A Machine Learning Based Approach for Detecting DRDoS Attacks and Its Performance Evaluation

Gao, Yuxuan
Department of informatics, Graduate School of Information Science and Electrical Engineering, Kyushu University

Feng, Yaokai
Faculty of Information Science and Electrical Engineering, Kyusyu University : Assistant Professor

Kawamoto, Junpei
Fuclty of Information Science and Electrical Engineering, Kyushu University : Assistant Professor

Sakurai, Kouichi
Faculty of Information Science and Electrical Engineering, Kyushu University : Professor

他

出版情報：Proc. of the 11th Asia Joint Conference on Information Security, 2016-08-04. AsiaJCIS
バージョン：
権利関係：

A Machine Learning Based Approach for Detecting DRDoS Attacks and Its Performance Evaluation

Yuxuan Gao, Yaokai Feng, Junpei Kawamoto, Kouichi Sakurai
Kyushu University
Department of informatics, Sakurai Laboratory
744 Motooka, Nishi-ku, Fukuoka 819-0395, JAPAN
yuxuangao92@gmail.com
fengyk@ait.kyushu-u.ac.jp, {kawamoto, sakurai}@inf.kyushu-u.ac.jp

***Abstract*—DRDoS (Distributed Reflection Denial of Service) attack is a kind of DoS (Denial of Service) attack, in which third-party servers are tricked into sending large amounts of data to the victims. That is, attackers use source address IP spoofing to hide their identity and cause third-parties to send data to the victims as identified by the source address field of the IP packet. This is called reflection because the servers of benign services are tricked into "reflecting" attack traffic to the victims. The most typical existing detection methods of such attacks are designed based on known attacks by protocol and are difficult to detect the unknown ones. According to our investigations, one protocol-independent detection method has been existing, which is based on the assumption that a strong linear relationship exists among the abnormal flows from the reflector to the victim. Moreover, the method is assumed that the all packets from reflectors are attack packets when attacked, which is clearly not reasonable. In this study, we found five features are effective for detecting DRDoS attacks, and we proposed a method to detect DRDoS attacks using these features and machine learning algorithms. Its detection performance is experimentally examined and the experimental result indicates that our proposal is of clearly better detection performance.**

Keywords—DRDoS, Machine Learning, attack detection

I. BACKGROUND

DoS (Denial of Service) attack is an attack which the victim will be prevented to do useful work by one or more machines [1]. That is, DoS attacks aim at making services unavailable to their legitimate users. Attackers can use different methods to consume bandwidth or deplete other resources of the victim. In order to improve the attack effect, the actual DoS attackers often hijack numerous machines (called bots) and use them to attack simultaneously, which is known as DDoS (Distributed Denial of Service). Furthermore, DRDoS (Distributed Reflection Denial-of-Service) attacks have become a headache problem in the Internet security community. In DRDoS attacks, an attacker sends forged requests to several servers with the victim's spoofed source address. In response, the servers will send replies to the victim. And these replies are often significantly (many times) larger than the requests. In such cases, the attacks also can be called amplification attacks [7][8]. In this way, the bandwidth or deplete other resources of the target (victim) will be consumed badly. As a result, the victim will be received a lot of response packets and cannot do normal work.

Recent research has shown that at least 14 UDP-based protocols are vulnerable to such attacks [3]. Reports show that current attacks can result in more than 100 Gbit/s of bandwidth consumption [10]. The spam block-list provider Spamhaus was attacked in March 2013 with an unprecedented traffic rate of up to 300 Gbit/s [11].

The countermeasure of DRDoS attacks generally consists of two parts: detection and packet-filtering [9]. In this paper, we focused on the detection of DRDoS attacks, and propose a new approach to improve the detection performance.

Many approaches have been proposed to fight against DRDoS attacks, which will be introduced briefly in Section III. Furthermore commercial products for the purpose exist [12]. However, many of them try to detect such attacks in the reflectors. Of course, operators of the reflectors are in a good position to take effective countermeasures if they are aware of that their services are used in an attack. However, to enable service operators to employ countermeasures, they first must know that their services are abused as amplifiers. In fact, it is nearly impossible to make all of them take the effective measures for such attacks. This mainly has the following two reasons. 1) There exist so many potential reflectors. For example, only for open recursive resolver (DNS server), it is said that this number had been up to 28,000,000 by Oct. 2013 [13]. 2) Illegitimate incoming requests might look the same as legitimate requests in reflectors.

Thus, protection and detection in end users (computers or edge routers) are also critical. However, only a few such researches exist. In this paper, we propose a protocol-free and feature-based detection method for end users.

Typical detection method of DRDoS attack is based on the statistical analysis of the number of the request-response pairs [8]. If you cannot find the corresponding requests for a large amount of responses, or say, you receive a lot of responses, although you not sending the requests then, you have been attacked. However, such approaches are designed by protocol, it is difficult to detect a new kind of DRDoS attack which utilizes whatever a protocol not utilized. On the other hand, although the protocol-independent approach has been proposed, it is difficult to detect such a small scale attack, which only occupies a small portion of traffics, because it is assumed that all of the traffics from the reflectors are attack ones. And since the detection approach only counts the number of packets, it

may result that the normal communication which accounts for all traffic will be detected as an attack. In order to solve such a drawback, we proposed an approach which will improve the protocol-independent detection approach.

To detect DRDoS attack without relying on protocol, it is necessary to find a common feature which will be active to all of the kinds of DRDoS attack. In the conventional approach, the packets from the reflectors are all assumed as attack packets, and detected by the flow unit, which contains the packets with the same source and destination. By comparing the flow received with the known DRDoS attack flow, if the received one is also attack flow, then the two flows are both attack ones, even though they are different kinds of DRDoS attacks, they will have the following features. The cumulative of the number of packets will have a strong linear relationship with a time unit. And this feature can be used to detect a DRDoS attack.

We found five features which will largely change during DRDoS attacks compared with the normal value. They are the number of packets in a time unit which only contain the IP header without TCP or UDP header in the packet header part; the sum of the sizes of the UDP packets sent to the target in a time unit; the number of the packets sent to the target in a time unit; the difference between the number of the packets sent from the target and the number of the packets sent to the target; and the maximum number of the packets in a time unit sent to the target among all the ports. In this paper, we proposed an approach based on these five features and machine learning algorithm.

The rest of the paper is organized as follows. We will introduce the conception and types of the DRDoS attack in section 2, and in section 3 we will introduce the relation research of DRDoS detection approaches. In section 4 and section 5 we will discuss the approach we proposed and the experiment and verification for it. At last, in section 6, we will make a summary.

II. THE DRDOS ATTACK

A. Introduction

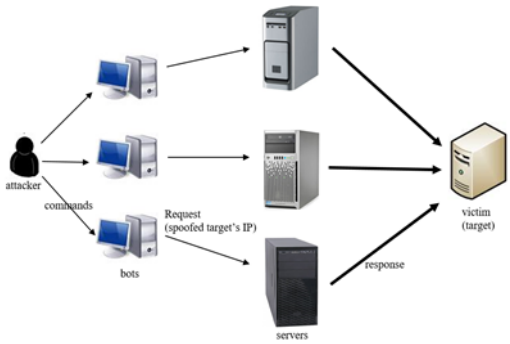


Fig. 1 General architecture of DRDoS attack.

Figure 1 shows an example of DRDoS. In this figure, an attack compromised a group of computers (bots), each of which sends forged requests to one or multiple servers (or say reflectors) with the target's IP address as the (spoofed) source address of the requests. Then, in response, the servers are cheated and send replies to the target (victim). And these replies are often significantly (many times) larger than the requests. In such cases, the attacks also can be called amplification attacks [7][8]. In this way, the bandwidth or deplete other resources of the target (victim) will be consumed badly. As a result, the victim will be received a lot of response packets and cannot do normal work.

B. Amplification Factors

As we introduced in the first section, DRDoS attack refers to the reflection attack. And the attackers often utilize amplification attacks to increase the attack effect. Thus, in order to measure the effect of the DRDoS attack, the concept of amplification factor has been introduced [3]. Amplification factor is divided into two types: PAF (packet amplification factor) and BAF (bandwidth amplification factor), which are defined in Equation (1) and Equation (2), respectively [3].

$$BAF = \frac{len(UDP\ payload) reflector\ to\ victim}{len(UDP\ payload) attacker\ to\ reflector} \quad (1)$$

$$PAF = \frac{number\ of\ packets\ reflector\ to\ victim}{lnumber\ of\ packets\ attacker\ to\ reflector} \quad (2)$$

In other words, BAF measures the amplification effect in terms of payload, and PAF measures the amplification effect in terms of the number of packets. The BAF measures the actual impact of the attacks [3] because a larger BAF means a bigger effect of the attack.

C. Types of DRDoS Attack

DRDoS attack can be divided into two types based on the protocol used in the attack. One is attacks utilizing TCP and called as TCP-based attacks. Obviously, it will be impossible for an attacker to launch any DRDoS attacks after completing the TCP handshake. This is because the session between the server and the bot (attacker) has already been established at that time. That is, if an attacker wants to launch a TCP-based attack, only the SYN/SYN-ACK pair can be used. In this case, the amplification attack is difficult to apply and BAF is always only around 1. In some SYN/ACK attacks, an attacker sends spoofed SYN requests to a reflector so that the reflector sends SYN/ACK packets to the target [24]. As well as the final destination (target/victim) as indicated by the spoofed source IP address, it is also possible for reflectors, uplinks, and other end-hosts which rely on them to be victims of reflection attacks. In SYN flooding attacks [16], [19]–[23], the attacker floods a reflector with spoofed SYN requests and changes the source IP address of packets so they do not receive replies. The aim of SYN flooding attacks is not only to attack the final destination indicated by the spoofed IP address, but also to consume enough resources at the reflector to make it unresponsive to legitimate traffic.

The other kind of DRDoS attacks is those utilizing UDP and are called UDP-based attacks. Since no handshake is necessary in UDP communicating, the number of the kinds of request-response pairs that may be utilized by DRDoS attacks is increased significantly. Handley et al. made an experiment to calculate the BAF and PAF for each 14 kinds of protocols [3]. The results of the experiment are shown in Table 1. Just like the result showing, there are a few protocols which will cause

high BAF in UDP-based attacks. For this reason, the UDP-based attack is the mainstream of DRDoS attacks.

TABLE I. TYPICAL AMPLIFICATION FACTORS OF EACH PROTOCOL

Protocol	BAF	PAF	Scenario
SNMP v2	6.3	1.00	GetBulk request
NTP	556.9	3.84	Request client statistics
DNS_{NS}	54.6	2.08	ANY lookup at author. NS
DNS_{OR}	28.7	1.32	ANY lookup at open resolv.
NetBios	3.8	1.00	Name resoluteion
SSDP	30.8	9.92	SEARCH request
CharGen	358.8	1.00	Character generation request
QOTD	140.3	1.00	Quote request
BitTorrent	3.8	1.58	File search
Kad	16.3	1.00	Peer list exchange
Quake 3	63.9	1.01	Server info exchange
Steam	5.5	1.12	Server info exchange
ZAv2	36.0	1.02	Peer list and cmd exchange
Sality	37.3	1.00	URL list exchange
Gameover	45.4	5.39	Peer and proxy exchange

Akamai detected 9 attacks involving NTP, Char-Gen, and SSDP which peaked over 100 Gbps in the last 3 months of 2014. This is three times more than in the same period in 2013 [17]. The work [4] showed that the bandwidth used in DRDoS attacks is growing. In March 2013, an attack was launched against Spamhaus [14]. The DNS based attack reached an estimated peak of about 300Gbps and was the biggest DoS attack ever recorded [18]. Nearly a year later and an even bigger attack reportedly reached a peak of 400Gbps by using NTP [15]. The attack traffic generated during the Spamhaus attack came from over 30,000 different DNS servers.

Figure 2 shows typical DRDoS attacks in 2013 and 2014 [4]. The y-axis is the amount of attack traffics (Gbps). From the figure, we also can see that UDP-based attack is the mainstream of DRDoS.

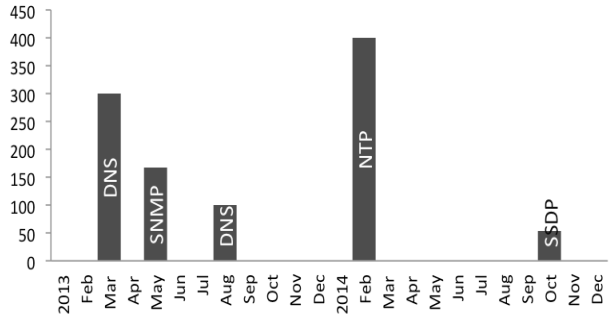


Fig.2 DRDoS attack strength in recent years [4].

III. RELATED WORK

It is said that, there are four possible detection positions from the attackers to their targets for DRDoS attacks. They are the network which the target belongs to, the ISP network which the target uses, the upstream network and the network which the attacker uses [5]. However, it is not easy to detect DRDoS attacks. Among the existing approaches, the most detect the attacks at the network which the target belongs to. Furthermore, the existing approaches can be classified as shown in Figure 3 [3]. In this study, we try to detect attacks at individual routers and our proposal is protocol-independent. That is, our proposal will ignore the protocol in the applications (whatever it is DNS, NTP or anything else).

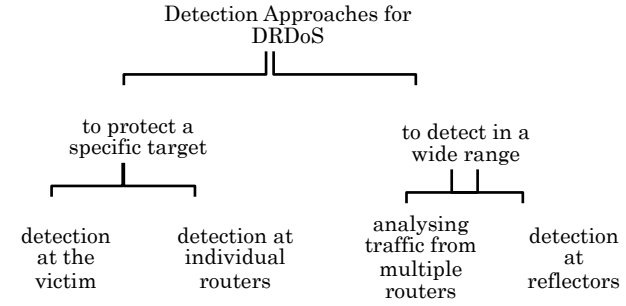


Fig.3 relationship diagram of DRDoS detection approaches.

As a proposal to detect DRDoS attacks at individual routers, Tsunoda et al. [6] try to match the responses and the requests at a point between the server (reflector) and the monitored target, and the detection result (whether the target was attacked or not) is determined according to the matching results. The approach recorded the requests and conjectured the possible responses. Then, the responses will be matched with the conjectured ones. The mismatched ones will be marked. However, in order to conjecture correctly, the important information of each packet such as source address, destination address, protocol and header must be recorded. Moreover, the approach can only detect known DRDoS attacks, which have been detected before.

Wei et al. proposed an approach [2], in which DRDoS attacks are detected by a unit of flow. Flow refers to the all packets which contains same source address and same destination address. The approach assumed that all the packets from reflectors are attacks during the attack period. Thus, in the work [2], it was said that there is a strong linear correlation between two DRDoS flows. Based on this feature, by computing the linear correlation between the coming flow and a known DRDoS flow, it can be determined whether or not a DRDoS has occurred. Figure 4 shows this idea of this approach [2]. In this figure, R_o, R_a, R_b are servers (possible reflectors). If the flow f_a and the flow f_b are DRDoS attacks, then it was said they should be of linear correlation. And this approach does not depend on protocols.

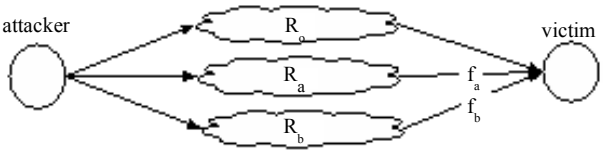


Fig. 4 the approach in [2] (from [2]).

On the other hand, some problems exist in this approach. Firstly, its assumption that all the packets from the reflectors are attack packets during an attack is obviously unreasonable. Secondly, since the approach only count the number of packets when detecting, the normal communication which accounts all of the traffics will have a high risk to be detected as an attack. Moreover, such an approach which detect at individual routers only work in the router closed to the monitored terminal. This is because that the communications between two terminals on the Internet unnecessarily always choose the same route.

In this study, five features and machine learning are utilized for detecting DRDoS attacks.

IV. OUR APPROACH

In order to solve the above-mentioned drawback of the protocol-independent detection approach, we proposed a novel approach. Since DRDoS attacks are typically UDP-based in recent years, we focus on detecting UDP-based attacks in this paper. In our proposal, five features and machine learning are utilized for detecting DRDoS attacks.

A. the features

In the approach we proposed, in order to protect a particular terminal, we choose the router in the boundary of the network which the terminal belongs to and the external network. We monitor the communications and the following five features are extracted from the traffic in each time unit.

- The number of the packets in a time unit that only contain the IP header without TCP or UDP header in the packet header part. Since the maximum bytes of a UDP datagram is larger than the maximum bytes of an IP packet, just as shown in Figure 5, a large UDP datagram will be divided into several IP packets. In other words, during a DRDoS attack, the packets that only contains the IP header without TCP or UDP header in the packet header part may be found repeatedly in a short time, which means that a large amount of UDP packets with a large size has been coming.

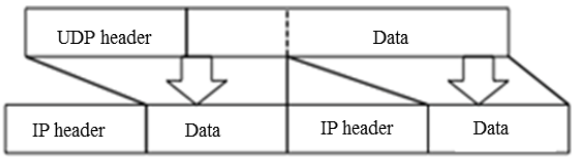


Fig.5 schematic diagram how UDP datagram divided.

- The size of the UDP packets sent to the target in a time unit. The sum of the size of the received UDP packets are used. Obviously, the value of this feature tends to become larger during a DRDoS attack.
- The total number of all the packets sent to the target in a time unit. For the DRDoS attacks with a small BAF value and a large PAF value, which is very possible, the change of this number is much bigger than the change of data size. Therefore, it is difficult to detect such attacks just based on the sum of the UDP packet size.
- The difference between the number of packets sent from the target and the number of packets sent to the target in a time unit. Since the DRDoS attack is a reflection attack, the number of responses to the target will be much larger than the number of requests from the target during a DRDoS attack.
- The maximum number of the packets in a time unit sent to the target among all the ports. In general, one DRDoS attack utilize one protocol. In other words, even if the attack is a distributed one, the attack packets are all from a same port. It means that the number of packets from a certain port will be increased clearly when a DRDoS attack occurred.

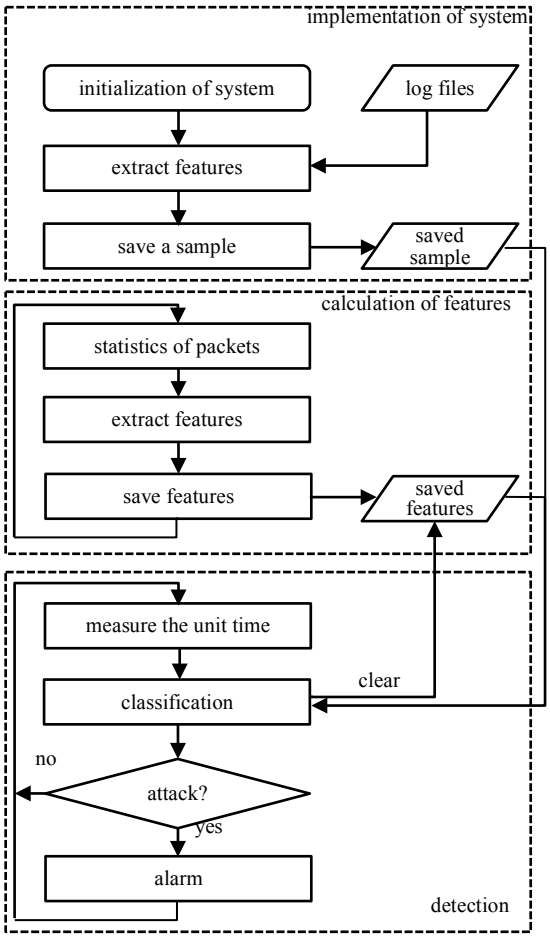


Fig.6 Our detection system of DRDoS attacks.

B. construction of a detection system

We constructed a system to detect DRDoS attack as shown in Figure 6. The system we proposed consists of three parts including the implementation of the system, the calculation of the features and detection.

Among them, the part of implementation of system shows the flow of system initialization. After taking the historic data of the terminal which we want to protect, each feature will be calculated.

The part of calculation of features shows the states of the packets and the flow of the feature quantity extraction. After receiving a packet, the five features will be updated by the new packet.

The part of detection shows the flow of how to determine whether attacked or not in a time unit. In order to measure the unit time, a timer will be used. After starting the timer, when it reaches the time set before, the following processes will be performed. First, the features which were saved until now will be classified based on the sample which were saved when the system initialize. The classification algorithm which will be used may be changed by historic data. We will discuss about it based on the result of the experiment in the next section. After classifying, the features saved will be cleared. In other words, the features saved just the statistical results in a unit of determined time. Then, if it is classified as an attack, the timer will be reset after an alarm, if not the timer will be reset directly.

V. EXPERIMENT AND VERIFICATION

In order to verify the detection rate of the proposed approach, we simulate DRDoS attacks and collect the data. After that, we make a classification about the data based on the five features we proposed. In this section, we will describe the data at first, then introduce the verification of each feature and the discussion about the detection rate.

A. experiment data

We collected five datasets from the attack simulation. We used the Chargen as the attack protocol, and used two computers as reflectors. See Figure 7. The reflectors PC-C and PC-D provide Chargen service. PC-A is the attacker who sent random UDP packets to the port 19 of PC-C and PC-D. The source IP address of the request packets have been faked as PC-B. Then, PC-B became the target of the attack. The response packets from reflectors became the attack packets. Finally, we collected packet data at PC-B.

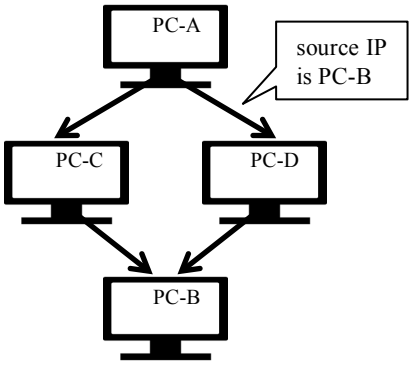


Fig.7 chematic diagram of the experiment.

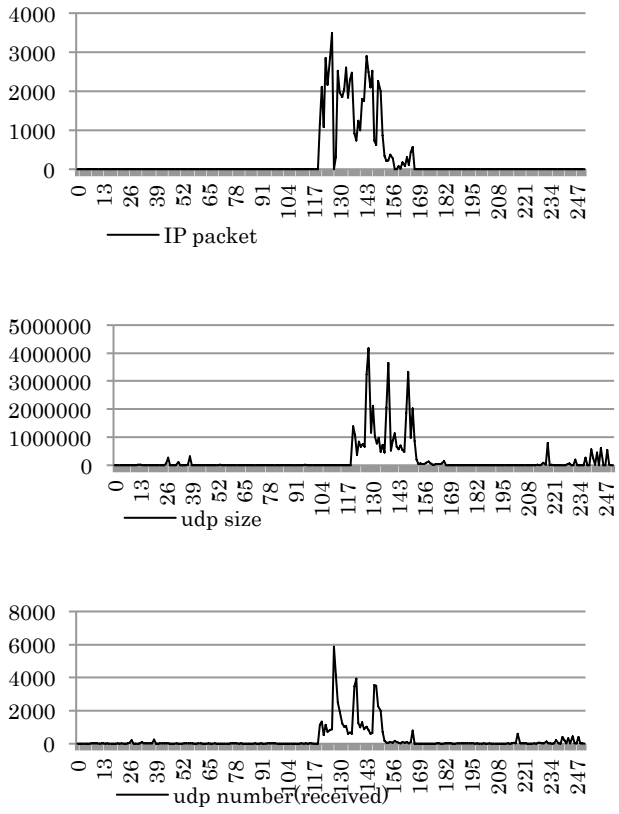
The characteristics of each dataset are shown in Table II. The unit of collection time and attack time is second.

TABLE II. CHARACTERISTICS OF EACH DATASET

Dataset	Collection time (s)	Attack time (s)	Attack catalog
1	668	117	Chargen
2	524	32	Chargen
3	940	40	Chargen
4	1038	46	Chargen
5	212	52	Chargen

B. the vertification of each feature

Figure 8 shows how each feature changed in dataset 5. The x-axis is the time in second. The y-axis shows the value of each feature, and from top they are, (feature 1) the number of packets which only contain the IP header without TCP or UDP header in the packet header, (feature 2) the sum of the size of the UDP packets which destine to the target, (feature 3) the number of the packets which destine to the target, (feature 4) the difference between the number of the packets sent from the target and the number of the packets destining to the target, and (feature 5) the maximum number of the packets which destine to the target for each port. The attack occurred from 120 seconds to 171 seconds. According to the results shown in the figure, we can see that each of the features is effective for detecting DRDoS.



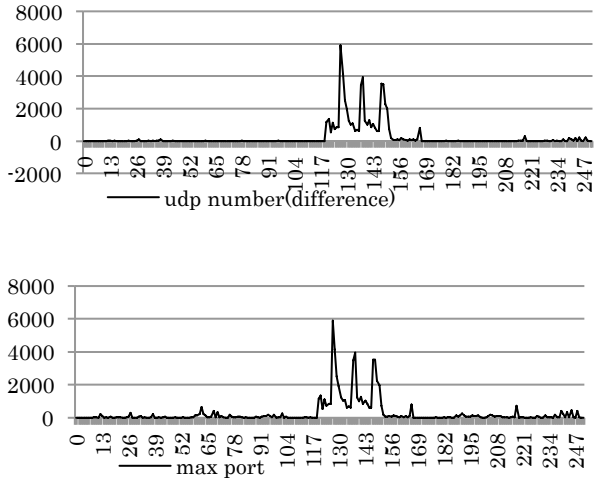


Fig. 7 the change of each features

C. discussion about detection rate

In our experiment, a sample dataset and a test dataset are needed. The experiment is conducted using all the possible pair of the above-mentioned five datasets as the sample dataset and test dataset. The total success rate, the detection rate and the false positive rate are used to evaluate the detection performance of our proposal. Each definition of the evaluation criterion is showed following.

$$Total\ success\ rate = \frac{The\ number\ of\ data\ classified\ correctly}{The\ number\ of\ total\ data}$$

$$Detection\ rate = \frac{The\ number\ of\ attack\ data\ that\ are\ classified\ correctly}{The\ number\ of\ total\ attack\ data}$$

$$False\ positive\ rate = \frac{The\ number of\ normal\ data\ not\ classified\ correctly}{The\ number\ of\ total\ normal\ data}$$

The three evaluation criterion are defined as above. The total success rate evaluates the accuracy of the classification with both normal data and attack data. The detection rate evaluates the ratio of correctly detected attack data to all of the attack data. And the false positive rate evaluates the ratio of the data which is normal but detected as attack to normal data. The larger total success rate, detection rate and the lower false positive rate means a better result.

For classification algorithm, we chose SVM to conduct the experiment. And we used the normalized polynomial kernel as a kernel function. Table III shows the result of the experiment. As a comparison, we also calculated the total success rate, detection rate and false positive rate by using the approach proposed in the related research [2] with the same dataset. And the result is showed in Table IV.

TABLE III. RESULT BY USING APPROACH WE PROPOSED

Total success rate(%)					
test / sample	1	2	3	4	5
1	99.55	99.62	100.00	99.90	99.06
2	98.20	99.24	99.57	99.61	97.64
3	93.26	93.13	99.79	99.81	97.17
4	92.81	92.18	99.79	99.71	97.17
5	95.51	93.51	99.89	100.00	98.11
Detection rate(%)					
test / sample	1	2	3	4	5
1	97.44	93.75	100.00	97.83	96.15
2	92.31	90.63	92.50	91.30	96.15
3	92.31	100.00	97.50	97.83	92.31
4	89.74	100.00	97.50	95.65	92.31
5	97.44	100.00	100.00	100.00	96.15
False positive rate(%)					
test / sample	1	2	3	4	5
1	0.00	0.00	0.00	0.00	0.00
2	0.54	0.20	0.11	0.00	1.88
3	6.53	7.32	0.11	0.10	1.25
4	6.53	8.33	0.11	0.10	1.25
5	4.90	6.91	0.11	0.00	1.25

TABLE IV. RESULT BY USING APPROACH IN RELATED RESEARCH [2]

Total success rate (%)					
test / sample	1	2	3	4	5
1	67.90	77.78	81.50	89.29	83.96
2	71.60	79.01	82.66	90.08	85.85
3	74.07	87.04	88.44	92.06	90.09
4	55.56	76.54	69.36	80.16	77.36
5	54.32	77.16	71.10	79.76	78.30
Detection rate (%)					
test / sample	1	2	3	4	5
1	96.15	95.65	100.00	100.00	96.15
2	96.15	95.65	100.00	100.00	98.08
3	96.15	95.65	100.00	100.00	98.08
4	96.15	95.65	100.00	100.00	96.15
5	92.31	95.65	100.00	100.00	94.23
False positive rate (%)					
test / sample	1	2	3	4	5
1	45.45	25.18	21.05	13.17	20.00
2	40.00	23.74	19.74	12.20	18.13
3	36.36	14.39	13.16	9.76	12.50
4	63.64	26.62	34.87	24.39	28.75
5	63.64	25.90	32.89	24.88	26.88

By this comparison between Table III and Table IV, we can see that the approach we proposed maintains a clearly higher detection rate and, at the same time, the false positive rate was much reduced.

VI. CONCLUSION

In this paper, we introduced the background and related researches about detection of DRDoS attack. And we also pointed out some drawbacks of the existing approaches. Then our new approach using five features was proposed and its performance was verified by experiments. The experiment result indicated that our proposal has a clearly better performance for detecting DRDoS attacks. In the future, some other datasets and other machine learning algorithms will be used to examine the behavior of our proposal.

REFERENCES

[1] Handley, M., and Eric Rescorla. "RFC 4732: Internet Denial-of-Service Considerations." (2006).

[2] Wei W., et al. "A rank correlation based detection against distributed reflection DoS attacks." Communications Letters, IEEE 17.1 (2013): 173-175.

[3] Rossow C., "Amplification hell: Revisiting network protocols for DDoS abuse." Symposium on Network and Distributed System Security (NDSS). 2014.

[4] Ryba, Fabrice J., et al. "Amplification and DRDoS Attack Defense--A Survey and New Perspectives." arXiv preprint arXiv:1505.07892 (2015).

[5] Chang, Rocky KC. "Defending against flooding-based distributed denial-of-service attacks: a tutorial." Communications Magazine, IEEE 40.10 (2002): 42-51.

[6] Tsunoda, Hiroshi, et al. "Detecting DRDoS attacks by a simple response packet confirmation mechanism." Computer Communications 31.14 (2008): 3299-3306.

[7] T.Bottger, L. Braun, O. Gasser, F. Eye, H. Eeiser, and G. Carle, "DoS Amplification Attacks—Protocol-Agnostic Detection of Service Abuse in Amplifier Newtworks., IFIP Intenational Federation for Information Processing, TMA2015, LNCS 9093, 205-218, 2015

[8] G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, "Detecting DNS Amlification Attacks", CRITIS2007, LNCS 5141, 185-196, 2008

[9] C. Sun, B. Liu, and L. Shi, "Efficient and Low-Cost Hardware Defense Against DNS Amplification Attacks", IEEE GLOBALCOM2008.

[10] https://www.arbornetworks.com/ (last accessed: April 2016).

[11] M. Kumar, "World's biggest DDoS attack that Almost Broke the Internet", The Hacker News, Mrch 28, 2013. http://thehackernews.com/2013/03/worlds-biggest-ddos-attack-that-almost.html (last accessed: April 2016).

[12] CloudFlare: https://www.cloudflare.com (last accessed: April 2016).

[13] http://www.openresolver.jp/ (last accessed: April 2016).

[14] Prince M., "The DDoS That Almost Broke the Internet", March 2013 [Online]. http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet (last accessed: April 2016)

[15] Prince M, "Technical Details Behind a 400Gbps NTP Amplification DDoS Attack," Feb 2014 [Online]. http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack (last accessed: April 2016)

[16] Chang R, "Defending against flooding-based distributed denial-of-service attacks: A tutorial," Communications Magazine,IEEE, vol. 40, no. 10, pp. 42–51, Oct 2002.

[17] Akamai, "The State of the Internet [security]," September 2014. [Online]. http://www.stateoftheinternet.com/resources-web-security-2014-q4-internet-security-report.html (last accessed: April 2016)

[18] T. Brewster, "Prolexic CEO: Biggest Cyber Attack Ever Was Built on Lies," April 2013. [Online]. http://www.techweekeurope.co.uk/workspace/prolexic-ceo-scott-hammack-biggest-cyber-attack-lies-spamhaus-113551 (last accessed: April 2016)

[19] Chen W. and Yeung Y., "Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing", International Conference on Networking, IEEE, April 2006.

[20] Nashat D, Jiang X, "Detecting SYN Flooding Agents under Any Type of IP Spoofing," IEEE International Conference on e-Business Engineering, October 2008, pp. 499–505.

[21] Noureldien A., "Block Spoofed Packets at Source (BSPS): A Method for Detecting and Preventing all Types of Spoofed Source IP Packets and SYN Flooding Packets at Source: A Theoretical Framework", Second International Conference on the Applications of Digital Information and Web Technologies. IEEE, pp. 579–583. Aug 2009.

[22] Kavisankar L. and Chellappan C., "A Mitigation Model for TCP SYN Flooding with IP spoofing," in International Conference on Recent Trends in Information Technology (ICRTIT). IEEE, pp. 251–256, June 2011.

[23] Gilad Y. and Herzberg A., "LOT: A Defense Against IP Spoofing and Flooding Attacks," ACM Trans. Inf. Syst. Secur.,vol. 15, no. 2, pp. 6:1–6:30, Jul. 2012.

[24] Paxson V., "An Analysis of Using Reflectors for Distributed Denial-of-service Attacks," ACM SIGCOMM Comput. Commun. Rev., vol. 31, no. 3, pp. 38–47, Jul. 2001.