An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine

Keisuke Kato, Vitaly Klyuev
Department of Computer Science and Engineering
The University of Aizu, Japan

Abstract

Nowadays, many companies and/or governments require a secure system and/or an accurate intrusion detection system (IDS) to defend their network services and the user's private information. In network security, developing an accurate detection system for distributed denial of service (DDoS) attacks is one of challenging tasks. DDoS attacks jam the network service of the target using multiple bots hijacked by crackers and send numerous packets to the target server. Servers of many companies and/or governments have been victims of the attacks. In such an attack, detecting the crackers is extremely difficult, because they only send a command by multiple bots from another network and then leave the bots quickly after command execute. The proposed strategy is to develop an intelligent detection system for DDoS attacks by detecting patterns of DDoS attack using network packet analysis and utilizing machine learning techniques to study the patterns of DDoS attacks. In this study, we analyzed large numbers of network packets provided by the Center for Applied Internet Data Analysis and implemented the detection system using a support vector machine with the radial basis function (Gaussian) kernel. The detection system is accurate in detecting DDoS attacks.

1. Introduction

In past years, the news about distributed denial of service (DDoS) attack is rapidly increased around the world. Many services of companies and/or governments are victims of the attack. A hacker groups developed tools to execute DDoS attack very easily and sell them to many people. As the results, DDoS attacks became one of most harmful attacks in network security.

The main purpose of DDoS attacks is to jam the service for a long time, rather than to steal money or data from the targets. Since a user might not re-use services jammed by crackers, a company attacked by the crackers will lose many benefits. A DDoS attack can be initiated from many computers hijacked by crackers, and then every computer will send large numbers of packets to the target server simultaneously. The server attempts to respond to all the packets, but its bandwidth gets exhausted very quickly and the service stops. A cracker who has hijacked many computers only sends some attack commands to the hijacked computers. These computers can be connected to multiple bots either directly or through a botnet. Consequently, detecting a cracker is extremely difficult. Hence, it seems that the right strategy is to detect DDoS attacks rather than the crackers.

To develop a detection system for DDoS attacks, we obtained an actual DDoS attack dataset and utilized machine learning techniques to analyze the data. The dataset was provided by the Center for Applied Internet Data Analysis (CAIDA) and had a total size of 44 gigabytes. In this study, we analyzed this large dataset and developed the detection system using a support vector machine (SVM).

This paper is based on study [20]. The remainder of this paper is organized as follows. In Section 2, we review publications in the area of this research. In Section 3, we present the details of Dataset and data analysis [1]. In Section 4, we discuss the DDoS attack by calculating bytes per second. In Section 5, we evaluate and discuss the detection system using an SVM. In Section 6, we highlight our significant findings.

2. Related Work

Scientists can find many studies on protection against DDoS attacks. Proposed methods utilize various algorithms and techniques.

Studies utilized machine learning techniques and algorithms [2] [3] [4]. Study proposed an anomaly-based DDoS detection system using radial basis function (RBF) neural networks [3]. The proposed system was examined using a dataset from UCLA, and the results showed that the system could achieve real-time DDoS attack detection accuracy of more than 96 %. The goal of Agrawals study was to predict the number of zombies in DDoS attacks using an SVM [3]. The found predicted number is very close to the actual number of zombies. Another study introduced a statistical preprocessor and an unsupervised artificial neural network as a tool for detecting DDoS attacks [4].

Limwiwatkul's study discovered the DDoS attacking signature by analyzing TCP/IP packet headers against the well-defined rules and conditions, and distinguished the difference between

normal and abnormal traffic [5]. The authors could obtain some sample signatures of the basic DDoS attack. A study by Zhang discussed a prediction-based detection algorithm against DDoS attacks [6]. Based on the proposed prediction, they could detect abnormal states of the server that may be caused by DDoS attacks. Other studies used entropy for developing a detection system [7] [8]. Study by Navaz proposed a statistical approach using joint entropy for DDoS attack detection and also used the CAIDA dataset containing information for denial of service attacks [8]. This study calculated entropy for packets, with IP addresses, ports, and flow size as inputs, and compared normalized entropy with that of the assigned threshold value. The threshold value depends primarily on the false positive rate.

Zhong analyzed the characteristics of DDoS attacks and the DDoS attack detection method using a data-mining algorithm [9]. The fuzzy c-means (FCM) clustering algorithm and Apriori association algorithm were used to extract features in network traffic. Study by Bhuyan presented a survey with the results of DDoS attacks, detection methods, and tools used in wired networks [10]. Mirkovic proposed a source-based DDoS attack detection system, D-WARD [11]. This system is installed at the edge routers of a network and monitors the behavior of each peer with which the source network communicates. D-WARD can detect many common patterns of DDoS attacks. Other studies classified types of DDoS attack and defense mechanisms [12]. Another study presented the design of a general triggered framework for scalable threat analysis for large-scale automated systems [14]. According to CSI survey in 2007, DDoS attacks were recognized as one of the major causes of financial losses [14].

Aforementioned studies do not investigate the patterns of the attackers. In this paper, we focus on this topic.

3. Dataset and Big Data Analysis

In this section, we show the details of the dataset and some important outcomes that we obtained analyzing the data and discuss some difficulties of developing the DDoS attack detection system by comparing the data analysis of the attacker and victims [1].

3.1. DDoS Dataset

To develop a DDoS attack detection system utilizing machine learning techniques and algorithms, we need an actual DDoS dataset to detect and learn patterns of DDoS attack. However, we do not have such dataset and in any study on DDoS attacks, collecting data is a challenging task: It is difficult for any researcher to collect appropriate datasets of actual DDoS attacks. However, there are some alternative methods. One of them is to set up an environment that can generate simulated network communication data. We can use tools such as NS-2, Qualnet, or OMNet++. However, in this study, the goal is to develop a detection system that can predict a forthcoming attack and detect the attack before the bandwidth is exhausted by using machine learning techniques. Some institutions provide such datasets. The 2000 U.S. Defense Advanced Research Projects Agency (DARPA) Intrusion Detection Evaluation Dataset and Knowledge Discovery and Data Mining (KDD) Cup 1999 Dataset are the most popular publicly available datasets, but the first one was created prior to ten years and the second one is not suitable for DDoS attacks [10]. We used CAIDA DDoS Attack 2007 Dataset to analyze the actual DDoS attack data and utilize them for training data patterns [1].

This dataset contains approximately one hour of anonymized traffic traces that include the attack traffic on the victims and the response from the victims on August 4, 2007. The total size of the original dataset is 21 gigabytes. The type of the file is the packet capture file. Since there are few applications to read these data, we exported all the data to comma-separated value files for easy data reading in any programming language and machine. The total size of final dataset increased to 44 gigabytes and the total number of packets we analyzed was 359,655,765 from the attacker and 12,131,655 from the victim.

3.2. Data Analysis

The size of the dataset that we obtained is big and analyzing all data takes very long time. So, to analyze the dataset efficiently and quickly, we extracted some features including source IP address, destination IP address, time interval in seconds between packets, and packet size in bytes from the dataset. We analyzed the total number of packets that were sent from the attacker and victim, the mean time intervals in seconds, and mean packet size in bytes for each packet. Table 1 shows the summary of dataset statistics for each feature from the attacker and victim. Figure 1 shows that the most common mean packet size for each IP address is almost the same for the attacker and victim. In addition, the maximum and minimum packet sizes are 1,500 and 46 bytes for the attacker and 1,474 and 40 bytes for the victim. Figure 2 shows the packet flow of the total victim's packets and 12,895,257 (3.5%) of the attacker's packets. This 3.5% of packets are generated by the uniform random number block. These results show that there are no significant differences distinguishing attack packets from normal packets except for the total number of packets. Therefore, detecting DDoS attacks from individual packet data is extremely difficult, because

some of their packets are very similar, and the maximum and minimum packet sizes for attackers and victims are almost the same in terms of size.

However, in the data analysis for each IP address, we found that their respective results differ for each feature, if we set some conditions. Table 2 shows the results under the condition that the total number of packets is greater than two and the time interval is less than 0.01 seconds. These conditions cover about 50% of the attacker's IP addresses and 91% of network packets, but most of the victim's data are not covered under this condition. Consequently, we can find some important patterns to detect DDoS attacks, when we analyze packet data for each IP address under different conditions. These patterns are very helpful for developing a DDoS attack detection system.

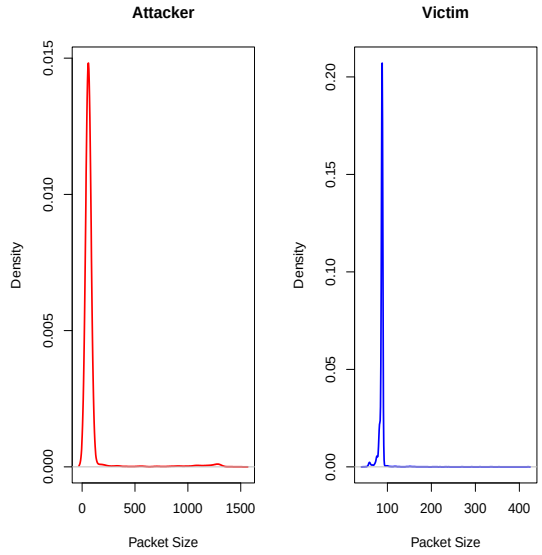

Figure 1. Density of Packet Size for Each IP Address

Figure 3 shows the frequency of the mean time interval for each attacker's IP address under the aforementioned condition. Figure 4 shows how mean time intervals for each IP address are different for attackers and victims under the condition. The attacker's condition is the same condition that we aforementioned and the victim's condition is that the total number of packets is greater than two and the time interval is less than 0.3 seconds. These conditions cover about 63% of the IP addresses and 91% of the network packets in the victim's packet data. Therefore, the ratio of packet data is almost the same as in the attacker's condition, as shown in Table II. Consequently, we see that the attacker's time interval is very short and the victim's is long, because the attacker must send many packets at the same time.

Under the victim's condition, the mean time interval is 0.1584 seconds, and the mean packet size is 87.47 bytes. While the mean size of all attacker packets is greater than the size of all victim packets, the mean size of the attacker's packet is less than the victim's size for about 91% of the packets. In addition, the maximum packet size is 1,500 bytes in all of the attacker's packets and 1,474 bytes in all of the victim's packets, but when we analyze all packets for each IP address, the maximum packet size is 1,490 bytes for the attacker and 420 bytes for the victim. Therefore, the attacker will send some large packets and a huge number of small packets.

We demonstrated some differences between the attacker and victim. To develop the detection system, we utilized these differences as DDoS attacks patterns. Consequently, we utilized the total number of packets, mean time interval, mean packet size, number of packets per second, amount of bytes per second, and total amount of bytes for each IP address from our dataset.

Table 1. Results for Each Feature

	Total number of IP addresses	Total number of packets	Mean of time interval in sec	Mean of packet size in bytes
Attacker	9,311	359,655,765	0.3646	91.2169
Victim	9,325	12,131,655	0.7016	87.2543

Table 2. Results for Each Feature Under Conditions: Number of Packets > 2 and Time Interval < 0.01 sec

	Total number of IP addresses	Total number of packets	Mean of time interval in sec	Mean of packet size in bytes
Attacker	4,604	329,113,446	0.0048	60.3489
Victim	10	151	0.0067	100.6067

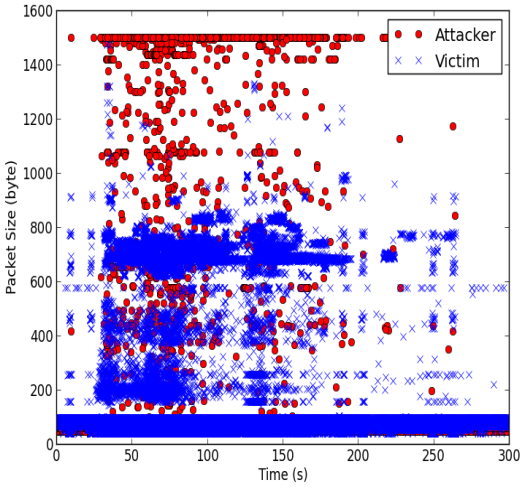

Figure 2. Attacker's and Victim's Packet Flow Illustration

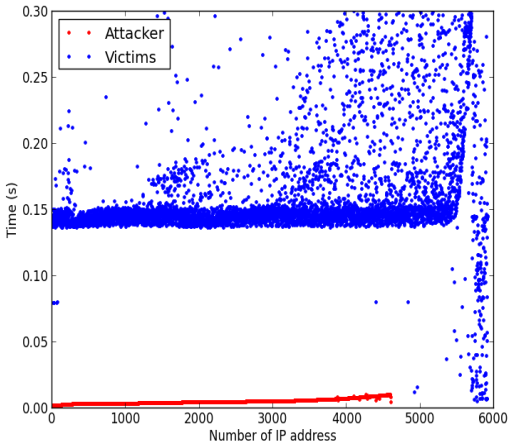

Figure 4. Difference of Mean Time Interval Between Attacker and Victim

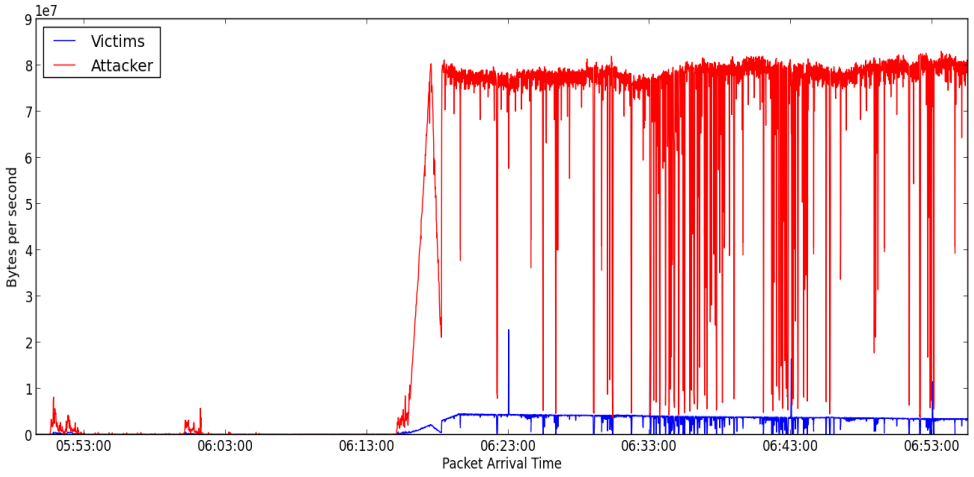

Figure 5. Bytes per Second with the Time Sequence

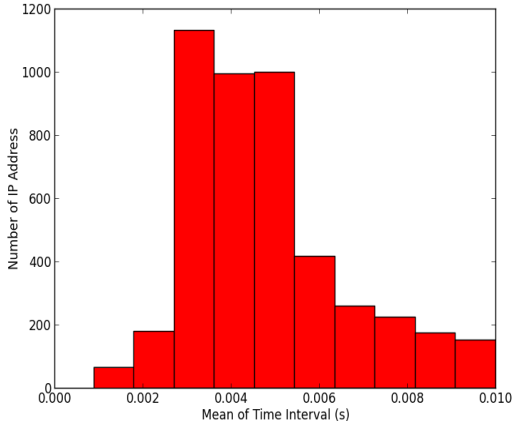

Figure 3. Frequency of Mean Time Interval for Attacker's IP Address

4. Analysis of DDoS attack

In this section, we analyze the DDoS attack by calculating bytes per second (bps). To plot the amount of bps with the time sequence, we try to find difficult points to develop an accurate DDoS attack detection system.

We calculated bps for all packet data and tried to detect the point when the attack started and difference in the amount of bytes between normal communication and abnormal communication. Figure 5 shows amount of bps for the attackers and victims. In this figure, the attacker does not quickly attack the victim after the communication begins. Looking at Figure 5, we can classify the attack mainly in two parts. Those are an incubation period to trick the victims into being normal

communication, and attacking period to execute commands and jam the services. We consider that the incubation time is about from 05:53 JST to 06:13 JST, and attacking period is about from 06:13 JST to 06:53 JST. The victim's server has started network communication with the attacker more than 20 minutes before they start attacking. However, it is difficult for victims to recognize that because the attacker is good at imitating normal communication. It means that the attacker can easily start network communication with victim's server and attack them anytime. After the incubation period, the attacker executes their commands and the victim's server receives abnormal amount of bytes in short time and keeps it for long time. Finally, the server's bandwidth is exhausted and the services will be jammed.

We considered that this problem makes developing the accurate DDoS attack detection system difficult to detect and/or predict the attack before the bandwidth of the victim's server is exhausted. In this study, we tried to develop the detection system considering this problem, but we could not achieve any good results. Tackling this problem will be our future work.

5. Experimental Results

In Section 3 and 4, we presented some important features of DDoS attacks. Utilizing these outcomes, we implemented a DDoS attack detection system and tested the accuracy of detection. In this section, we present the details of creating the training and test data, the algorithm that we utilized, and the detection system using an SVM with an RBF (Gaussian) kernel.

5.1. Training and Test Dataset

To compare the performance of the SVM with different datasets, we created three types of training and test datasets including different patterns and different number of patterns. One of the datasets (Dataset 1) has three features: the total number of packets, time interval, and the total amount of bytes for each IP address. Another dataset (Dataset 2) also has three another features: the number of packets per second, time interval, and the amount of bytes per second. In addition to this, Dataset 3 has five features: the total number of packets, time interval, the total amount of bytes, the number of packets per second, and the mean packet size. The number of packets in one second (*Npps*) and the amount of bytes per second (*Abps*) are calculated using (1) and (2).

$$Npps = \frac{1.0}{\frac{1}{N-1}\sum_{i=2}^{N} time(i) - time(i-1)} \qquad (1)$$

where N is the number of packets, and *time(i)* is the arrival time of the i^{th} packet.

$$Abps = Npps * \left(\frac{\sum_{i=1}^{N} size(i)}{N}\right) \qquad (2)$$

where N is the number of packets, and *size(i)* is the i^{th} packet size.

We analyzed all of 18,636 IP addresses based on 371,787,420 network packets from the dataset. To learn the patterns of a DDoS attack and test it using the SVM, we created training and test data from the initial dataset. However, the ratio of test and training data is one of important problem because the ratio may affect the detection accuracy. One study suggests 2/3 as a proportion of data to be used as a training set for data not meeting assumptions required for the application of parametric tests [17]. Some studies used up to 80% of data for training purposes [18] [19]. In this study, we executed the detection system using different ratio of test and training data. Table 3 shows the detection accuracies with each ratio of test and training data. We randomly selected 1864 (10%), 4000 (22%), 5591 (30%), and 6150 (34%) IP addresses for test data and 16772 (90%), 14636 (78%), 13045 (70%), and 12486 (66%) IP addresses for training data from the attacker and victim pool. As the results, there are some differences between each ratio of data in all datasets, but we could not find big differences. In Table 3, dividing the original dataset into 22% of test data and 78% of training data shows good accuracy with all datasets. Therefore, we selected 4,000 IP addresses consisting of 2,000 IP addresses from the attacker pool and 2,000 IP addresses from the victim pool as the test data. The remaining 14,636 IP addresses are selected as the training data.

Table 3. Detection Accuracy with Different Ratio of Test and Training Data

	Ratio of test and training data Test (%) : Training (%)			
	10:90	**22:78**	**30:70**	**34:66**
Dataset 1	0.915	0.914	0.914	0.917
Dataset 2	0.863	0.851	0.845	0.848
Dataset 3	0.986	0.987	0.987	0.986

5.2. C-Support Vector Classification

In machine learning, there are mainly three types of leaning algorithms: supervised learning, unsupervised learning, and reinforcement learning. SVM is one of the most popular supervised learning algorithms for many applications, such as intrusion detection, spam filtering, and pattern recognition. There are various SVM formulations for classification, regression, and distribution estimation. As we mentioned above, in this study, the main goal is to classify each IP address as an attacker or normal one. Therefore, we selected c-support vector classification (C-SVC) for training and testing datasets.

Let $\boldsymbol{x}_i \in \mathrm{R}^n$, $i = 1, 2, \ldots l$, where l is the number of training examples, and an indicator vector $\boldsymbol{y} \in \mathrm{R}^l$ where $y_i \in \{-1, 1\}$ be given training vectors. In the experiments, the dimension parameter n ranges from three to five, because we have prepared three datasets with different numbers of features. We use -1 to represent *"Normal IP"* for IP addresses from the victim pool and +1 as *"Attacker IP"* for IP addresses from the attacker pool, and we use C-SVC to solve the following the optimization problem [21] [22].

$$\begin{aligned} \underset{\boldsymbol{w},b,\boldsymbol{\xi}}{\text{minimize}} \quad & \frac{1}{2}\boldsymbol{w}^{\mathrm{T}}\boldsymbol{w} + C\sum_{i=1}^{l}\xi_i \\ \text{subject to} \quad & y_i(\boldsymbol{w}^{\mathrm{T}}\phi(\boldsymbol{x}_i) + b) \geq 1 - \xi_i, \\ & \xi_i \geq 0,\ i = 1, 2 \ldots, l. \end{aligned} \tag{3}$$

where $\phi(\boldsymbol{x}_i)$ maps $\boldsymbol{x}_i$ into a higher dimensional space, and C is the regularization parameter, which must be greater than zero. Since the vector variable $\boldsymbol{\omega}$ may be highly dimensional, we solve the following quadratic programming problem [16].

$$\begin{aligned} \underset{\boldsymbol{\alpha}}{\text{minimize}} \quad & \frac{1}{2}\boldsymbol{\alpha}^{\mathrm{T}}Q\boldsymbol{\alpha} - \boldsymbol{e}^{\mathrm{T}}\boldsymbol{\alpha} \\ \text{subject to} \quad & \boldsymbol{y}^{\mathrm{T}}\boldsymbol{\alpha} = 0,\ 0 \leq \alpha_i \leq C,\ i = 1, \ldots, l. \end{aligned} \tag{4}$$

where $\boldsymbol{e} = [1, \ldots 1]^T$ is the vector whose components are all ones, Q is an l by l positive semidefinite matrix, $\mathrm{Q}_{ij} \equiv y_i y_j \mathrm{K}(\boldsymbol{x}_i, \boldsymbol{x}_j)$, and $\mathrm{K}(\boldsymbol{x}_i, \boldsymbol{x}_j) \equiv \varphi(\boldsymbol{x}_i)^T\varphi(\boldsymbol{x}_j)$ is the kernel function. After (4) is solved, using the primal dual relationship, the optimal □ satisfies (5) and the decision function is (6).

$$\boldsymbol{w} = \sum_{i=1}^{l} y_i\alpha_i\phi(\boldsymbol{x}_i) \tag{5}$$

$$sgn(\boldsymbol{w}^{\mathrm{T}}\phi(\boldsymbol{x}) + b) = sgn\left(\sum_{i=1}^{l} y_i\alpha_i K(\boldsymbol{x}_i, \boldsymbol{x}_j) + b\right) \tag{6}$$

Table 4. Confusion Matrix of the SVM Classification with Dataset 1

		SVM Classification	
		Attacker IP	Normal IP
Classification according to the data	Attacker IP	0.8285	0.0065
	Normal IP	0.1715	0.9935

We store $y_i\alpha_i\ \forall i$, b, labels, support vectors, and other information, such as kernel parameters, in the model for prediction. In this study, we utilized the following RBF (Gaussian) kernel as the kernel function.

$$K(\boldsymbol{x}_i, \boldsymbol{x}_j) = \exp(-\gamma\|\boldsymbol{x}_i - \boldsymbol{x}_j\|^2) \tag{7}$$

5.3. DDoS Attack Detection System

We trained and tested three types of dataset using C-SVC with the RBF (Gaussian) kernel. We applied five cross validations to our datasets to produce training and test datasets, and finally we found the best values of parameters C and γ which were 32,768 and 8, respectively. Tables 4, 5, and 6 show the confusion matrix of the SVM classification with different datasets for best parameters. Experimental results show that detection accuracy is approximately 91.1%, 85.1% and 98.7% for the Dataset 1, 2, and 3, respectively.

In the experiment with Dataset 1, the detection system could successfully detect the normal packets, but detecting the attack packets was not accurate; moreover, in the experiment with Dataset 2, the efficiency of the performance decreased compared with Dataset 1. The main difference between Dataset 1 and Dataset 2 is to utilize the number of packets per second instead of the total number of packets. We prepared Dataset 2 for considering the real-time detection system for DDoS attack because we cannot get the total number of packets when we execute the system in a real-time. Thus, we utilized the number of packets per second and the amount of bytes per second by using (1) and (2). If we changed 1.0 to *n,* we can generate the number of packets per *n* seconds. By considering the results, using the number of packets per *n* seconds is an effective

Table 5. Confusion matrix of the SVM classification with Dataset 2

		SVM Classification	
		Attacker IP	Normal IP
Classification according to the data	Attacker IP	0.716	0.014
	Normal IP	0.284	0.986

Table 6. Confusion matrix of the SVM classification with Dataset 3

		SVM Classification	
		Attacker IP	Normal IP
Classification according to the data	Attacker IP	0.995	0.0205
	Normal IP	0.005	0.9795

feature to develop the DDoS attack detection system in real-time but it is not an ideal solution for the highly accurate detection of the DDoS attack. However, when we further added two features in Dataset 1, we obtained a higher accuracy for detecting both types of IP addresses. Therefore, to obtain a high accuracy for detecting a DDoS attack, we must extract at least three features and utilize both the statistical analysis results and real-time analysis results. If we extract five or more features and utilize such results, we get the higher accuracy.

In addition, we calculated precision, recall, negative predictive value (NPV) utilizing the following equations.

$$Precision = \frac{True\ Positive}{True\ Positive + False\ Positive} \quad (8)$$

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad (9)$$

$$NPV = \frac{True\ Negative}{True\ Negative + False\ Negative} \quad (10)$$

The precision for each dataset is 0.99, 0.98, and 0.98. These numbers mean that the detection system could successfully predict the attack. These results show that the detection accuracy is high when the system should be alerted. However, the recall is 0.83, 0.72, and 0.99. These results show that the system predicted some normal data as the attack data. The NPV is 0.85, 0.78, and 0.99 and means that the system predicted some attack data as the normal data. These results mean that it is very difficult to detect some data whether from the attacker or normal users. Consequently, the detection system could detect the attack, but it is still difficult to recognize some data whether from attacker or normal with high accuracy.

6. Conclusion

In this paper, we proposed one approach using machine learning to develop an DDoS attack detection system. We analyzed a large number of network communication packets, and implemented a DDoS attack detection system using the patterns of DDoS attacks for each IP address. We presented and discussed the difficulties involved in developing a DDoS attack detection system using packets and features of DDoS attacks that are important to detect an attack. These features are very helpful in developing a detection system for DDoS attacks. Analyzing the packets, we calculated bytes per second with the time sequence and found that there are mainly two periods in DDoS attack. We recognized those the incubation period to trick the victims into being normal communication and attacking period to execute commands and attack the services.

In developing the DDoS attack detection system, we utilized machine learning techniques and algorithms. We selected the SVM with RBF (Gaussian) kernel to train and test the DDoS attack detection system. We prepared three types of datasets that we utilized with three and five features. Our detection system was more than 85% accurate with all types of dataset and 98.7% accurate with five features. The strategy for developing a DDoS attack detection system show that the detection system with SVM trained using the proposed features can successfully detect DDoS attacks with high accuracy.

8. Acknowledgements

Support for CAIDA's Internet Traces is provided by the National Science Foundation, the US Department of Homeland Security, and CAIDA members.

7. References

[1] "The CAIDA UCSD DDoS attack 2007 dataset," http://www.caida. org/data/passive/ddos-20070804 dataset.xml [accessed: July 18, 2014].

[2] R. Karimazad and A. Faraahi, "An anomaly-based method for DDoS attacks detection using RBF neural networks," International Confer- ence on Network and Electronics Engineering, 2011.

[3] P. Agrawal, B. Gupta, and S. Jain, "SVM based scheme for predicting number of zombies in DDoS attack," European Intelligence and Security Informatics Conference, 2011.

[4] R. Jalili, F. Imani-Mehr, M. Amini, and H. R. Shahriari, "Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks," Proceedings of the First inter- national conference on Information Security Practice and Experience (ISPEC'05), 2005.

[5] L. Limwiwatkul and A. Rungsawang, "Distributed denial of service detection using TCP/IP header and traffic measurement analysis," International Symposium on Communications and Information Technologies, 2004.

[6] G. Zhang, S. Jiang, G. Wei, and Q. Guan, "A prediction-based detection algorithm against distributed

denial-of-service attacks," International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, 2009.

[7] H.Rahmani, N.Sahli, and F.Kammoun,"Joint entropy analysis model for DDoS attack detection," International Conference on Information Assurance and Security, 2009.

[8] A. Navaz, V.Sangeetha, and C.Prabhadevi, "Entropy based anomaly detection system to prevent DDoS attacks in cloud," International Journal of Computer Applications, 2013.

[9] R. Zhong and G. Yue, "DDoS detection system based on data mining," Proceedings of the Second International Symposium on Networking and Network Security, 2010

[10] H. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, "Detecting distributed denial of service attacks: methods, tools and future directions," Oxford Journal, 2013

[11] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source," International Conference on Network Protocols (ICNP'02), 2002.

[12] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communications Review, 2004.

[13] V. Kekar, N. Duffield, O. Spatscheck, J. van der Merwe, and H. Zhang, "LADS: Large-scale automated DDoS detection system," USENIX Technical Conference, 2006.

[14] "The 12th annual computer crime and security survey," http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf [accessed: November 27, 2014].

[15] B. E. Boser, I. Guyon, and V. Vapnik, "A training algorithm for optimal margin classifiers," In Proceedings of the Fifth Annual Workshop on Computational Learning Theory, pp. 144-152, ACM Press, 1992.

[16] C. Cortes and V. Vapnik, "Support-vector network," Machine Learning," 20:273-297, 1995.

[17] Dobbin. K. K and Simon, R. M, "Optimally splitting cases for training and testing high dimensional classifiers," BMC Medical Genomics, 4(1), 31, 2011.

[18] M. F. Akay, "Support vector machines combined with feature selection for breast cancer diagnosis," Expert Systems with Applications, vol. 36, no.2, 2009.

[19] B. Sarwar, G. Karypis, J. Konstan, and J. Riedl, "Item-based collaborative filtering recommendation algorithms," Proceedings of 10th International Conference on the World Wide Web, pp. 285-295, 2011.

[20] K. Kato, V. Klyuev, "Large-scale Network Packet Analysis for Intelligent DDoS Attack Detection Development," The 9th International Conference for Internet Technology and Secured Transactions, pp. 361 – 366, 2014.

