# Detection of Denial-of-Service Attacks with SNMP/RMON

O. Boyar*, M. E. Özen** and B. Metin*
* Management Information Systems Department, Istanbul, Turkey
** Electrical and Electronics Eng. Department, Istanbul, Turkey
boyaronur@gmail.com, menesozen13@gmail.com, bilgin.metin@boun.edu.tr

***Abstract*—In this study, a Denial of Service (DoS) attack scenario is examined using Ethernet switch that supports Remote Monitoring (RMON) and Simple Network Management Protocol (SNMP). Detecting DoS attacks may require special software or appliance based firewall devices, but they are not economical. Therefore, manageable network devices supporting SNMP protocol can be employed for DOS attack detection. They give traffic information such as the byte and packet count level network usage, packet size, and packet transmission error events. These can be polled through RMON, which is a special Management Information Base (MIB). In this study, using RMON data polled from the switch, machine learning algorithms are used to detect DoS attacks that achieve a high detection rate and low false alarm rate based on our traffic in our laboratory environment.**

## I. INTRODUCTION

While digitalization provides a great deal of advantages to institutions, it also brings new unique problems along with itself. Now almost all devices are connected to the Internet; the number of the devices used in the companies is increasing. The intent of the objects is based on the interaction of these devices and on making life easier. With Industry 4.0, this affects the operation of factories and production chains. Be-side these advantages, many of these devices that make our life easier lead to a digital complexity. This situation makes the systems vulnerable to cyber-attacks. There are now more and more devices in the companies. On the other hand, we can say that there are many more points from where the Distributed Denial of Service attacks (DDoS) can begin. With DDoS, companies' operations may come to a halt. This year, a DDoS attack in the U.S. used security IP camera systems in houses [1].It is very difficult to stop DDoS attacks because they generate heavy traffic from many sources. It is necessary to use DDoS mitigator systems [2] in internet service providers to prevent these attacks. However, these are uneconomical solutions and can be ineffective if the attack is very powerful. It is therefore crucial to be able to recognize these attacks at the points where they are initiated. Some compromised computers in large local area network (LAN) structures can be used for these attacks. It is, thus, crucial to examine the network traffic to detect these computers used in DDoS attacks and take the necessary precautions [3]. One of the easiest ways to do this is to look at the information on SNMP / RMON protocols that are commonly used on network devices.

In the literature different methods are used to detect DDoS attacks. The references [4] and [5] states the capabilities of an entropy-based network anomaly detection method. K-Nearest Neighbors (KNN) classifier is used as a DoS attack detection method [6]. The importance of efficient detection with a small number of false alarms is emphasized. 2000 DARPA Intrusion Detection Scenario Specific Data Set is used in [6]. Procedures of DDoS attack are investigated and feature selection is performed. Cluster based approach is used in [7]. Reference [8] uses Artificial Neural Networks and Ref. [9] employs C5.0 algorithm to classify DDoS attacks in real time environments.

In our study, machine learning algorithms are simulated using RMON data polled from the switch. As stated in Ref. [3], RMON1 data are used in our analysis. Six features explained below are used. Different from Ref. [3], bandwidth values are not used in our experiment. Artificial Neural Networks, KNN and C5.0 algorithms are used. Moreover, our approach is different than cluster-oriented approach in [7].

The remainder of this paper is organized as follows. Section II presents the methodology followed and the network setup is defined. Section III describes the data analysis process and the data used in our study. Section IV explains our experiment. The comparison of the classifiers used is showed in Section IV as well. Section V shows the results of this paper.

## II. METHODOLOGY

For our experiment, we have created an environment that has three hosts and one Ethernet switch in the laboratory. Windows 10 operating system is installed in victim host. An SNMP management software are installed in another Windows 10 host for data collection. As a attacker computer, a host with Kali Linux operating system is employed. This host is used to send huge amount of traffic to simulate DoS attack. The setup of our network environment is shown in Fig. 1.

978-1-5386-1122-7/18/$31.00 ©2018 IEEE

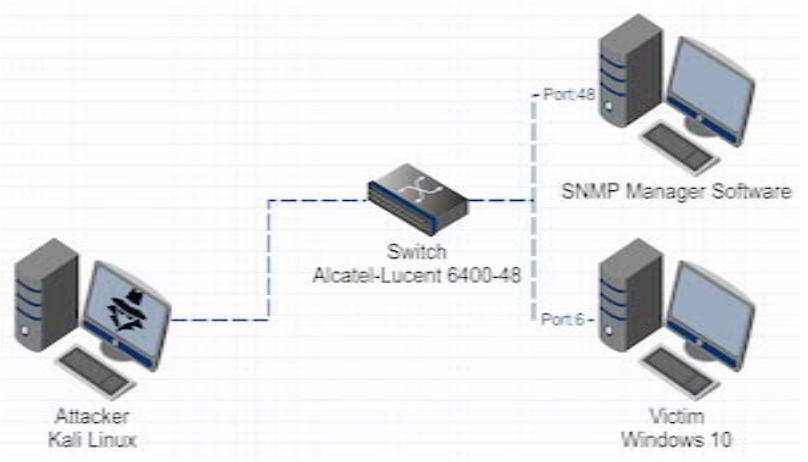


Figure 1. Network setup

In the data collection step, network flow data of the victim host that is connected to the Ethernet switch is collected for 24 hours in a workday via SNMP/RMON1 management tool. SNMP/RMON1 management tool is installed in the other host that is also connected to the switch. During certain periods, different number of packets are sent to the victim host to make the network traffic even higher. The data is visualized after collection. Figure 2 shows the values of megabits per second in hourly basis. As it can be seen from the figure, the busiest period during a day is from 14.00 to 16.00 o'clock. After collection of normal network flow data, DDoS attack is simulated using another host in the same network that has Kali Linux as its operating system. Sample code to generate DDoS attack in Kali Linux operating system is *hping3 -d 64 -S -p21 –flood –rand-source*. This script code generates packets of 64 kilobytes from random source IP adreses. Using such a code, SYN attacks from a random source is created. Attacks are generated using 64 and 1270 kilobytes of packets. A DoS attack is simulated for 2 hours. The data generated during the attack is also collected minutely using SNMP / RMON1 management tool.

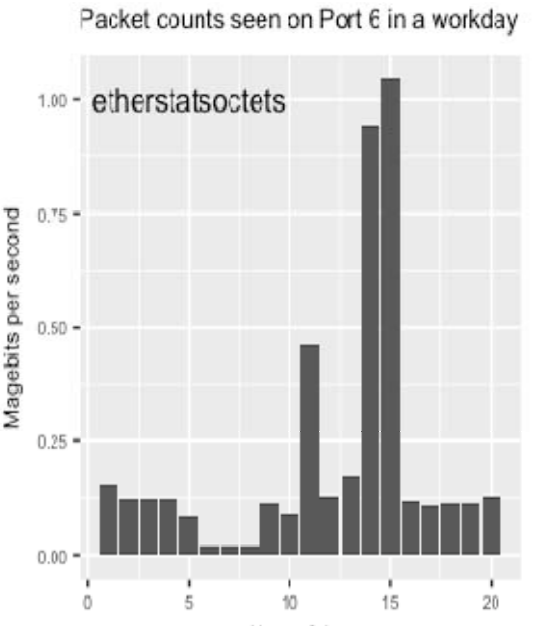


Figure . Packet counts per hour

## III. Data Analysis

In the data analysis step, the data collected from LoriotPro SNMP / RMON1 management tool's Management Information Base (MIB) table is used. MIB table has information about packet counts in the network traffic. Packet counts according to their packet sizes are given in the MIB table. In our study the data from MIB table are used. Six features among nine can be given as follows:

- etherstatspkts64octets
- etherstatspkts65to127octets
- etherstatspkts128to255octets
- etherstatspkts256to511octets
- etherstatspkts512to1023octets
- etherstatspkts1024to1518octets

After collecting the data including those features, the sum of each packet count features is calculated. The purpose of this operation is to calculate the packet count ratios for each feature. Instead of packet counts itself, packet ratios are used to train the classifiers. [3]. New features are,

- etherstatspkts64octetsRatio
- etherstatspkts65to127octetsRatio
- etherstatspkts128to255octetsRatio
- etherstatspkts256to511octetsRatio
- etherstatspkts512to1023octetsRatio
- etherstatspkts1024to1518octetsRatio

We have sent 64 and 1270 sized packets during our DoS attack simulation. The count of the packets in the

network is increased dramatically during our simulation. The data of the DDoS attack simulation are also collected using SNMP/RMON1 management tool.

In our study, two different cases are taken into consideration. In the first case, the network traffic data with low traffic are used. After collection of this data, three different classifiers which are namely Artificial Neural Networks, K-Nearest Neighbors and C5.0 algorithms are used. In the second case the network flow data with a higher traffic is used. The further details and the results of the two different experiments are as follows.

After collection of the normal flow data and DoS attack data, train and test sets are created. 80% of the data are partitioned as train set and 20% of the data are selected as test set.

For our analysis, we used three different algorithms which are namely Artificial Neural Networks, K-Nearest Neighbors and C5.0 algorithms. Artificial Neural Networks are created with two hidden layers with 4 and 2 nodes. Number of neighbors selection for K-Nearest Neighbors is 5. Both Artificial Neural Networks [8] and K-Nearest Neighbors [6] are widely used algorithms for detection of DoS. The reason behind using C5.0 algorithm is that it uses information gain as splitting criteria. Information gain is the expected reduction in entropy caused by the partitioning of the observations according to the attributes given. Entropy is a widely used method in anomaly detection [5].

## IV. Experiment

In the first experiment, network traffic data with low traffic is used. No extra flow is created during this period and the data are collected. Next, a DoS attack is simulated for an hour and its data are collected. Normal network traffic data and DoS data are collected.

In the first experiment, due to the huge difference between DoS attack data and normal traffic data, the classification of attack was simple. KNN, C5.0 and Neural Networks algorithms anticipated at a 100% prediction rate. In the second experiment, we created a busier network environment with HTTP and FTP traffic. We generated packets and a communication between hosts. As in the first experiment, again a DoS attack is simulated for an hour. The objective of this experiment is to test our algorithms in a busier network environment in which normal flows have some similar patterns with DoS attacks. In the second experiment, none of our algorithms could achieve a 100% prediction rate. By accepting DoS attack as a "positive" observation, true positive rate of Neural Networks algorithm is 100% while true negative rate is 99.3%. True positive rate of C5.0 algorithm is 98.4% while true negative rate is 98.89%. True positive rate of KNN algorithm is 100% while true negative rate is 98.49%. The comparison of accuracy, sensitivity and specificity ratios of each algorithm are shown in Table 1.

The main objective is to detect DoS attacks. We accepted DoS attack as a positive observation in our case. False positive rate is a good measure for evaluating each algorithms performance of detecting DoS attacks. False positive rate of Neural Networks algorithm is approximately 0.69%, which is equal to 5 false positive observations in our data set. False positive rate of C5.0 algorithm is 1.11%, which is equal to 8 false positive observations in our data set. False positive rate of KNN algorithm is 1.15%, which is equal to 11 false positive observations in our data set. Figure 3 shows false positive rates for the mentioned algorithms. The architecture of our artificial neural network algorithm is shown in Fig. 4. It uses *tanh* function as activation function. The convergence is completed in 3281 steps.

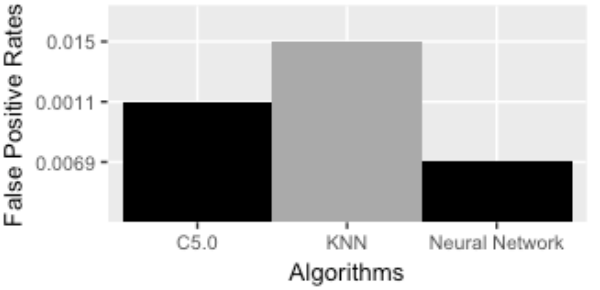


Figure 3. False positive rates of algorithms.

## V. Results

In this work, an experiment environment to collect network traffic data with and without a DoS attack is created and RMON1 data from MIB table are used. RMON1 data are extracted minutely throughout 24 hours from a network in a production environment. Three different algorithms are used to predict the DoS attack. Although Artificial Neural Networks performed most efficiently, K-Nearest Neighbors and C5.0 algorithms performed efficiently as well.

TABLE I. COMPARISON OF ACCURACY, SENSITIVITY, SPECIFICITY RATIOS OF ALGORITHMS

| **Algorithm** | **Measurements** | | |
|---|---|---|---|
| | ***Accuracy*** | ***Sensitivity*** | ***Specificity*** |
| ANN | 0.9945593 | 1 | 0.9747475 |
| KNN | 0.9889395 | 1 | 0.944 |
| C5.0 | 0.988035 | 0.9958391 | 0.9595960 |

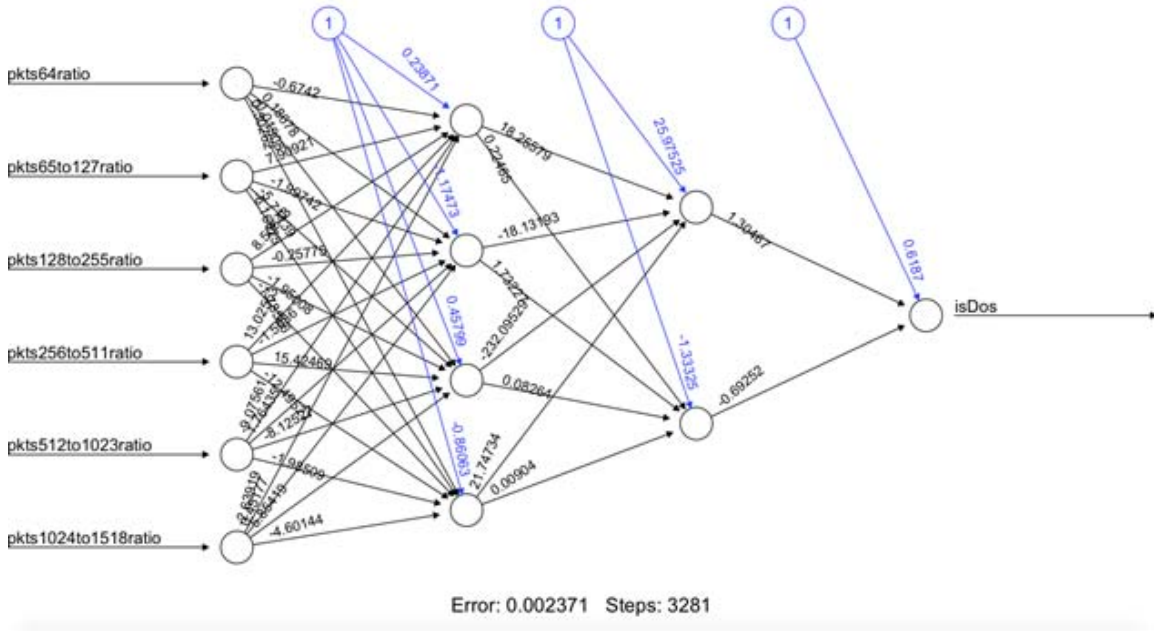


Figure 4. The architecture of artificial neural networks.

## REFERENCES


[1] NY Times "Hackers Used New Weapons to Disrupt Major Websites Across U.S", https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html, Retrieved 24 December 2017

[2] F. Tan (2 May 2011). "DDoS attacks: Prevention and Mitigation". https://thenextweb.com/media/2011/05/02/ddos-attacks-prevention-and-mitigation/#!tIvKh, The Next Web. Retrieved 24 December 2017.

[3] W.W. Streilein, D. J. Fried, R. K. Cunningham, "Detecting Flood-based Denial-of-Service Attacks with SNMP/RMON," MIT Lincoln Laboratory.

[4] A. Saied, R. E. Overill, T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks", *Neurocomputing*, 2015, 385 – 393.

[5] P. Bereziński, B. Jasiul and M. Szpyrka, "An Entropy-Based Network Anomaly Detection Method", *Entropy* 2015, ISSN 1099-4300, 2367 - 2408

[6] H.V. N Guyen and Y. Choi, "Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework", *International Journal of Computer and Information Engineering*, Vol:4, No:3, 2010, 537 - 542.

[7] K. Lee, J.Kim, K. H.Kwon, Y.Han, S. Kim, "DDoS attack detection method using cluster analysis, Elsevier, *Expert Systems with Applications* 34, 2008, 1659 - 1665

[8] J. Li, Y.Liu, L.Gu, "DDoS Attack Detection Based On Neural Network", 2nd International Symposium on Aware Computing (ISAC 2010), Tainan, China, 2010, 196 – 199.

[9] D. M. Farid, M. Z. Rahman, "Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm", *Journal of Computers,* Vol. 5, No. 1, 2010, 23-31.