PAPER DETAILS

TITLE: Detecting Different Types of Distributed Denial of Service Attacks

AUTHORS: Esra SÖGÜT,Saadin OYUCU,O Ayhan ERDEM

PAGES: 12-25

ORIGINAL PDF URL: https://dergipark.org.tr/tr/download/article-file/1446269

GU J Sci, Part C, 9(1): 012-025 (2021)

Gazi Üniversitesi

Fen Bilimleri Dergisi

PART C: TASARIM VE TEKNOLOJİ

http://dergipark.gov.tr/gujsc

Detecting Different Types of Distributed Denial of Service Attacks

Esra SÖĞÜT[1,*], Saadin OYUCU[2], O. Ayhan ERDEM[1]

[1]*Gazi Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, 06500, Yenimahalle, ANKARA*

[2]*Adıyaman Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 02040, Merkez, ADIYAMAN*

Article Info

Research article
Received: 13/12/2020
Revision: 20/01/2021
Accepted: 22/01/2021

Makale Bilgisi

Araştırma makalesi
Başvuru: 13/12/2020
Düzeltme: 20/01/2021
Kabul: 22/01/2021

Keywords

DDoS
SYN Flooding
Spoofing IP
Cyber Security
Data Mining

Anahtar Kelimeler

DDos
SYN Saldırısı
IP Sahteciliği Saldırısı
Siber Güvenlik
Veri Madenciliği

Abstract

Distributed Denial of Service Attacks (DDoS) threaten every device connected to the Internet. The fast progress and wide spreading DDoS attacks are among the most well-known features of them. Many studies have been conducted to reduce the impact of these fast-progressing and widespread attacks. However, due to the continuous development of attack types and the implementation of different techniques, the prevention of attacks has not been fully achieved. Therefore, within the scope of this study, a DDoS attack was examined first and applications used to detect it were investigated. A system has been proposed to detect DDoS attacks using data mining methods. For the proposed system, experiment mechanisms for Transmission Control Protocol (TCP) Flooding, Spoofing Internet Protocol (IP), SYN Flood with Spoofed IP, and User Datagram Protocol (UDP) Flooding, which are among the DDoS attack types, were established and the attacks were performed to obtain network flow data. The classification was made with appropriate data mining methods according to the specified features and ZeroR, OneR, Naive Bayes, Bayes Net, Decision Stump, and J48 algorithms were used. According to these algorithms, the best classification rate has been reached with J48 algorithm. The results have shown that the proposed system plays an important role in determining the DDoS attack type. The proposed system will ensure that appropriate detection mechanisms are applied more quickly, effectively and efficiently in real attacks.

Farklı Türde Dağıtık Hizmet Dışı Bırakma Saldırılarının Tespiti

Öz

Dağıtık Hizmet Dışı Bırakma Saldırıları (DDoS: Distributed Denial of Service Attacks) internete bağlı her bir cihazı tehdit etmektedir. DDoS saldırılarının hızlı ilerlemesi ve geniş alana yayılması en bilinen özelliklerindendir. Hızlı ilerleyen ve geniş alana yayılan bu saldırıların etkisini azaltmak için birçok çalışma yapılmıştır. Ancak saldırı türlerinin sürekli gelişmesi ve farklı tekniklerin uygulanması nedeni ile saldırıların engellenmesi tam olarak gerçekleştirilememiştir. Bu nedenle çalışma kapsamında öncelikle DDoS saldırısı incelenmiş ve tespit etmeye yönelik uygulamalar araştırılmıştır. Veri madenciliği yöntemleri kullanılarak DDoS saldırılarını tespit etmek için bir sistem önerilmiştir. Önerilen sistem için DDoS saldırı türlerinden Aktarım Denetimi Protokolü Saldırısı (TCP: Transmission Control Protocol Flooding), IP Sahteciliği Saldırısı (Spoofing IP: Internet Protocol), Maskelenen IP ile SYN Saldırısı (SYN Flood with Spoofed IP) ve Kullanıcı Veribloğu İletişim Kuralları Saldırısı (UDP: User Datagram Protocol Flooding) için deney düzenekleri kurulmuş ve saldırılar gerçekleştirilerek ağ akış verileri elde edilmiştir. Belirlenen özniteliklere göre uygun veri madenciliği yöntemleri ile sınıflandırma yapılmış ve ZeroR, OneR, Naive Bayes, Bayes Net, Decision Stump ve J48 algoritmaları kullanılmıştır. Bu algoritmalara göre en iyi sınıflandırma oranına J48 algoritması ile ulaşılmıştır. Elde edilen sonuçlar, önerilen sistemin DDoS saldırı türü belirlenmesinde önemli rol oynadığını göstermiştir. Önerilen sistem, gerçek saldırılarda uygun tespit mekanizmalarının daha hızlı, etkin ve verimli şekilde uygulanmasını sağlayacaktır.

* Corresponding author, e-mail: esrasogut@gazi.edu.tr
DOI: 10.29109/gujsc.840126

1. INTRODUCTION

Every day there are new and rapid developments in the field of cyber security. This innovation in the cyber world makes it increasingly difficult to maintain security in the same world. Attack types in the cyber world are also affected by these developments and become more diversified. It is becoming increasingly difficult to detect evolving and diverse types of attacks with the traditional methods. Instead of single types of attacks, advanced types of attacks with very different characteristics are realized. Defense methods applied to different types of attacks should also be different and applicable. Therefore, detection and prevention systems with different or new features from traditional methods should be developed against cyber attacks.

DDoS (Distributed Denial of Service Attacks) come first in cyber attacks [1]. The main purpose of DDoS attacks is to disable accessibility, which is one of the information security features. DDoS attacks aim to make the resources of a target or target systems unavailable. These resources (processor, memory, disk space, etc.) are usually resources that will prevent the system from serving. Damaging these resources or preventing them from working will cause major disruptions in the continuity of the service provided. Each DDoS attack can occur in different types [2,3]. Generally, while the packets sent to the target system are being processed, system resources and bandwidth are consumed excessively and a DDoS attack occurs. As a result of these attacks, the target system becomes unresponsive to incoming requests and packets and becomes out of service [4,5].

DDoS attack types have different features and characteristics from each other. Attacks such as Transmission Control Protocol (TCP) Flooding, Spoofing IP (Internet Protocol), SYN Flood with Spoofed IP, User Datagram Protocol (UDP) Flooding, Internet Control Message Protocol (ICMP) Flooding, Hyper-Text Transfer Protocol (HTTP), Get/Post, and Ping of Death are types of DDoS attacks [6-11]. In this study, four different types of DDoS attacks encountered most in the literature were examined and discussed experimentally. These attack types are TCP Flooding, Spoofing IP, SYN Flood with Spoofed IP, and UDP Flooding.

The main purpose of the TCP Flooding is to fill the memory by sending a large number of packets to the content from the open ports of the target system and to put the system out of service [12]. Spoofing IP Attack is the unauthorized use of an IP address during an attack. The main purpose of this attack is to hide the identities of attacker systems and to make it difficult to be discovered [13]. In SYN Flood with Spoofed IP, SYN packets are sent to the target system by being masked by an IP address and the system memory is filled. The system sending the packets is in unidentified status and the target system becomes inoperable due to over-sent packets [12]. The main purpose of UDP Flooding is to randomly select the ports of the target system and send a large amount of UDP packets to the system [14]. Each of these mentioned attack types has different characteristics from the other. Therefore, within the scope of the study, sample experiments and different analyzes were made for the mentioned attack types.

When the related studies are examined, it is seen that the detection and prevention studies of traditional attacks are insufficient in detecting DDoS attacks [15]. The unknown source of the attack, large number of the attack sources, attacks having more than one part, the network flow generated at the time of the attack is similar to the normal network flow, and the failure of certain rules used before can be shown as the reasons of this situation [16]. In their study on early detection of DDoS attacks, Yuan and Mills monitored the network-wide effects of the attacks. They used cross-correlation analysis to create traffic patterns. These patterns are used to indicate where and when a DDoS attack may occur [17]. Shiaeles et al. proposed a system using a fuzzy prediction method against real-time DDoS attacks. If the packet arrival time which they observe is lower than the average packet arrival time, then the event is seen as a DDoS attack. Besides, network-based DDoS attacks were investigated in their study [18]. In a different study, Karimazad and Faraahi proposed an anomaly-based detection method based on the characteristics of attack packets. By activating the Radial Basis Function neural network with vectors based on seven attributes, they classified the traffic as normal or a DDoS attack. The data set of the University of California at Los Angeles was used for this process. The proposed method can classify the system as normal or attack, but cannot define and classify the types of attacks [19]. In the study of Al-Duwairi, correlation analysis between the outgoing and incoming traffic of a network was made and the occurring

changes were used to detect DDoS attacks. DARPA dataset is used for this and Fuzzy classification methods have been preferred to ensure their accuracy [20].

When the studies in the literature are examined, it has been seen that many studies in which TCP/IP packet header is analyzed according to well-defined rules and conditions have been conducted [17,21], and packet features showing DDoS attack in network traffic [19,20,22] have been performed. However, these studies made a limited progress and the desired level of attack detection could not be achieved. One of the biggest reasons for this situation is that each attack has its characteristics. For this reason, DDoS attacks were primarily examined within the scope of the study. As a result of the investigations, information was provided to understand DDoS attacks and to increase awareness. Besides, a system using data mining methods to detect DDoS attacks has been proposed. For the proposed system, firstly, experimental mechanisms for TCP Flooding, Spoofing IP, SYN Flood with Spoofed IP, and UDP Flooding, which are among DDoS attack types, have been established. Network flow data were obtained through these experimental setups. The Source Port, Source IP, Destination IP, Destination Port, Protocol, Size, Number, Delay Time, and DDoS Type features are specified to be used in data mining. The classification was made with data mining methods suitable for these features and algorithms such as ZeroR, OneR, Naive Bayes, Bayes Net, Decision Stump and J48. The results obtained showed that the proposed system plays an important role in determining the type of attack when there is a DDoS attack.

The study consists of six parts. In the first part, basic information and a review of literature are given. Information about the systems used and the steps for to perform DDoS attacks are given in the second part. In the third part, studies on listening to attacks and obtaining data set are presented in detail. The development of the proposed system with data mining methods is given in the fourth part, and the results of the classification algorithm, which is suitable for the developed system and has the highest success rate, are given in the fifth part. In the last part, a general evaluation of the study has been done and information about the future planned studies is presented.

2. PERFORMING DDOS ATTACKS

DDoS attack mechanisms were prepared to be used in the experiments performed in this study. With the prepared DDoS attack mechanisms, the target system, which is previously determined, was reached and the attack operations were performed. The target system has been reached, system resources have been used excessively, and the performance level of the system has been minimized. Thus, the system has become inoperable. The steps determined for the attack carried out in this study are given in Figure 1.

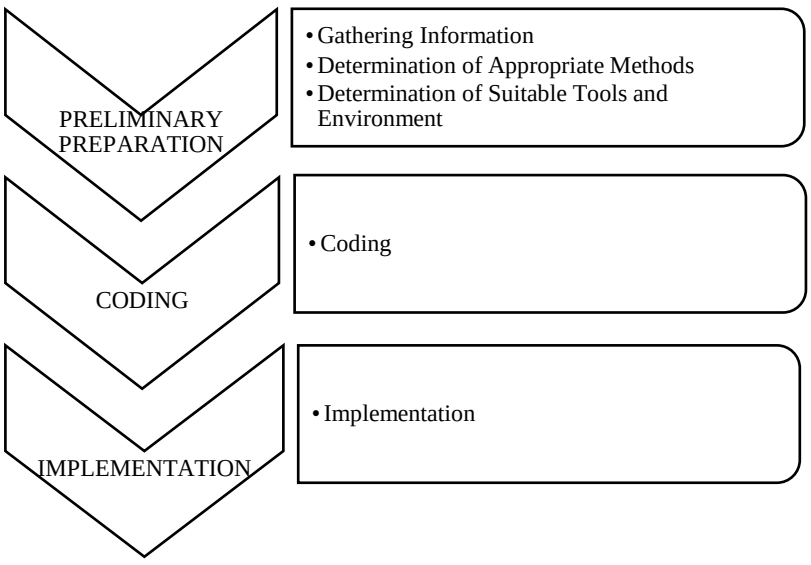

Figure 1. *Steps to perform DDoS attacks*

The steps taken for DDoS attacks are preliminary preparation, coding, and implementation, respectively (Figure 1). Preliminary preparation is an important step in the realization of DDoS attacks. The operations performed for preliminary preparation consist of three steps. The first of these steps is information gathering. At this step, target information (IP information, system information, function information, etc.) is obtained. In determining the appropriate methods, which is the second step of the preliminary phase, the types of attacks to be applied to the target system are determined. After gathering information about the target system and determining the appropriate attack type, the tools and environment suitable for the attack were determined. VirtualBox virtualization environment was chosen for the attack environment and the necessary experimental mechanisms for the attack were built on this environment. An environment with a Windows operating system as the target system and a Kali Linux operating system as an attacker was used. Screenshots of these systems are shown in Figure 2.

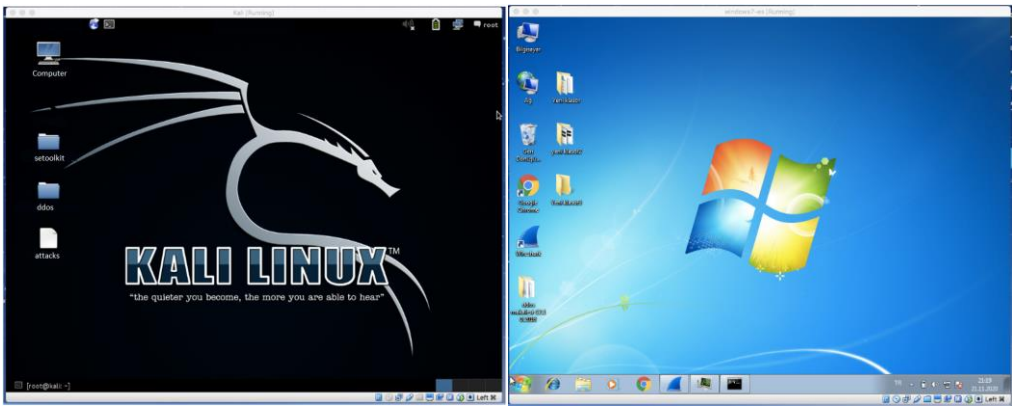

Figure 2. *Views of the attacker and target systems*

In the coding step, the necessary coding for the attack has been done. Experiments were prepared in two different ways for each of the four attacks using the hping3 tool in the attacker system. It is intended to damage the functioning of the target system. Attacking the target system was performed during the implementation phase. For this, four different DDoS attack types commonly seen in the literature were selected [6-11]. After the necessary steps were taken, the functioning of the target system was damaged. The visual about this is given in Figure 3.

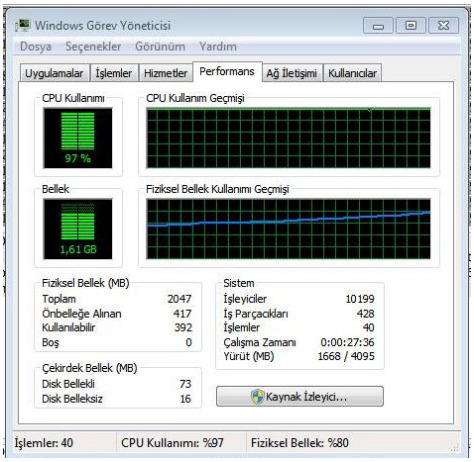

Figure 3. *The operating status of the target system at the time of the attack*

When the attacks were made, the resource usage and operating performance of the target system were significantly affected (Figure 3). The CPU utilization rate of the target system has reached 97% and the physical memory utilization rate has exceeded 80%. The operating condition of the system is affected and has been minimized.

3. DATA OBTAINING

After the performance analysis of the target system could be tracked live when the attack was made, the data collection step was started. Wireshark packet analysis tool was used to listen to the target system network for each attack and to collect the obtained network flow data. Wireshark is a useful tool that enables network traffic to be monitored, analyzed, and filtered on-demand, where necessary, via a graphical interface [23]. An example of monitoring attacks with Wireshark is given in Figure 4.

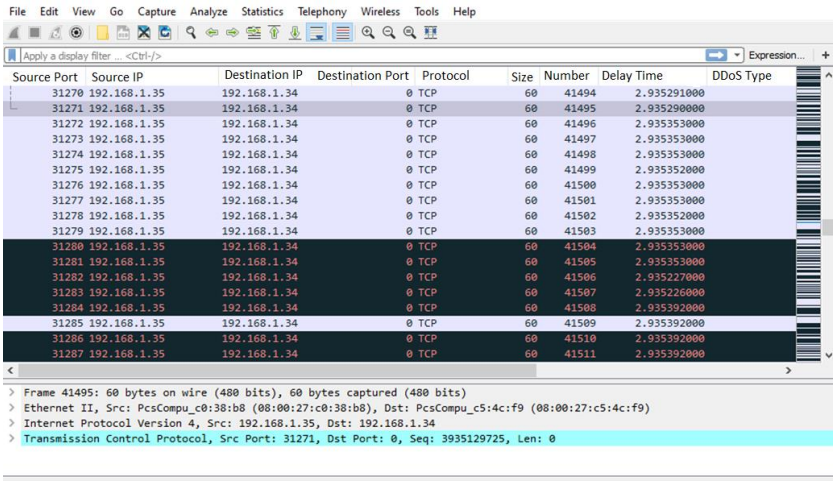

Figure 4. *Tracking attacks with Wireshark*

Detecting network traffic completely in a short time is of great importance for attack detection [24]. The data set KDDCUP99 was examined and 9 features found suitable for this study were determined [25-27]. Descriptions and explanations of these features belonging to the data set obtained by Wireshark are given in Table 1.

Table 1. *Network flow data features*

No	***Feature***	***Explanation***
1	*Source Port*	*It contains the port information used by the computer sending the packet.*
2	*Source IP*	*The IP address of the computer sending the packet.*
3	*Destination IP*	*The IP address of the computer receiving the package.*
4	*Destination Port*	*It contains the port information of the computer receiving the packet.*
5	*Protocol*	*It shows which protocol the packet belongs to.*
6	*Size*	*The size of the packet sent/received. The data size type used in this study was determined as Byte.*
7	*Number*	*The number of all packets sent/received.*
8	*Delay Time*	*It is the time difference between the previous pack and the next pack. This difference is handled in seconds (sec).*
9	*DDoS Type*	*It shows the type of DDoS attack implemented.*

For the detection of the attack using the attributes specified in Table 1, a network-based system according to its location, anomaly-based according to the identification method, and non-real-time according to the data processing time has been proposed.

4. SYSTEM DEVELOPMENT

Data mining is one of the methods used to transform large amounts of data collected very quickly, into meaningful information as a result of various analyzes [24]. In this study, data mining was used to detect attacks. When using data mining methods, the Weka tool is used for data processing and statistical evaluation of learning methods on data [27]. In the proposed system, the Weka tool was used to perform these operations and to apply data methods such as visual monitoring of the model extracted from the raw data.

When the literature is examined, it is seen that different classification algorithms are prominent in data mining for attack detection and some of them are frequently used [28-30]. ZeroR, OneR, Naive Bayes, Bayes Net, Decision Stump, and J48 algorithms were used in this study. ZeroR algorithm is an algorithm that estimates the mean value of numerical test data and applies the basic algorithm rules [24]. OneR algorithm is one of the algorithms that tests property and generates a list of rules.

Table 2. *Comparison of the performance of algorithms*

Algorithm	***Test Mode***	***Number of Correctly Classified Instances***	***Number of Incorrectly Classified Instances***	***Accuracy Percentage***	***Working Duration (sec.)***
ZeroR	*Cross-Validation (10)*	*71184*	*175219*	*28.8893*	*0.11*
ZeroR	*Percentage Split (%66)*	*24149*	*59628*	*28.8253*	*0.32*
OneR	*Cross-Validation (10)*	*72921*	*173482*	*29.5942*	*0.27*
OneR	*Percentage Split (%66)*	*24775*	*59002*	*29.5726*	*0.29*
Naive Bayes	*Cross-Validation (10)*	*218964*	*27439*	*88.8642*	*0.23*
Naive Bayes	*Percentage Split (%66)*	*74489*	*9288*	*88.9134*	*1.60*
Bayes Net	*Cross-Validation (10)*	*219059*	*27344*	*88.9027*	*0.67*
Bayes Net	*Percentage Split (%66)*	*74547*	*9230*	*88.9827*	*0.94*
Decision Stump	*Cross-Validation (10)*	*135467*	*110936*	*54.9778*	*0.31*
Decision Stump	*Percentage Split (%66)*	*45982*	*37795*	*54.8862*	*0.16*
J48	*Cross-Validation (10)*	*197006*	*49397*	*79.9528*	*1.74*
J48	*Percentage Split (%66)*	*75215*	*8562*	*89.78*	*1.50*

Naive Bayes and Bayes Net algorithms, on the other hand, make statistical classifications to predict whether the data belong to a certain class or not. These algorithms are very successful in making decisions in uncertain situations [31,32]. The Decision Stump algorithm creates a single-level decision

tree and performs the classification process directly based on a single input feature value [24]. The J48 algorithm is a decision tree algorithm based on ID3 and C4.5 algorithms, and the information gain rate is used as the feature selection criterion in this algorithm [33]. If-Then rules are used in the tree structure and membership function sets are given as output. To create a simple classification model on the data, insignificant branches in the tree are cut by pruning [34].

Data preprocessing, cleaning, reduction, and transformation operations were performed on the data set to use it in algorithm analysis and get more accurate results. Accordingly, a data set with 9 attributes and 246403 rows was obtained. Information about this data set is given in Table 3. Two methods were used while creating the model. First, the Cross-Validation ratio was chosen as 10. Secondly, 66% of the data was used for training the model and the rest of the data was used for testing. These two methods were performed using each classification algorithms. The obtained network flow data were analyzed and compared with the specified algorithms. Information about the number of samples that were classified correctly and incorrectly, the correct classification rates of the algorithms, and the classification time of the algorithms are given in Table 2.

According to the information given in Table 2, the best result was obtained with the J48 algorithm (89.78%), as a result of comparing the accuracy performances of the algorithms used. Accuracy refers to the ratio of data perceived as accurate to the entire test data set. The higher the accuracy value, the more successful the machine learning model is [35]. The lowest accuracy rate was obtained with the ZeroR algorithm (28.8253%). J48 algorithm is the longest-running algorithm to make the classification. ZeroR is the algorithm that makes the classification in the shortest time.

5. EXPERIMENTAL RESULTS

In the study, the visual results produced by Weka of the J48 algorithm with which the highest success rate was obtained are examined. The inferences from the reviews are given in this part. The values of each attack class and the methods used are given in Table 3 in detail.

Table 3. *Values belonging to the attacks used in visual results*

Attack	***Number Used in Visual Results***	***Colour Used in Visual Results***	***Packet Number***	***Packet Size (Largest)***	***Attack Time (sec.)***	***Maximum Delay Time of Next Packet (sec.)***
TCP Flooding-1	*1*	*Dark Blue*	*25198*	*110*	*6.667*	*0.482*
TCP Flooding-2			*23557*	*113*	*7.994*	*0.974*
Total Packets for TCP Flooding			*48755*			
Spoofing IP-1	*2*	*Red*	*37902*	*182*	*8.828*	*0.925*
Spoofing IP-2			*26449*	*113*	*7.123*	*0.712*
Total Packets for Spoofing IP			*64351*			
SYN Flood with Spoofed IP-1	*3*	*Green*	*34367*	*105*	*10.664*	*2.056*

SYN Flood with Spoofed IP-2			*27746*	*113*	*6.179*	*1.712*
Total Packets for SYN Flood with Spoofed IP			*62113*			
UDP Flooding-1	*4*	*Blue*	*36229*	*542*	*13.326*	*1.789*
UDP Flooding-2			*34955*	*298*	*20.323*	*3.169*
Total Packets for UDP Flooding			*71184*			
Total Packets for All Attacks			*246403*			

To be used in visual results, numbers from 1 to 4 were made for TCP Flooding, Spoofing IP, SYN Flood with Spoofed IP, and UDP Flooding, respectively. Besides, coloring was done by indicating the number of packets used in the analysis. The maximum number of packets, packet size, attack time, and delay time were reached with UDP Flooding.

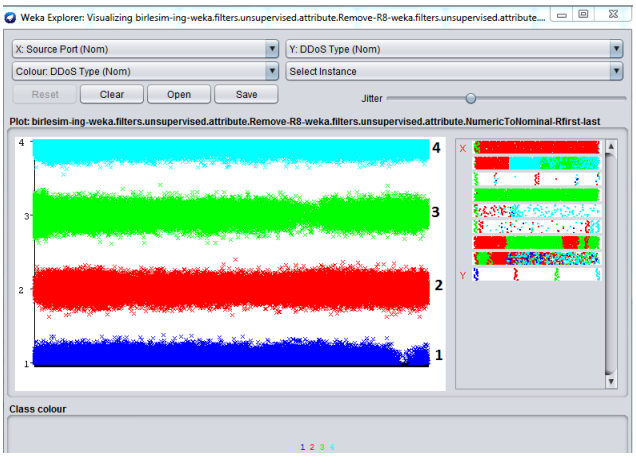

Figure 5. *Visual of the source port value*

When Figure 5 is examined, it is seen that the source port range of all attacks is very wide and varied. Almost all ports are used for every attack experiment.

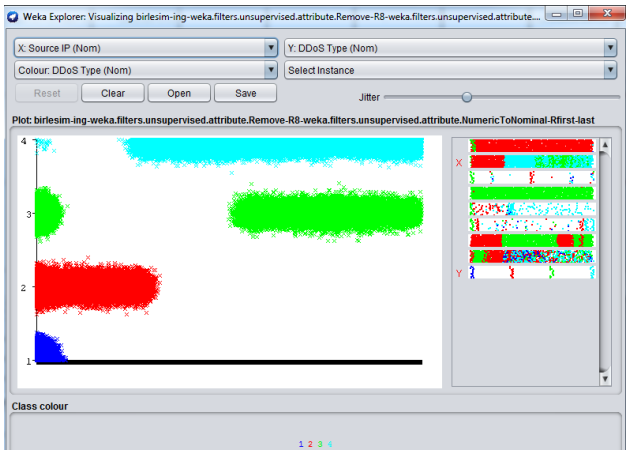

Figure 6. *Visual of the source IP value*

When we consider the source IPs, it was seen that very few IPs were used in the TCP Flooding. The IP range used in Spoofing IP is narrow. In SYN Flooding and UDP Flooding, the range of source IP used is wide and varied (this is more obvious especially for UDP Flooding).

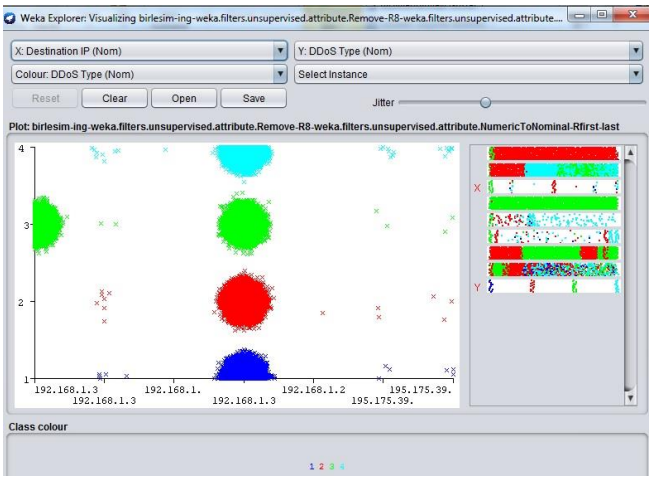

Figure 7. *Visual of the destination IP value*

The same IP was used as the target in all attack experiments, and the other IPs were rarely used, as can be seen in Figure 7. The target IP range is wider than the others in SYN Flooding.

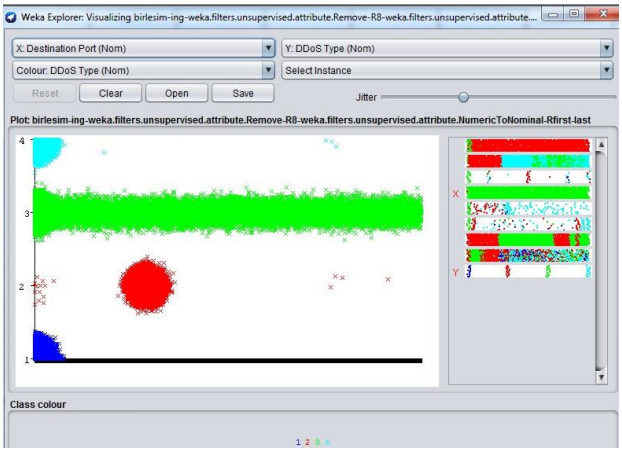

Figure 8. *Visual of the destination port value*

When we consider the target port, it has been observed that SYN Flooding has used almost all ports. The port range used in TCP and UDP floodings is very narrow and has not varied. In Spoofing IP, the destination port usage is in a wider range and more varied than TCP and UDP Floodings.

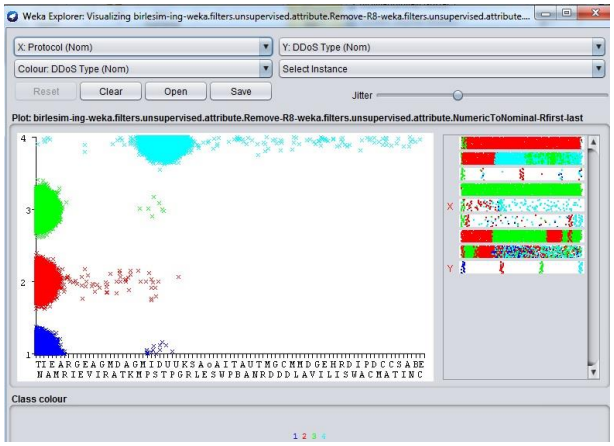

Figure 9. *Visual of the protocol value*

When we look at the protocols used in the attack experiments, it was seen that the protocols used in UDP Flooding were more and more varied. Protocols such as TCP, UDP, and DNS are frequently used in this attack. TCP Flooding, Spoofing IP, and SYN Flooding used similar protocols. These attacks focused on the TCP protocol and used very few different protocols.

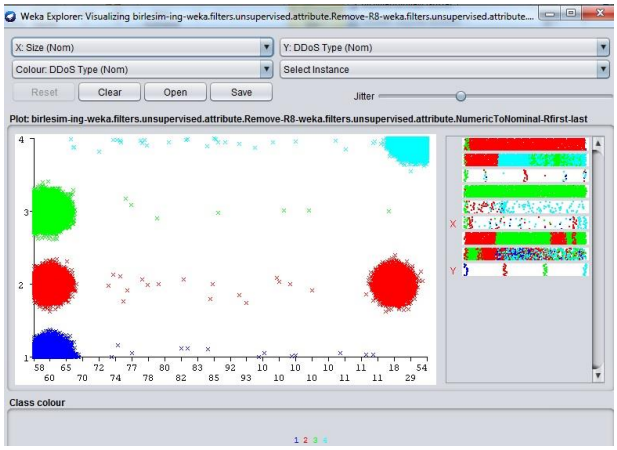

Figure 10. *Visual of the size value*

Based on Figure 10, it has been concluded that the size of the packet used at once in UDP Flooding is large. Also, a small number of sizes and different sizes were used. In the Spoofing IP, packets with different sizes were used. TCP and SYN Floodings used similar and smaller packet sizes.

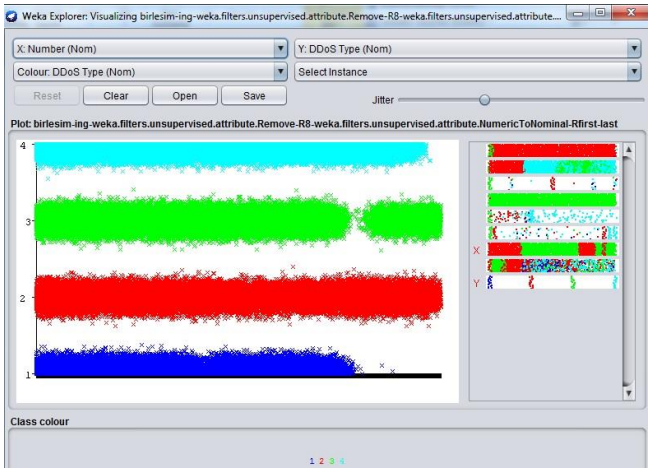

Figure 11. *Visual of the number value*

When the value of the number of packets obtained in the attack experiments was examined, it was seen that the TCP Flooding had the least number of packets. The other three attacks have several packets that are close to each other.

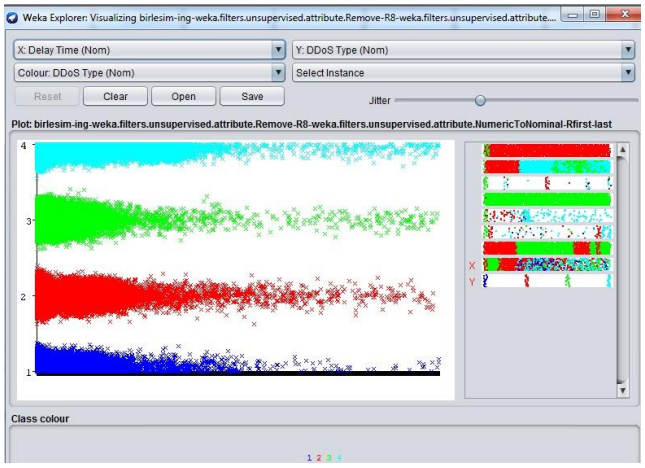

Figure 12. *Visual of the delay time value*

When the delay time of the packets was examined, the highest values were reached with the UDP Flooding. The SYN Flooding has come in second place. Similar situations were observed for the other two attacks.

6. CONCLUSION

In this study, sample experiments have been performed by considering the important features of DDoS attacks. With these experiments, the attacker reached the target system and performed the desired operations. During these processes, the target system became inoperable and system performance was reduced to a minimum.

The data set was obtained by listening and evaluating the systems where different DDoS attack experiments were performed, and data analysis was performed by applying the selected methods. Different methods have been tried to detect DDoS attack types and the method with the highest result has been examined in detail. Studies have been performed on classification algorithms using the data mining method. According to the studies performed, the highest classification success rate was obtained with the J48 algorithm. The visual results obtained with this algorithm were discussed and detailed information

about the characteristics of each attack type was given. Unlike the studies in the literature [36-38], defining the type of attack and determining its characteristic features have been focused on.

This study on the detection of DDoS attack types applied to any system will be a guide to develop a detection mechanism against attacks. The same detection or protection method will not be the solution for every type of attack. For this reason, it is necessary to develop methods suitable for the type of attack to protect systems and to make quick decisions. With this study, a different perspective and solution are presented for the detection of DDoS attacks. In future studies, it is aimed to consider the normal network data which have not been attacked, to evaluate different features, and to make a more comprehensive analysis.

REFERENCES

[1] Kabakuş A. T., Kara R. (2016). DDoSdaps4web: Web'e Yönelik DDoS Tespit ve Koruma Yöntemi. Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 32(1), 1-9.

[2] Devi S. R., Yogesh P. (2012). Detection of Application Layer DDoS Attacks Using Information Theory Based Metrics. Computer Science & Information Technology, Vol. 10, 217–223.

[3] Baykara, M., Daş, R. (2017). A Novel Hybrid Approach for Detection of Web-Based Attacks in Intrusion Detection Systems. International Journal of Computer Networks and Applications, 4(2), 62-76.

[4] Stein, L. D., Stewart, J. N., "The World Wide Web Security FAQ: Securing Against Denial of Service Attacks", www.w3.org/Security/Faq/wwwsf6.html.

[5] Gezgin, D. M., Buluş, E. (2014). Kablosuz Ağlar için Bir DoS Saldırısı Tasarımı. Bilişim Teknolojileri Dergisi, 6(3), 17-23.

[6] Raza, A. (2012). Anomaly Detection Systems for Distributed Denial of Service Attacks. University of Sindh, the Department of Electrical and Computer Engineering, Master Thesis, Pakistan.

[7] Wueest, C. (2014). Security Response: The Continued Rise of DDoS Attacks. Symantec White Paper, 1.

[8] Sonar, K., Upadhyay, H. (2014). A Survey: DDoS Attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58-63.

[9] Çelikbilek, İ. (2016). TCP SYN Seli Saldırısının Etkilerini Azaltmak için Yeni SYN Çerezleri Gerçeklemesi. İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul.

[10] McGregory, S. (2013). Preparing for the Next DDoS Attack. Network Security, 2013(5), 5-6.

[11] Ingle, A., Awade, M. (2013). Intrusion Detection for TCP–SYNC Flood Attack. International Journal of Advanced Research in Computer Science, 4(5) Special Issue, 9-11.

[12] Duan, Z., Yuan, X., Chandrashekar, J. (2006). Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates. In 25th IEEE International Conference on Computer Communications, Spain.

[13] Pahwa, P., Tiwari, G., Chhabra, R. (2010). Spoofing Media Access Control (MAC) and Its Counter Measures. International Journal of Advanced Engineering & Application, 186-192.

[14] Xie, Y., Yu, S. (2009). Monitoring the Application-Layer DDoS Attacks for IEEE. ACM Trans Netw, 17(1), 15-25.

[15] Söğüt, E. (2016). Gelişmiş Israrcı Tehdit Tespit Yöntemleri ve Bir Uygulaması. Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara.

[16] Cepheli Ö., Büyükçorak S., Karabulut K. G. (2014). Kullanıcı Modellemesi Tabanlı Dağıtık Servis Reddi Ataklarının Sezilmesi. In 22nd Signal Processing and Communications Applications Conference, 2186-2189, Trabzon.

[17] Yuan, J., Mills, K. (2005). Monitoring the Macroscopic Effect of DDoS Flooding Attacks. IEEE Transactions on Dependable and Secure Computing, 2(4), 324-335.

[18] Shiaeles, S. N., Katos, V., Karakos, A. S., et al. (2012). Real Time DDoS Detection Using Fuzzy Estimators. Computers & Security, 31(6), 782-790.

[19] Karimazad, R., Faraahi, A. (2011). An Anomaly-Based Method for DDoS Attacks Detection Using RBF Neural Networks. In International Conference on Network and Electronics Engineering, vol. 11, IACSIT Press, Singapore.

[20] Al-Duwairi, B. N. (2005). Mitigation and Traceback Countermeasures for DDoS Attacks. Iowa State University, Doctoral Thesis, USA.

[21] Limwiwatkul, L., Rungsawang, A. (2004). Distributed Denial of Service Detection Using TCP/IP Header and Traffic Measurement Analysis. In IEEE International Symposium Communications and Information Technology, vol. 1, 605–610, Japan.

[22] Oo T. T., Phyu T. (2014). Analysis of DDoS Detection System Based on Anomaly Detection System. In International Conference on Advances in Engineering and Technology, Singapore.

[23] Wireshark, www.wireshark.org.

[24] Witten I. H., Frank E., Hall M. A., et al. (2016). Data Mining: Practical Machine Learning Tools and Techniques, Morgan Kaufmann, Fourth Edition, Boston.

[25] KDD Cup 1999 Data, kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[26] Roolvink, S. (2008). Detecting Attacks Involving DNS Servers. University of Twente, Design and Analysis of Communication Systems. Master Thesis, The Netherlands.

[27] Erhan, D., Anarim, E., Kurt, G. K., Koşar, R. (2013). Effect of DDoS Attacks on Traffic Features. In 21st Signal Processing and Communications Applications Conference, Girne, 1-4.

[28] Sahi, A., Lai, D., Li, Y., et al. (2017). An efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment. IEEE Access, Vol. 5, 6036-6048.

[29] Han, F., Xu, L., Yu, X., et al. (2016). Sliding-Mode Observers for Real-Time DDoS Detection. In IEEE 11th Conference on Industrial Electronics and Applications, 825-830, USA.

[30] Osanaiye, O., Choo, K. K. R., Dlodlo, M. (2016). Analysing Feature Selection and Classification Techniques for DDoS Detection in Cloud. In Southern Africa Telecommunication and Applications Conference, 198-203, South Africa.

[31] Pala, T. (2013). Tıbbi Karar Destek Sisteminin Veri Madenciliği Yöntemleriyle Gerçekleştirilmesi. Marmara Üniversitesi, Yüksek Lisans Tezi, İstanbul.

[32] Kökver, Y., Barışçı, N., Çiftçi, A., Ekmekçi, Y. (2014). Hipertansiyona Etki Eden Faktörlerin Veri Madenciliği Yöntemleriyle İncelenmesi. Engineering Sciences, 9(2), 15-25.

[33] Quinlan, J. R. (1986). Induction of Decision Trees. Machine learning, 1(1), 81-106.

[34] Daş, B., Türkoğlu, İ. (2014). DNA Dizilimlerinin Sınıflandırılmasında Karar Ağacı Algoritmalarının Karşılaştırılması. Elektrik-Elektronik-Bilgisayar ve Biyomedikal Mühendisliği Sempozyumu, 381-383, Bursa.

[35] Tekerek, A. (2021). A Novel Architecture for Web-Based Attack Detection Using Convolutional Neural Network. Computers & Security, 100, 102096, ISSN 0167-4048.

[36] Tuan, T. A., Long, H. V., Son, L. H., et al. (2020). Performance Evaluation of Botnet DDoS Attack Detection Using Machine Learning. Evolutionary Intelligence, Vol. 13, 283-294.

[37] Devi, B. S. K., Preetha, G., Selvaram, G., et al. (2014). An Impact Analysis: Real Time DDoS Attack Detection and Mitigation Using Machine Learning. In International Conference on Recent Trends in Information Technology, 1-7.

[38] Doshi, R., Apthorpe, N., Feamster, N. (2018). Machine Learning DDoS Detection for Consumer Internet of Things Devices. In IEEE Symposium on Security and Privacy Workshops, 29-35.