*2011 International Conference on Network and Electronics Engineering*
*IPCSIT vol.11 (2011) © (2011) IACSIT Press, Singapore*

# An Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks

Reyhaneh Karimazad[1 +] and Ahmad Faraahi[2]

[1] M.S Student, Department of Computer Engineering and Information Technology, Payame Noor University
[2] Assistant Professor, Department of Computer Engineering and Information Technology, Payame Noor University

**Abstract.** Distributed denial of service (DDoS) attacks are serious threats for availability of the internet services. These types of attacks command multiple agents to send a great number of packets to a victim and thus can easily exhaust the resources of the victim. In this paper we propose an anomaly-based DDoS detection method based on the various features of attack packets, obtained from study the incoming network traffic and using of Radial Basis Function (RBF) neural networks to analyze these features. We evaluate the proposed method using our simulated network and UCLA Dataset. The results show that the proposed system can make real-time detection accuracy better than 96% for DDoS attacks.

**Keywords:** DDoS attack; abnormal traffic; RBF neural networks; network security.

## 1. Introduction

As the Internet becomes an essential part of human life, providing security of data passed over the internet is getting more crucial. The Internet was initially designed for openness and scalability without any security concern. Hence, malicious users exploit this weakness to achieve their purpose. In recent years, the number of network-based threats has been significantly increased. DDoS attacks are one of the major types of these threats. The aim of these attacks is to make internet-based services unavailable to its legitimate users. Although widely known web sites, such as Yahoo, CNN, eBay, and Amazon.com were well-equipped in security, reports show that in 2000 they were damaged by DDoS attacks [1]. The DDoS attacks usually do not exploit of security vulnerabilities of network-connected systems, but instead they aim to disrupt victim services by overwhelming the processing capacity of system or by flooding the bandwidth of the target. SYN flooding attacks, DNS flooding attacks and Smurf attacks are major DDoS attacks according to Arbor's survey in 2008[2].

There are two separate steps of DDoS attacks: compromising internet hosts and flooding the victim system. In the first step, attacker compromises a large number of internet hosts using vulnerable software installed on them. Then, attacker installs attack software on compromised systems. These hosts called agent and attacker controls them via handler systems. In the second step, attacker commands to the agents through handler systems to generate and send high volume of useless packets to victim simultaneously. The volume of sent packets is so high that the victim cannot response to them and then be exhausted. Using multiple agents and IP (Internet Protocol) spoofing techniques in DDoS attacks causes the detection becomes more difficult [3]. In this paper, we propose an anomaly-based DDoS detection method based on features obtained from attack packets analysis. The RBF neural network is then utilized to analyze proposed features. The result of this study can be applied to edge router of victim networks.

[+] Corresponding author. Tel.: +98-912-216-2958.
*E-mail address*: r.karimazad@gmail.com.

This paper organized as follows: Section 2 introduces the previous researches relevant to DDoS attack detection. The proposed method architecture is presented in Section 3. DDoS detection module is detailed in Section 4. Experimental evaluation results are included in Section 5. Finally, this paper is concluded in Section 6.

## 2. Related researches

As the damage by DDoS attack increases, a great number of detection methods have been presented. Many of these methods are based on identifying anomalies in network traffic. In [4], seven variables are selected by exploiting of DDoS attacks architecture properties in order to detect DDoS attacks. Then clustering analysis is performed to distinguish the normal traffic from attack phases. DARPA Dataset 2000 [5] is applied to evaluate this method. The proposed detection system can be used in a way that both of attacker and victim are in the same network.

In [6], the correlation between the outgoing and incoming traffic of a network is analyzed and the changes in the correlation are used to detect DDoS attack. Fuzzy classification is used in this method in order to guarantee the accuracy. This method is evaluated using DARPA datasets. In [7], a combined data mining approach is proposed to classifying the traffic pattern to normal and diverse attacks. This approach is used decision tree to selecting important attributes and neural networks are exploited to analyze the selected attributes. In [8], a source-based DDoS attack detection system called D-WARD is proposed. This system is installed at the edge routers of network and monitors the incoming and outgoing packets and limits the traffic based on asymmetric packet rate.

## 3. System Architecture

The system architecture is shown in Figure 1. It can be divided into four modules, i.e. Packet Capturing Module, DDoS Detection Module, Filtering Module and Attack Alarm Module.

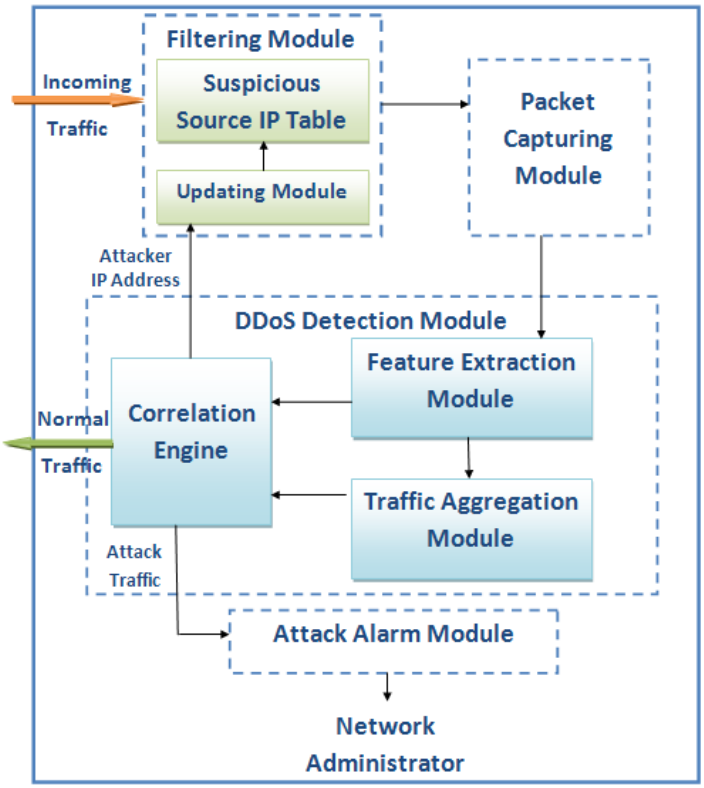


Fig. 1: The overall architecture of proposed DDoS detection system.

### 3.1. Packet Capturing Module

Packet Capturing Module sniffs incoming traffic to the network and captures packets with each TCP, UDP and ICMP protocols in fixed time-windows. All of the captured packets are sent to DDoS Detection Module and proposed features are estimated via Feature Extraction Module.

### 3.2. DDoS Detection Module

Proposed DDoS Detection Module consists of three parts: Feature Extraction Module, Traffic Aggregation Module and Correlation Engine. This module analyzes captured packets to recognize attacks and classifies packets to attack traffic and normal traffic classes. We will explain this module in next section in details.

### 3.3. Filtering Module

Filtering Module consists of two sub modules: Suspicious Source IP Table and Updating Module. After detecting attack packets, DDoS Detection Module sends attack source IP address to Updating Module. Updating Module updates the Suspicious Source IP Table and afterwards, Filtering Module filters incoming packets to the network based on Suspicious Source IP Table.

### 3.4. Attack Alarm Module

After detecting attack through DDoS Detection Module, this module sends alarm to administrator for further actions.

## 4. DDoS Detection Module

As mentioned in section 3, DDoS Detection Module consists of three main parts.

### 4.1. Feature Extraction Module

Feature Extraction Module calculates the selected features for captured packets. We propose these features by observing the characteristics of DDoS attack packets. These features can be used to recognize and classify incoming attack packets and will be analyzed in Correlation Engine. Time-window are used as the unit to deal with packet's features in this model. Experiments showed that these features contain significant information related to the presence of a DDoS attack. The following explains these proposed features:

- Average Packet Size: DDoS attacks flood victim to consume system resources, then Average Packet Size increases in attack time. We use this feature to identify DDoS attacks.
- Number of Packets: DDoS attacks send a great number of packets to the victim network. Therefore, the number of packets increases in comparison to normal case. We exploited this feature to detect DDoS attacks.
- Time Interval Variance: The experiments show when DDoS attack launches, agents send attack packets in the same time span. Then we can detect this attacks using Time Interval Variance. Whenever packet sending time spans are more similar together, Time Interval Variance will be closer to zero.Variance can be calculated through (1):

$$\frac{1}{n}\sum_{i=1}^{i=n}(X_i-\overline{X})^2 \quad (1)$$

- Packet Size Variance: According to our studies, we found that attack packets sizes are the same. However, normal packets have different sizes even when they belong to the same file. DDoS packets can be identified by using the Packet Size Variance.
- Number of Bytes: Increase in number of bytes demonstrates launching DDoS attacks.
- Packet Rate: This feature shows the packet rate sent from a source address to a destination in a specific time span. Packet rate increases significantly in attack time.
- Bitrate: A very high rate of this feature indicates launching DDoS attack.

### 4.2. Correlation Engine

Seven-feature vector produced by Feature Extraction Module is used to activate RBF neural network at each time-window. RBF neural network is applied to classify data to normal and attack categories. The most active output of RBF neural network indicates the presence of DDoS attack or normal traffic. If the incoming traffic is recognized as attack traffic, source IP address of attack packets will be sent to Filtering Module and

Attack Alarm Modules for further actions. Otherwise, if the traffic is normal, it will be sent to the destination. RBF neural network training can be performed as off-line process and used in real-time to detect attack faster.

### 4.3. Traffic Aggregation Module

As we know, DDoS attacks are distributed threats and attack packets are sent through multiple agents distributed on the internet. In reality, it is possible that packets captured from different Source IP addresses, are not recognized as attack packets while aggregation of packets sent from different sources to a specific destination makes a DDoS attack together. Therefore we proposed a Traffic Aggregation Module to aggregates incoming traffic from different sources to one specific destination and sends result table to Correlation Engine to detecting DDoS attack.

## 5. Experimental Evaluation

This section describes the performance evaluation results of proposed DDoS attack detection system. We evaluated our system with traffic traces of DDoS attacks designed in our simulated network and UCLA Dataset [9]. The evaluation process is divided to 3 steps. In the first step, the packets are captured from the network using a Linux based sniffer. In the second, step the proposed features are calculated from captured packets and related table is created, which each row of this table belongs to packets sent from one source IP address to a specific destination IP address. In the final step, the features were used to train the RBF neural network and test the proposed system.

### 5.1. Simulated Network Structure

Basically, our system is deployed at the ingress router of the victim network. By monitoring the incoming data, this system analyzes packets and detects attacks and normal traffic. We have implemented and evaluated our detection mechanism on a simulated network and UCLA Dataset. Figure 2 shows the structure of simulated network used in the experiments. It consists of 23 nodes. We choose a specific node to play the role of the victim while the other nodes send attack traffic to it. The DDoS attack was carried out using the Tribe Flood Network (TFN2k).

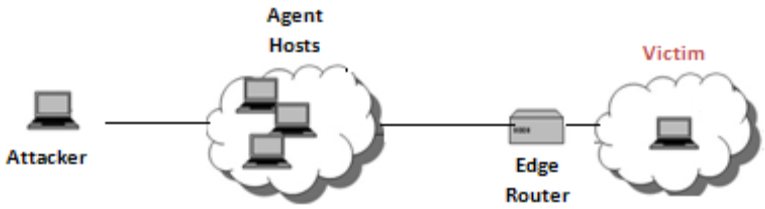


Fig. 2: The network structure used in the experiments.

### 5.2. The Feature Extraction Results

Table 1 summarizes the results of the Feature Extraction Module process. The results show that proposed features contain considerable information related to the presence of DDoS attack. For example Number of Packets increases in attack time and Time interval variance in attack case is close to zero because in DDoS attack, agents send packets in equal time spans. Because of high packet size similarity in attack packets, Packet size variance is close to zero. Moreover, Packet rate and Bitrate in attack time increases in compare to normal time.

Table1: Results of Feature Extraction Module process.

| No | Source IP | Destination IP | Calculated Features | | | | | | | Class |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | *Number of Packets* | *Average of Packet Size* | *Time Interval Variance* | *Packet Size Variance* | *Number Of Bytes* | *Packet Rate* | *Bite Rate* | |
| 1 | 58.129.199.9 | 1.1.54.40 | 3 | 31 | 0.58 | 3.6 | 94 | 0.61 | 154.89 | Normal |
| 2 | 69.9.232.197 | 1.1.180.177 | 17 | 67 | 5.78 | 64.88 | 1140 | 1.27 | 682.79 | Normal |
| 3 | 1.1.139.167 | 1.1.236.8 | 1544 | 995 | 0.001 | 0.02 | 1536535 | 34.73 | 276529.58 | Attack |
| 4 | 1.1.139.229 | 1.1.236.8 | 1604 | 994 | 0.001 | 0.01 | 1594593 | 36.08 | 286958.36 | Attack |

## 5.3. The RBF Training Process

RBF is a non-linear neural network with 2 layer hidden neurons. We estimate our proposed system with hidden neurons ranging from 2 to 15. Gaussian functions are used as the non-linear RBF functions and K-means cluster algorithm estimates mean and variance for Gaussian function [10]. The captured packets and UCLA Dataset are used to train RBF neural network. We used combination of normal and attack packets to this purpose. K-Fold Cross validation, with value 10 for variable K, is applied on datasets to produce test and train data.

## 5.4. The Experiments

In the experiments, DDoS attack was launched on the simulated network. We captured 41,175 packets for the normal traffic and 36,325 packets for the DDoS attack traffic. Table 2 shows the performance results of our detection mechanism in terms of false alarms and correct detection rate. Experimental results show DDoS attack detection accuracy about 98.2% for UCLA Dataset and also about 96.5% for simulated network.

Table2: RBF neural network analysis results in terms of false alarms and correct detection rates.

| **Proposed system evaluation results** | **False alarm** | | **Correct detection** | |
|---|---|---|---|---|
| | ***Normal Data (False Positive Rate)*** | ***Attack Data (False Negative Rate)*** | ***Normal Data (True Negative Rate)*** | ***Attack Data (True Positive Rate)*** |
| UCLA Dataset | 0.01 | 0.02 | 0.98 | 0.97 |
| Simulated Network | 0.03 | 0.04 | 0.96 | 0.96 |

# 6. Conclusion

The DDoS is becoming one of the most common types of attacks on the internet. As the use of the internet increasing, the need for more efficient DDoS detection system becomes critical. In this paper we present an efficient method to detect DDoS attacks using RBF neural networks. To this purpose, DDoS attack packets are studied and seven features proposed which show the abnormal changes in incoming traffic. After the feature extraction, RBF neural network is applied to classify traffic into normal and DDoS attack traffic classes. In order to evaluate our detection method, we experiment with our simulated network and UCLA Dataset. Experimental results show that proposed method can detect DDoS attacks effectively. Moreover, our system can filter the attack traffics quickly and forward the normal traffics simultaneously. It is shown that the proposed method can successfully identify DDoS attacks with very high detection rates.

# 7. References


[1] Z. Fengxiang, Sh.ABE. A Heuristic DDoS Flooding Attack Detection Mechanism Analyses based on the Relationship between Input and Output Traffic Volumes. *Computer Communications and Networks*. 2007, pp. 798-802.

[2] Arbor Networks. *Worldwide Infrastructure Security Report*, http://www.arbornetworks.com/report. Sept 2008.

[3] Ch.Douligeris, A. Mitrokotsa. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks, Elsevier*. 2003, 44(5): 643-666.

[4] K.Lee, J.Kim,K. Hoon Kwon, Y.Han and S.Kim. DDoS attacks detection method using cluster analysis. *Expert System with Applications, Elsevier*. 2008, 34(3): 1659–1665.

[5] DARPA intrusion detection datasets. http://www.ll.mit.edu/IST/ideval/data/2000/2000_data_index.html.

[6] W.Wei, Y.Dong, D.Lu, and G. Jin. Combining Cross-Correlation Fuzzy Classification to Detect Distributed Denial-of-Service Attacks. *LNCS,Springer*. 2006, 3994: 57-64.

[7] M.Kim, H.Na, k.Chae, H.Bang, J.Na. A Combined Data Mining Approach for DDoS Attack Detection. *LNCS, Springer*. 2004, 3090: 943-950.

[8] J. Mirkovic, G. Prier, P. Reiher. Attacking DDoS at the source. *Proc of ICNP 2002, France*. 2002, pp. 312–321.

[9] UCLA CSD packet traces. http://www.lasr.cs.ucla.edu/ddos/traces/public/usc.

[10] S. Haykin. *Neural networks: A Comprehensive Foundation*. Predice Hall, Upper Saddle River, NJ, 1994.