INTRUSION DETECTION SYSTEM USING DISCRETE FOURIER TRANSFORM WITH WINDOW FUNCTION

Yusuke Tsuge and Hidema Tanaka

National Defense Academy of Japan
Hashirimizu 1-10-20 Yokosuka, Kanagawa Japan 239-8686,

ABSTRACT

An Intrusion Detection System (IDS) is countermeasure against network attack. There are mainly two types of detections; signature-based and anomaly-based. And there are two kinds of error; false negative and false positive. In development of IDS, establishment of a method to reduce such false is a major issue. In this paper, we propose a new anomaly-based detection method using Discrete Fourier Transform (DFT) with window function. In our method, we assume fluctuation of payload in ordinary sessions as random. On the other hand, we can see fluctuation in attack sessions have bias. From the viewpoint of spectrum analysis based on such assumption, we can find out different characteristic in spectrum of attack sessions. Using the characteristic, we can detect attack sessions. Example detection against Kyoto2006+ dataset shows 12.0% of false positive at most, and 0.0% of false negative.

KEYWORDS

Intrusion Detection System, Discrete Fourier Transform, window function, Kyoto2006+ dataset

1. INTRODUCTION

As one of countermeasures for cyber-attack, applying Intrusion Detection System (IDS) is now in common method [8]. The construction methods of IDS are divided into two types; signature-based and anomaly-based. In signature-based IDS, characteristic of intrusion packets are stored as signatures in a database [1][2][4][10][14]. By comparing contents of captured packets with the signatures, intrusion packets can be detected. This method can detect known attacks that are already analyzed. However, it is difficult to detect unknown attacks such as Zero-day attacks. So, signature-based IDS has false negative. Anomaly-based IDS, normal behavior is defined to distinguish abnormal communications [3][9][12]. Therefore, it may be able to detect unknown attacks. However, it is difficult to define “normal behavior”. So, anomaly-based IDS has false positive.

Nowadays, the speed of complication and evolution of attack technique is fast, so necessity of anomaly-based IDS is increasing, in especially for critical infrastructure. There are many techniques to construct anomaly-based IDS, we focus on the technique using Discrete Fourier Transform (DFT) [6][13]. Existing method shown in [13] is the method to focus on the number of access in the unit time and they claim their method is effective in detection of DoS attack and Table attack which needs huge number of access. In our basic method [6], discrete waveforms are made from fluctuation of payloads in each session. Then, each spectrums of session is derived using DFT. By comparing spectrums of sessions with the standard spectrum, which is derived from ordinary sessions, we can distinguish ordinary ones from attack ones. However, when we perform DFT to discrete waveforms directly, noise spectrums will be generated. In order to solve
the problem, we apply window function to discrete waveforms. From our experimental search, we conclude that Hanning window is the most suitable function for our method.

To evaluate effectiveness of our proposal method, we executed detection experiment using data of three days; 2008/1/10, 2008/1/20 and 2008/1/30 in Kyoto2006+ dataset[5]. As the results, false positive rate is 12.0% at most (2008/1/10), and false negative rate is 0.0% (all three days). Comparing with a detection result of another technique of anomaly-based IDS[11], the proposal method is confirmed to be more effective.

![Outline of our proposal method](image)

**Figure 1. Outline of our proposal method**

### 2. FALSE OF IDS

As an index to evaluate performance of IDS, we use false occurrence rate. There are two types of false; false negative and false positive. False negative is wrong detection that attack session is decided as ordinary one. On the other hand, false positive is wrong detection that ordinary session is decided as attack one. In this paper, we calculate the rate of false negative $R_{FN}$ and one of false positive $R_{FP}$ as follows[11].

$$R_{FN} = 1 - \frac{n_{wa}}{n_{a}}, \quad (1)$$

$$R_{FP} = 1 - \frac{n_{fo}}{n_{o}}, \quad (2)$$

where $n_{wa}$ and $n_{a}$ denote the number of correctly detected attack sessions and one of whole attack sessions, and $n_{fo}$ and $n_{o}$ denote the number of falsely detected ordinary sessions and one of the whole ordinary sessions. There are trade-off relation between Eq. (1) and (2). When $R_{FN}$ is low, $R_{FP}$ becomes high. On the other hand, when $R_{FP}$ is low, $R_{FN}$ becomes high. Considering balance of $R_{FN}$ and $R_{FP}$, we improve performance of IDS. For use in critical Communication system, it is obvious that small $R_{FN}$ is more important than small $R_{FP}$. Therefore, in this paper, we give priority to small $R_{FN}$. 
3. PROPOSAL METHOD

3.1. Outline of proposal method

Figure 1 shows outline of our proposal method. It consists of the following procedure.

**Preparation**: Make the standard discrete waveform from the average of payload and time elapsed of ordinary session. Apply window functions to the standard discrete waveforms. Derive the standard spectrum by performing DFT to resultant discrete waveform.

**Step-1**: Make discrete waveform from value of sessions.
**Step-2**: Apply window function to the discrete waveform. Perform DFT to the resultant.
**Step-3**: Compare the spectrum with the standard spectrum.

Note that the details of window function are described in section 3.2, we omit them in this section.

In Preparation, we make the standard spectrum. Its process is the same as the procedure of Step-1 and Step-2. We define the standard session by an average of ordinary sessions, and the standard spectrum is derived from it. Note that ordinary sessions mean the sessions, which are checked as normal from the past log data.

In Step-1, we make discrete waveform by regarding positive values as payload from client and negative value as payload from server. We make discrete waveform \( f(x) \) based on time elapsed in transmission as shown in Figure 1. Let \( \mu \) be the number of session samplings per unit time and \( t \) be session time from start to end \( (0 \leq x \leq t) \). Then, the total number of samples \( N \) is calculated as \( N = \mu \times t \).

In Step-2, we perform DFT to discrete waveform \( f(x) \), and make spectrum as follows.

\[
|F(k)| = \sum_{x=0}^{N-1} f(x) e^{-j2\pi k x / N} \quad (k = 0, 1, \ldots, N - 1), \quad (3)
\]
where $|F(k)|$ is power of the spectrum.

In Step-3, we compare the spectrum derived in Step-2 with the standard spectrum. Figure 2 shows an example of detection. We use visual identification in Figure 2, and focus on status of spectrums between 0 [Hz] and 65 [Hz]. The behavior of standard spectrum and ordinary ones become random in the frequency range. However, attack spectrums have almost constant comparing with the standard spectrum. As a result, we can distinguish ordinary spectrums from attack ones.

### 3.2. Window functions

To determine the most suitable window function, we compare the effectiveness by executing detection experiments applying the candidates of window function. We choose following typical three window functions as candidates; Hanning window, Hamming window and Blackman window [7].

\[
W_{\text{Hann}}(n) = 0.5 - 0.5\cos\left(\frac{2\pi n}{N-1}\right) \quad (4)
\]

\[
W_{\text{Ham}}(n) = 0.54 - 0.46\cos\left(\frac{2\pi n}{N-1}\right) \quad (5)
\]

\[
W_{\text{Bl}}(n) = 0.42 - 0.5\cos\left(\frac{2\pi n}{N-1}\right) + 0.08\cos\left(\frac{4\pi n}{N-1}\right) \quad (6)
\]

The characteristics of each window functions are summarized in Table 1. “Frequency resolution” denotes the characteristic of window function depended on frequency width. When a window function has good frequency resolution, we can distinguish each spectrum clearly. As a result, we can evaluate more detailed spectrums. In general, frequency resolution and noise suppression have trade-off relation as shown in Table 1.

The calculation of DFT applying window function is as follows.

\[
|F(k)| = \sum_{n=0}^{N-1} (f(x) \times W_j(n))e^{-j2\pi kn} \quad (k = 0, 1, \ldots, N-1), \quad (7)
\]

where $W_j(n)$ denotes window functions and symbol “*” denotes element of $\{\text{han, ham, Bl}\}$. In order to choose a window function suitable for our proposal method, we execute detection experiments by applying each window functions (see section 4.5).

<table>
<thead>
<tr>
<th>Table 1. Characteristics of each window function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
</tr>
<tr>
<td>Noise</td>
</tr>
</tbody>
</table>
4. EXPERIMENT

4.1. Kyoto2006+ dataset

In this paper, we execute detection experiment using Kyoto2006+ dataset [5] which is obtained by the honeypot system developed in Kyoto University. It consists of 14 conventional features and 10 additional features (Table 2). We use Source IP address, Destination IP address, Source bytes, Destination bytes, and Label.

<table>
<thead>
<tr>
<th>Duration</th>
<th>IDS detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Malware detection</td>
</tr>
<tr>
<td>Source bytes</td>
<td>Ashula detection</td>
</tr>
<tr>
<td>Destination bytes</td>
<td>Label</td>
</tr>
<tr>
<td>Count</td>
<td>Source IP address</td>
</tr>
<tr>
<td>Same srv rate</td>
<td>Source Port number</td>
</tr>
<tr>
<td>Serror rate</td>
<td>Destination IP address</td>
</tr>
<tr>
<td>Srv serror rate</td>
<td>Destination Port number</td>
</tr>
<tr>
<td>Dst host count</td>
<td>Start time</td>
</tr>
<tr>
<td>Dst host srv count</td>
<td>Duration</td>
</tr>
<tr>
<td>Dst host same src port rate</td>
<td></td>
</tr>
<tr>
<td>Dst host serror rate</td>
<td></td>
</tr>
<tr>
<td>Dst host srv serror rate</td>
<td></td>
</tr>
<tr>
<td>Flag</td>
<td></td>
</tr>
</tbody>
</table>

4.2. Classification of session forms

In order to compare the detection result of Sato [11], we take sessions of 2008/1/10, 2008/1/20 and 2008/1/30 in Kyoto2006+ dataset. These sessions can be categorized according to send-receive relations.

(1) One server One client (O-O)
(2) One server Multi client (O-M)
(3) Multi server One client (M-O)
(4) Multi server Multi client (M-M)

Since M-M is regarded as multiple O-O, we categorize M-M into O-O. These sessions are also categorized depending on payloads as follows.

(1) Fixed payload (F)
(2) Various payloads (V)

According to the information of Label, rates of sessions of per day are summarized as Table 3.
4.3. Procedure of experiment

**Preparation:** We classify ordinary sessions according to classifications shown in section 4.2. We derive each standard spectrum from discrete waveforms of average of ordinary sessions by applying three window functions. As shown in Table 3, there are cases that the number of ordinary sessions is too small to make the standard spectrum. Therefore, we omit M-O-F and M-O-V. Also, we determine that type of F is all attack sessions. Because type of F is against our assumption, which is the behavior of ordinary session is random. Hence, we derive two types of standard spectrum from O-O-V and O-M-V.

**Step-1:** We classify sessions according to section 4.2. Since Kyoto2006+ dataset has no information about time elapsed in each session, we assume that $\mu=20$ and $N=256$. From the condition of $\mu=20$, the network speed is estimated about 1 Gbps. There are 42 sessions whose number of communication is greater than $N=256$ in the target data (17 sessions in 1/10, 10 sessions in 1/20, and 15 sessions in 1/30). We omit these data in the experiment because they can be detected as attack sessions without using any IDS.

**Step-2:** We apply three types of window functions shown in section 3.2 to discrete waveforms in Step-1. We make spectrums by performing DFT in them. Frequency resolution in Step-1 becomes $\Delta f (=\mu/N)=0.078125$ [Hz] regarding $\mu=20$ as sampling frequency. It takes about 0.1 [sec] to make a spectrum per session and we need about an hour to complete all of three days sessions (OS: Windows 7 Professional, CPU: Intel Corei7-3770 3.4GHz, RAM: 16.0GB).

**Step-3:** We pay attention to send-receive relations and compare the standard spectrum. The necessary time for visual identification is about 1.0 [sec]. Since we found many sessions, which can be decided ordinary session or attack one without comparing with the standard spectrum, we execute visual identification again at random chosen 600 sessions in each day. We calculate false occurrence rate using detection error against these 600 sessions.

4.4. Experimental results

Typical detection results applying window functions for O-O-V are shown in Figure 3 ~ Figure 5. And the result for same session using method without window function is shown in Figure 6. Also, typical detection results applying window functions for O-M-V are shown in Figure 7 ~ Figure 9, and the result without window function is shown in Figure 10.

From these results and figures, obviously, we can find that our proposal methods suppress the noise spectrums by the effectiveness of window functions. Therefore, we can conclude
that window functions realize more effective detection in visual identifications. Then, the choice of the most suitable window function is next problem.

Figure 3. O-O-V (Hanning window)

Figure 4. O-O-V (Hamming window)

Figure 5. O-O-V (Blackman window)
Figure 6. O-O-V (No window)

Figure 7. O-M-V (Hanning window)

Figure 8. O-M-V (Hamming window)
4.5. Most suitable window function for IDS

We consider the most suitable window function among three ones shown in section 4.4. From Figure 3 ~ Figure 5 and Figure 7 ~ Figure 9, we cannot see any differences between the standard spectrum and ordinary spectrums among window functions. On the other hand, we can find remarkable differences in the attack spectrums among them. In particular, there are significant differences in O-M-V sessions. In Figure 7 ~ Figure 9, powers of attack spectrums seem to be almost constant. When we compare only attack spectrums among them, we can find there are differences in noise powers (Figure 11). From Figure 11, we can find that spectrums, which do not apply window functions, have larger noise. Also, when we apply a Hamming window, noise is still large. Therefore, we expect that the effective window function is Hanning window or Blackman window. Figure 12 shows the detailed comparison of Hanning window and Blackman window. From this figure, we can see that both of them have same effectiveness in noise suppression. However, the characteristic of peaks is well displayed in Hanning window because of its better frequency resolution (see Table 1). On the other hand, Blackman window makes
characteristic ambiguous because of too effective noise suppression. From these facts and
features, we conclude that Hanning window is the most suitable for IDS using DFT.

![Comparison of three types of window functions against attack session only](image1)

Figure. 11 Comparison of three types of window functions against attack session only

![Comparison of Hanning window and Blackman window](image2)

Figure. 12 Comparison of Hanning window and Blackman window

5. COMPARISON OF PERFORMANCE

We evaluate the performance of our proposal method comparing with Sato method [11]. Sato
method detects abnormal sessions using clustering process against statistical analysis of
procedural changes in data process, protocol manner and so on.

Table 4 shows the detection result of our proposal method. Note that this result is derived using
Hanning window. Table 5 shows the result of Sato method shown in [11]. In comparison of these
tables, $R_{FN}$ of proposal method is obviously lower than Sato method. On the other hand, our
proposal method has larger $R_{FP}$. This fact means that our proposal method may decrease quality
of service. However, from the viewpoint of security in the critical communication system, we can
ignore such value of $R_{FP}$. From these results, we can expect that our proposal method is more
effective than Sato method in the detection of unknown attacks.
Table 4. Detection result of our proposal method

<table>
<thead>
<tr>
<th></th>
<th>2008/1/10</th>
<th>2008/1/20</th>
<th>2008/1/30</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_{FN}$</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>$R_{FP}$</td>
<td>12.0%</td>
<td>10.4%</td>
<td>9.7%</td>
</tr>
</tbody>
</table>

Table 5. Detection result of Sato[11]

<table>
<thead>
<tr>
<th></th>
<th>2008/1/10</th>
<th>2008/1/20</th>
<th>2008/1/30</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_{FN}$</td>
<td>14.4%</td>
<td>16.2%</td>
<td>12.3%</td>
</tr>
<tr>
<td>$R_{FP}$</td>
<td>2.8%</td>
<td>3.6%</td>
<td>4.6%</td>
</tr>
</tbody>
</table>

6. CONCLUSION

In this paper, we propose a new method of IDS using DFT with window function. Our experimental results show Hanning window is the most suitable for the method. The comparison without window function, it is obvious that window function is effective in visual identification. And the comparison with Sato method, our method is expected high detection of unknown attacks. This result satisfies therequirement for critical communication system, which is our goal.

Our method will become more effective by the following improvements.

(i) **Improvement of the standard spectrum by weighted average calculation.**

In particular, we omit type of F session because of too small rate (see Table 3). The standard spectrum will be improved by using the distribution with weight of payload. Then, it can be expected that $R_{FP}$ improved.

(ii) **Derivation of discrete waveform using time elapsed session.**

In this paper, we set the condition of samplingsessions as $\mu = 20$ and $N = 256$ because of no information concerning to them in Kyoto2006+ dataset. Therefore, we omit time elapsed in deriving discrete waveform in our experiments. The appropriate values of $\mu$ and $N$ are depended on circumstance of network system. Development of the method to determine appropriate values for them is our future work.

In this paper and almost method of anomaly-based IDS, detection is made by visual identification. Therefore, successful decision is depended on the acqurement level of staff, and it is the disadvantageous point that there is no objectivity. For anomaly-based IDS, the evolution to the method, which can be decided objectively, is our future work.
REFERENCES


Authors

Yusuke Tsuge is a master course student of National Defense Academy Japan. His research area is cyber-attack detection and network security.

Hidema Tanka is an associate professor of National Defense Academy Japan. His main research area is analysis of cryptographic algorithm, code theory, information security and cyber warfare and its domestic laws.