Holt-Winter or Linear Regression also researched by Mohammed Salem and Helen Armstrong [10]. However, The ANN not the only method to classify DOS attacks. Gulay Oke, George Loukas and Erol Gelenbe has purposed detecting Denial of Service Attacks method using Bayesian Classifiers and the Random Neural Network [11]. They used such an RNN structure to fuse real-time networking statistical data and distinguish between normal and attack traffic during a DOS attack.

IV. Methodology

This section will explain the methodology that will be used to solve problem classification DoS Attack using

artificial neural networks Learning Vector quantization (LVQ). The output of research is software to classify types of attack has been determined and able to recognize new types of attacks.

A. IDS Model

IDS Model builds with several steps: generate packet traffic, and classify data input.

1) Generate Packet Traffic

Record of data is done by using two computers, which one computer as attacker and other computer as victim. These types of attacks that will be used is a DOS attack (ping flood and UDP flood).

PING Flood a condition in which the attacker sends ICMP echo request packets to the target computer IP packet exceeds the maximum size that is 65,536 bytes. Therefore ICMP echo request packet larger than normal, then the packet must be broken [12].

UDP flood attack occurs when an attacker sends UDP packets to random ports to target system and sends a number of packets of data continuously with the same size [13].

Traffic between two computers is captured using wireshark. Normal traffic will be compared with attack traffic to get the parameter. That parameter will be used for input of neural network Learning Vector Quantization (LVQ). And the output of neural network has three classes, that is normal, UDP flood and PING flood.

2) Classify Data Input

In designing the classification DoS attack with the neural network will use the types of DOS attacks as input information. The collected data contained a variety of protocol activities such as IP, ICMP and UDP.

B. Develop Classification DoS Attack Software

Characteristic data obtained from the experiments with a ping flood attack and UDP flood will be used as input for training and testing process using LVQ. Previously these data will be used as a form of binary (0 and 1) first so that the programming process can be done. We use the C++ program for processing the data for training and testing.

V. EXPERIMENT

A. Attack Experiment

1) Ping Flood

Ping flood attack is done by using two computers, where one computer as an attacker and the other one as the target computer, which is connected with a LAN cable. Flooding process is done by regular ping in command prompt, but the length of the data is converted to 65,500 bytes. Topology of Ping flood attack shown in Figure 3.

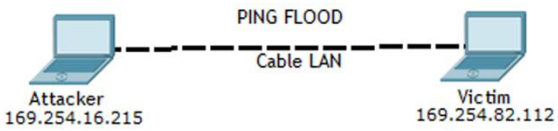

Fig. 3. Ping Flood Attack Topology

Analysis of normal traffic and ping flood on the network using wireshark application. After getting captured of the normal ping and ping flood, it will show the difference between the both is shown in Table 1.

TABLE I. DIFFERENCE PING NORMAL AND PING FLOOD

No	Characteristic	Ping Normal	Ping Flood
1	Time between echo request and echo reply	$< 5ms$	$\geq$ 5ms
2	Session	4 Session	88 Session
3	Fragment processed	0	44 Session
4	Reassemble processed	0	44 Session

2) UDP Flood

UDP attack utilities the characteristic of the UDP protocol, which is connectionless or send messages without having to make the process of negotiating the connection between the two hosts when exchange information. So that a large number of data packets that can be sent to the target. Attack tool that is used in this experiment is Warflood. Attack topology to get a data UDP Flood is shown in Figure 4.

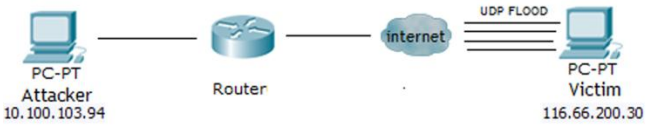

Fig. 4. Topology Attack with UDP Flood

The condition occurs when the UDP flood attack is shown in Figure 5.

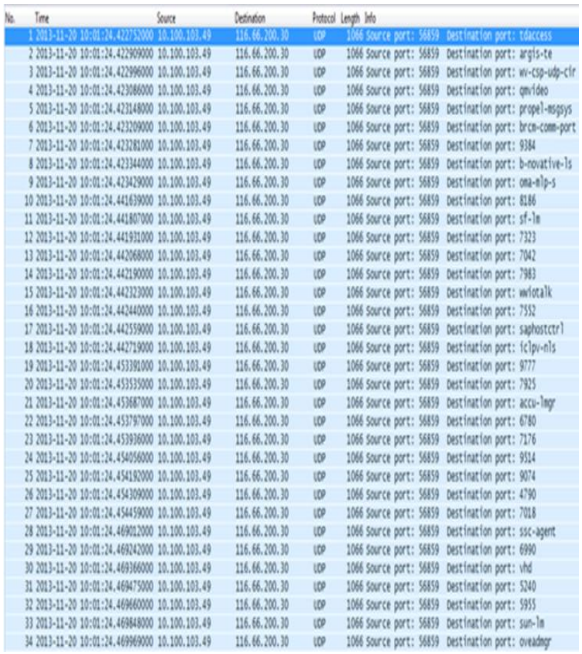

Fig. 5. UDP Flood

To obtain specific characteristics, then do a comparison between the normal UDP with UDP flood. Differences normal UDP with UDP flood is shown in Table 2.

TABLE II. DIFFERENCE UDP NORMAL AND UDP FLOOD

No	Characteristic	Ping Normal	Ping Flood
1	Average Packet per Second	39 Packet	100 Packet
2	Data Length	Varies	Similar
3	Size of Data	225 bytes	1,054 bytes
4	Source Port	< 45000	> 45000

3) Features

The selection of features is one of the most important factors in improving the accuracy of identifying the type of attack. Because the feature is to be used as input of the artificial neural network Learning Vector Quantization (LVQ) and get the learning process. In this paper, a feature that is obtained is the result of observation of normal conditions and conditions in the event of an attack (ping flood and UDP flood) in the network. That feature shown in Table 3.

TABLE III. FEATURES

No	Protocol	Features
1	ICMP	Echo ping reply fragmented
2	ICMP	Echo ping reassembled
3	ICMP	Frame length > 74 bytes
4	IP	Same request in specified time
5	IP	Total length > 1,400 byte
6	IP	Data send 32 bytes
7	UDP	Source port > 45000
8	UDP	Size of data
9	UDP	Time request in second

VI. EXPERIMENT RESULT

1) LVQ Architecture

Initialize the value of alpha, target error and decrement alpha are the beginning of a process of learning and testing. The amount of data that will be used as training and testing is 27 data, consisting of 9 data traffic normal, 9 data UDP flood and 9 data ping flood.

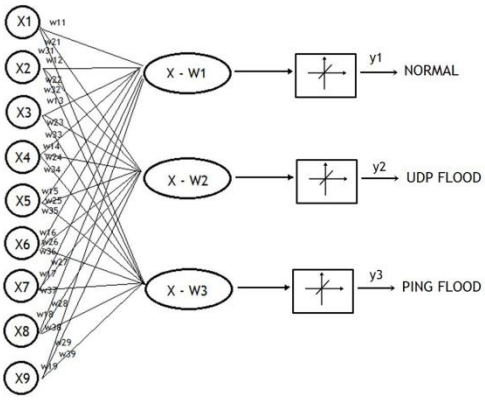

Fig. 6. LVQ Architecture

Processing that occurs at each neuron is finding the distance between an input vector to the weight. The process of finding the shortest distance is on Kohonen or competitive layer. The method used to find the shortest distance between vector input to weights are Euclidean Distance. Activation function (F) used in the LVQ network architecture is a linear function. The intention is that raised the same issue with the input according to the formula that is a linear function y = x. Formula of Euclidean distance which will be used as follows;

$$C=\sqrt{\sum (X-W)^2} \quad (1)$$

Where X is sign for the data and W for Weight.

2) Learning Rate of LVQ

Initialization process learning by setting the value of the learning rate (alpha) = 0.1, decrement alpha (dec alpha) = 0.1 and target error = 0.01. In addition, the weights are randomly selected that representing each target / class. Formula of alpha will be used as follows;

$$\alpha = \alpha - (\alpha * \text{dec}\alpha) \quad (2)$$

The results obtained with the value of learning rate (alpha) = 0.1, decrement aplha (dec alpha) = 0.1, minimum or target alpha error = 0.01 and a maximum epoch = 1000, still have errors in classifying types of attacks. Therefore, a process changes the value of the target error become 0.00001, and find the value of alpha and dec alpha that are close to the target error to reduce the error value when done grouping types of attacks.

TABLE IV. MINIMUM ERROR VALUE

No	Alpha	Dec Alpha	Max Epoch	Iteration stoped At Epoch	Minimum Error Value (10^{-5})
1.	0.01	0.1	15,000	88	1.044956207
		0.01		917	1.004241949
		0.001		9206	1.000731845
2.	0.025	0.1	15,000	75	1.027745202
		0.01		779	1.004896694
		0.001		7,821	1.000131761
3.	0.25	0.1	15,000	97	1.01209389
		0.01		1,008	1.005960712
		0.001		10,122	1.000566408
4.	0.50	0.1	15,000	103	1.075736327
		0.01		1077	1.005632657
		0.001		10815	1.000367047
5.	0.70	0.1	15,000	106	1.097896256
		0.01		1,111	1.000378506
		0.001		11,151	1.0006700363
6.	1.0	0.1	15,000	110	1.029042596
		0.01		-	-
		0.001		-	-

The comparison of the value of alpha (0:01, 0.025, 0:25, 0:50, 0.70 and 1.0) and dec alpha (0.1, 0:01, and 0001) in Table 4 are close to the target values obtained 0.00001 error is when the alpha-value 0.025 and a dec alpha-value 0.001. The learning process stops at the epoch to-7,821 and the minimum error value is 1.000131761 x 10^{-5}. When alpha - values have changed become 1.0 and 0.01, training process cannot be done. It has happened because the process of learning rate that is too fast and has reached more than the maximum specified epoch.

Thus, Alpha value is set to be 0.025, target of 0.00001 and a decrease in alpha error 0.001. In addition the maximum value of epoch also changed to 15,000.

The test results after the change in the value of alpha, decrement alpha, and the maximum epoch can minimize the error to classify types of attack that are equal to 3.70% when the previous error value reached 7.40%.

TABLE V. TESTING VALUE

No	Alpha	Dec Alpha	Target Error	Max. Epoch	Error Value
1.	0.1	0.1	0.01	1000	7,40 %
2.	0.025	0.001	0.00001	15000	3,70 %

3) Testing with New Input

One of the advantages using the artificial neural network method compared to *signature-based* method is able to recognize new attack patterns. Table 6 shown the result LVQ classify new attack patterns.

TABLE VI. TESTING WITH NEW INPUT

Data	Xi1	Xi2	Xi3	Xi4	Xi5	Xi6	Xi7	Xi8	Xi9	Class
1	0	0	0	0	0	0	1	0	0	normal
2	0	0	0	0	0	0	0	1	0	normal
3	0	0	0	0	0	0	0	0	1	normal
4	0	0	0	1	1	1	1	1	1	UDP
5	0	0	0	0	0	0	1	1	1	UDP
6	0	0	0	0	1	0	1	1	1	UDP
7	0	0	0	0	0	0	1	1	0	normal
8	1	1	1	1	1	1	0	0	0	PING
9	1	1	1	1	1	0	0	0	0	PING

Test results using the input that did not through the learning process has a one error from 11 new patterns, which is a characteristic 000000110 closer into UDP flood conditions. However, the test results showed that the characteristics included in normal class.

VII. CONCLUSION AND FUTURE WORK

Classification DoS attack using artificial neural network learning vector quantization (LVQ) can detect known (ping flood and UDP flood) and unknown attack (new patterns) efficiently.. The success rate of classification using LVQ is for normal conditions 90%, 100% PING flood, UDP flood and 100%. While in recognizing new patterns of attack gained success rate was 90.9%. Determination of the value of alpha, determent alpha, the maximum epoch greatly affects the value of the error obtained.

Characteristic for the future work and the amount of input data can be propagated to the results of training with artificial neural network is more accurate in identifying new attack patterns.

REFERENCES

[1] K. Kumar, R.C. Joshi and K. Singh, "An Integrated Approach for Defending against Distributed Denial-of-Service (DDoS) Attacks", iriss, 2006, IIT Madras.

[2] B. B. Gupta, "Distributed Denial of Service Prevention Techniques", International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010, 1793-8163

[3] Jarmo Mölsä, "Mitigating denial of service attacks: A tutorial", Journal of Computer Security 13 (2005) 807–837

[4] Reyadh Shaker Naoum and Zainab Namh Al-Sultani, " Learning Vector Quantization (LVQ) and k-Nearest Neighbor for Intrusion Classification", World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 3, 105-109, 2012

[5] Atuti, Erna Dwi. 2009. Introduction Artificial Neural Network Theory and Aplication. Center Java: Star Publising.

[6] Sven F. Crone, "forecasting with artificial neural networks", http://www.neural-forecasting.com/lvq_neural_nets.htm

[7] Suganda, Dearby,"Design of Intrusion Detection System Using Self-Organizing Maps", Sriwijaya University, 2012,Unpublished.

[8] M. Moradi and M. Zulkernine, "A neural network based system for intrusion detection and classification of attacks", In 2004 IEEE International Conference on Advances in Intelligent Systems.

[9] Abdulkader A. Alfantookh, "DoS Attacks Intelligent Detection using Neural Networks", Journal of King Saud University - Computer and Information Sciences,Volume 18, 2006, Pages 31–51

[10] Mohammed Salem and Helen Armstrong, "Identifying DoS Attacks Using Data Pattern Analysis", Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, Ist to 3rd December 2006.

[11] Gulay ¨ Oke, George Loukas, and Erol Gelenbe. "Detecting Denial of Service Attacks with Bayesian Classifiers and the Random Neural Network", In IEEE Fuzzy Systems Conference, London, 2007.

[12] Bogdanoski, Mitko and Aleksandar Risteski,"Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques",Military Academy,Macedonia,2011.

[13] Duraiswany and G. Palenivel, "Intrusion Detection System in UDP Potocol". King College of Engineering,2010.