DDoS Attack Detection Using Sliding Window Method

Lu-yong ZHANG, Ming QIAN* and Yun-bing CHI

School of Telecommunications Engineering, Beijing University of Posts and Telecommunications, Beijing, China

*Corresponding author

Keywords: DDoS, Detection, Sliding window, Traffic, Network security.

Abstract. DDoS (Distributed Denial of Service) attack, with its simple, difficult to detect, destructive features, causes a huge threat to the network security. In this paper, we construct a DDoS attack detection system and propose a DDoS detection algorithm based on sliding window. The effect of sliding window with different sizes on the accuracy of results is discussed and an optimal value is chosen as model parameter. Besides, we extract the characteristics of traffic and experiments show these features are meaningful to detect whether DDoS attack happens. Finally we choose some of the features and get a uniform standard of judgment by preprocessing, transforming these features and setting rules. The experimental result shows that the proposed algorithm can effectively detect DDoS attacks in real time, and the accuracy rate is 93%.

Introduction

As the rapid development of Internet technology, the network has entered into our daily life bringing great convenience. However, the network security issues have become increasingly prominent. The threat of cyber security has always been an important research in academia Research topics. There are many kinds of network attacks. In all network attacks, DDoS attacks with its strong concealment and permeability, particularly simple to implement has become one of the most harmful network attacks with high attack success rate, causing great harm. In the era of big data, the scale of DDoS attacks has gradually increased and their destructive power are further enhanced.

The prevention and research of DDoS attacks have always been a hot topic and many scholars have proposed a lot of sophisticated algorithms to detect DDoS attacks. There have been some approaches that have been widely used, such as white list filtering, random packet loss, SYN cookie and other methods.

This article is organized as follows: Section II introduces some of the relevant work done by other scholars on DDoS attack detection. Section III mainly presents the overall system architecture and the contents of the algorithm which we have proposed as well as some of the factors we considered. Experiments and analysis are detailedly described in Section IV. Finally, we conclude our work and elaborate the meaning of our work in Section V.

Related Work

There have been various kinds of approaches and methodologies to reduce the harm of DDoS attacks regardless of any network environments. Most of them have been evaluated to work effectively. Jie-Hao [1] proposed a methodology using ANN(Artificial Neural Network) to detect whether DDoS attacks happened. The authors used Turing Test method to identify which user visits the system and record user behavior data including what resources user accesses and how long and when user accesses. By designing an intelligent user control system and train RBF neural network to detect attack. Siaterlis and Maglaris [2] give up the way of finding a single detection metric to reliably detect DDoS attacks. On the contrary they have attempted to make use of multiple metrics and they use Multi-Layer Perception (MLP) as a data classifier. Train data comes from different kinds of network characteristics and use these data to train the MLP. Finally it evaluates its...
performance in terms of accuracy rates in the face of new data. In the literature [3], Vijayasarathy R et al. classified the packets by the information of the packet header and the Bayesian classifier is constructed according to the different events of type of packet. Because the number of normal data packets of different categories and different characteristics will satisfy the certain proportion relation. When the attack occurs, relationship will be broken. Thus with this feature we can detect whether attack happens and can be able to locate what kind of anomaly happens.

The study refers to the previous research of Reyhaneh Karimazad and Ahmad Faraahi [4]. They proposed some specific characteristic features in the network data packages to classify normal traffic or abnormal traffic. We combine the advantage of other scholars’ work and construct a DDoS detection system using siding-window method with the key target of accuracy and timeliness.

Methodology
The system architecture is shown in Fig. 1. The DDoS detection system can be divided into 3 modules: Packet Capture Module, Filter Traffic Module and DDoS Detection Module.

Packet Capture Module
Jpcap [5] provides a set of Jar packages which provide the ability to capture network packets. Jpcap depends on libpcap [6], providing a strong ability to capture underlying data packet.

Java programs can only operate the transport layer data. If you want to directly operate the network layer, such as writing their own transport layer data packets, or write their own IP packets to the network, it is powerless. The Jpcap extension packets make up for this, so that we can support receiving IP packets from the network card or sending IP packets to the network card.

Filter Traffic Module
The traffic filtering module can be divided into three sub-modules: Filter Strategy Module, IP Blacklist, and Update Module. When the traffic of the suspect source IP address arrives, the abnormal traffic is intercepted according to the filtering policy [7]. If the traffic looks like normal, successfully pass the Filter Traffic Module, but the packet is detected as a harmful attack in the DDoS detection module, the attack source IP address is sent to the Update Module, and the Update Module then updates the suspect source IP Table to the IP blacklist, so that abnormal flow can be quickly and effectively intercepted, preventing sustained damage.
DDoS Detection Module

DDoS Detection Module is the core part of the system which plays a vital role in the overall performance of the entire system. DDoS detection Module mainly contains 4 parts: Feature Extraction Module, Sliding Window, Judge Engine and Alarm Module.

**Feature Extraction Module.** To determine whether suffering DDoS attacks in a moment, the essence of the problem is to extract the characteristics of the current flow. Compared to the normal flow, suffering DDoS attack is bound to show a certain degree of difference. If this difference is found, it can be a judge criteria.

Reyhaneh Karimazad and Ahmad Faraahi [4] suggest following features which experiments shows these characteristics are meaningful.

- Average Packet Size
- Number of Packets
- Time Interval Variance
- Packet Size Variance
- Number of Bytes
- Packet Rate
- Byte Rate

In the study we use Byte Rate as a mainly characteristic to help us detect DDoS attack. In general, the byte rate in normal flow will be relatively stable. Although there will be some subtle fluctuations, but in the statistical regularity the traffic is still reflected in a certain range of fluctuations within the average. When the host is subjected to DDoS attacks, the byte rate will appear in a short period of time surge, quickly reach a large order of magnitude.

**Sliding Window.** Suppose there is a time sequence: \(X_1, X_2, X_3, \ldots, X_{t-1}, X_t\). Current time is \(t\), and the value of one feature at time \(t\) is \(X_t\). We define the length of sliding window as \(n\). At time \(t\), the data in sliding window can be described as [\(X_{t-n+1}, X_{t-n+2}, \ldots, X_{t-n+k}, X_t\)], \(t = n, n + 1, n + 2, \ldots\)

At time \(t+1\), the data could be described as [\(X_{t-n+2}, X_{t-n+3}, \ldots, X_{t-n+k}, X_{t-1}, X_t, X_{t+1}\)]. From the expression we can find as time goes by new data will enter sliding window, the elements of the tail will leave the sliding window. We use Fig. 2 to describe the process.

![Figure 2. Process of sliding window.](image)

Time series data is smoothed and filtered by the sliding window. In the window length \(n\), the data is close to the smooth, the data handled by local average can filter out frequent fluctuations in the random error. So the sliding window average could be describe as Eq. 1.

\[
f_t = \frac{1}{N} \sum_{i=t-n+1}^{t} X_i\tag{1}
\]

Through the experiment we found selection of length \(n\) is pretty important to the accuracy of DDoS attack detection. In the Fig. 3 displays different length of sliding window. There are two lines show in the figure: Real Time Total Received Bytes and Real Time Total Received Bytes Threshold, among them The Real Time Total Received Bytes Threshold is the result of byte rate applied to sliding window.

Through the experiment we found in contrast to Fig. 3(a), after use sliding window, the chart will become smooth. The smoothing byte rate is used to predict the total byte rate of the future network. If the real time rate exceeds the average rate in the sliding window, it is assumed that the DDoS...
attack happens. In the experiment we set the number 10 as the length of sliding window, and the results prove the selection is correct.

Figure 3. Different length of sliding window.

Judge Engine. We use Real Time Total Byte Rate and Real Time Total Byte Rate Threshold as two mainly feature. If the Real Time Total Byte Rate is greater than 1.5 times Real Time Total Byte Rate Threshold, we believe DDoS attack happens.

Alarm Module. After DDoS attack happens and the system successfully detects the event, the alarm module sends the information to the network administrator. Besides, the attack event will store in the database including when the attack happens and who cause the attack.

Experiments and Analysis

We use famous DDoS tools LOIC (Low Orbit Ion Cannon) [8] to simulate DDoS attack and write a script to control the LOIC, aiming to start alternate with stop in the interval of 10 second. Table 1 shows how LOIC works in one minute.

Table 1. LOIC tool in one minute simulating DDoS.

<table>
<thead>
<tr>
<th>time[s]</th>
<th>0 ~ 10</th>
<th>10 ~ 20</th>
<th>20 ~ 30</th>
<th>30 ~ 40</th>
<th>40 ~ 50</th>
<th>50 ~ 60</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOIC Tool</td>
<td>start</td>
<td>stop</td>
<td>start</td>
<td>stop</td>
<td>start</td>
<td>stop</td>
</tr>
</tbody>
</table>

We run the script for 24 hours and there are 43200 seconds in the state of DDoS attack and 43200 seconds in the state of normal traffic. We start a DDoS attack every 10 seconds, so there is a total of 4320 DDoS attacks. We store these data in the database and use these data to train our detection system. Fig. 4 shows some data we collection in 24 hours.

Figure 4. Some of collection data in 24 hours.

In the experiments, we train and test our detection system using history data. In the training data there are 4320 DDoS attacks and if the number which detection system judges to be subjected to a
DDoS attack is closer to 4320, higher the accuracy rate. Finally we set the threshold as 1.5 times the average of sliding window and experimental results show the best performance. Our detecting algorithm detects 4105 attacks in total and the historical accuracy is 95%. By training we get the best parameters and apply them to the genuine traffic. We also run the 24-hour LOIC attack script. The total number of DDoS attacks is still 4320. The system detected DDoS attack 4011 times and the correct rate is 93%. Table 2 shows the experiment result.

<table>
<thead>
<tr>
<th>Situation</th>
<th>Number of Attack</th>
<th>Number of Detection</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training data</td>
<td>4320</td>
<td>4105</td>
<td>95%</td>
</tr>
<tr>
<td>Genuine traffic</td>
<td>4320</td>
<td>4011</td>
<td>93%</td>
</tr>
</tbody>
</table>

From the table we could find the accuracy in genuine traffic is less than training data. The result is possible because there are network fluctuation. In a test the accuracy is 93% and in another test the accuracy is 92% or 94%. So we take an average number of test results.

Conclusion

Today DDoS attacks become one of the most dangerous network attacks on the Internet. How to prevent DDoS attacks for an application becomes critical. In this paper, a DDoS detection method based on sliding window is proposed, which can detect DDoS attacks in real time efficiently. In the experiment, the real time byte rate processed by the sliding window is used to represent the current network environment. It is predicted that the network speed will stabilize for a certain period of time in the future, so it can identify whether the DDoS attack occurs. The experimental results show that the proposed method has the accuracy rate of 93% in the actual network environment, which can successfully detect DDoS attacks.

References


