INTRUSION DETECTION SYSTEM USING DISCRETE FOURIER TRANSFORM WITH WINDOW FUNCTION

Yusuke Tsuge and HidemaTanaka

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

ABSTRACT

An Intrusion Detection System (IDS) is countermeasureagainst network attack. There are mainly two typesof detections; signature-based and anomaly-based. And thereare two kinds of error; false negative and false positive. Indevelopment of IDS, establishment of a method to reduce suchfalse is a major issue. In this paper, we propose a new anomaly-baseddetection method using Discrete Fourier Transform (DFT)with window function. In our method, we assume fluctuation ofpayload in ordinary sessions as random. On the other hand, we cansee fluctuation in attack sessions have bias. From the viewpointof spectrum analysis based on such assumption, we can find outdifferent characteristic in spectrum of attack sessions. Using thecharacteristic, we can detect attack sessions. Example detectionagainst 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 IntrusionDetection 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 signaturesin a database [1][2][4][10][14]. By comparing contents of captured packetswith the signatures, intrusion packets can be detected. Thismethod can detect known attacks that are already analyzed.However, it is difficult to detect unknown attacks such as Zero-dayattacks. So, signature-based IDS has false negative. Inanomaly-based IDS, normal behavior is defined to distinguishabnormal communications [3][9][12]. Therefore, it may be able to detectunknown attacks. However, it is difficult to define “normal behavior”.So, anomaly-based IDS has false positive.

Nowadays, the speed of complication and evolution ofattack technique is fast, so necessity of anomaly-based IDSis 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 basicmethod [6], discrete waveforms are made from fluctuation ofpayloads in each session. Then, each spectrums of sessionis derived using DFT. By comparing spectrums of sessionswith the standard spectrum, which is derived from ordinary sessions,we can distinguish ordinaryones from attack ones. However, when we perform DFT to discretewaveforms directly, noise spectrums will be generated. In order to solve

DOI : 10.5121/ijnsa.2016.8202

the problem,we apply window function todiscrete waveforms. From our experimental search, we conclude that Hanning window is the most suitable function for our method.

To evaluate effectiveness ofour proposal method, we executed detection experimentusing data of three days; 2008/1/10, 2008 /1/20 and 2008/1/30in Kyoto2006+ dataset[5]. As the results, false positive rate is12.0% at most (2008/1/10), and false negative rate is 0.0%(all three days). Comparing withadetection result of another technique of anomaly-based IDS[11],the proposal method is confirmed to be more effective.

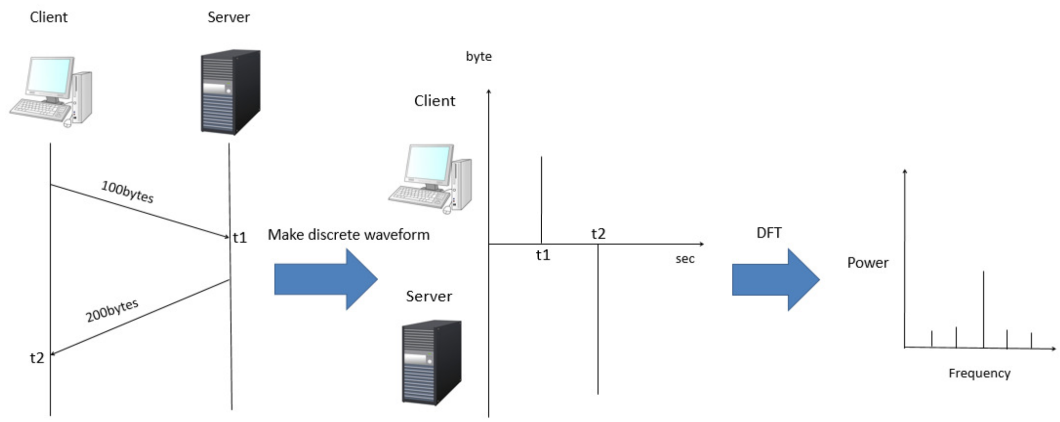

Figure 1. Outline of our proposal method

2. FALSE OF IDS

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

$$R_{FN} = 1 - \frac{n_{ta}}{n_a} \quad , \tag{1}$$

$$R_{FP} = 1 - \frac{n_{fo}}{n_o} \quad , \tag{2}$$

where $n_{ta}$and $n_a$denote the number of correctly detectedattack sessions and one of whole attack sessions, and $n_{fo}$and$n_o$denote the number of falsely detected ordinary sessions andone of the whole ordinary sessions. There are trade-off relationbetween Eq. (1) and (2). WhenR_{FN} is low, R_{FP}becomeshigh. On the other hand, whenR_{FP} is low, R_{FN} becomeshigh. Considering balance ofR_{FN}andR_{FP}, we improveperformance 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 smallR_{FN}.

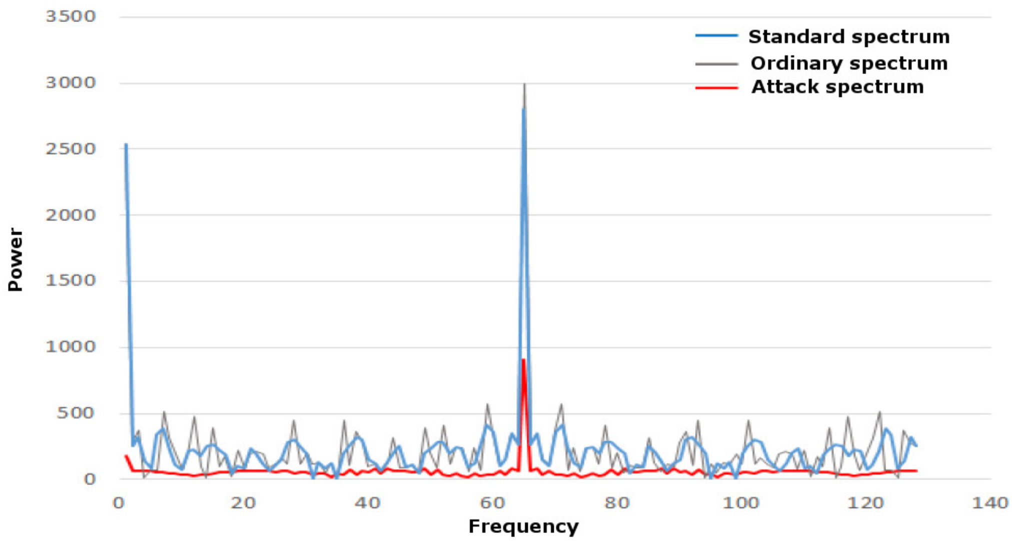

Figure 2. Example of attack detection

3. PROPOSAL METHOD

3.1. Outline of proposal method

Figure1 shows outline of our proposal method. It consists offollowing 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 byperforming DFT to resultant discrete waveform.

Step-1: Make discrete waveform from value of sessions.
Step-2: Apply window function to the discrete waveform. PerformDFT to the resultant.
Step-3: Compare the spectrum with the standard spectrum.
Note that the details of windows function are described in section 3.2, we omit them in this section.

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

In Step-1, we make discrete waveform by regarding positivevalues as payload from client and negative value aspayload from server. We make discrete waveform $f(x)$ basedon time elapsed in transmission as shown in Figure1. Letμbethe number of session samplings per unit time and t be sessiontime from start to end ($0 \leq x \leq t$). Then, the total number ofsamples N is calculated as $N = \mu \times t$.

In Step-2, we perform DFT to discrete waveform $f(x)$, andmake spectrum as follows.

$$|F(k)| = \sum_{x=0}^{N-1} f(x) e^{\frac{-j2\pi kn}{N}} \quad (k = 0,1,..,N-1), \quad (3)$$

where$|F(k)|$is power of the spectrum.

In Step-3, we compare the spectrum derived in Step-2 withthe standard spectrum. Figure2 shows an example of detection.We use visual identification in Figure.2, and focus on statusof spectrums between 0 [Hz] and 65 [Hz].The behavior of standard spectrumand ordinary ones become random in the frequency range.However, attack spectrums have almost constant comparingwith the standard spectrum. As a result, we can distinguish ordinaryspectrums from attack ones.

3.2. Window functions

To determine the most suitable window function, wecompare the effectiveness by executing detection experimentsapplying the candidates of window function. We choose followingtypical three window functions as candidates; Hanningwindow, Hamming window and Blackman window[7].

$$W_{han}(n) = 0.5 - 0.5\cos\frac{(2\pi n)}{(N-1)} \tag{4}$$

$$W_{ham}(n) = 0.54 - 0.46\cos\frac{(2\pi n)}{(N-1)} \tag{5}$$

$$W_{Bl}(n) = 0.42 - 0.5\cos\frac{(2\pi n)}{(N-1)} + 0.08\cos\frac{(4\pi n)}{(N-1)} \tag{6}$$

The characteristics of each window functions are summarized in Table 1. “Frequency resolution” denotes the characteristicof window function depended on frequency width. Whena window function has good frequency resolution, we can distinguish each spectrum clearly. As a result, we can evaluatemore detailed spectrums.In general, frequencyresolution and noise suppression have trade-off relation as shown in Table1.

The calculation of DFT applying window function is asfollows.

$$|F(k)| = \sum_{x=0}^{N-1} (f(x) \times \mathrm{W}_{*}(n)) e^{\frac{-j2\pi kn}{N}} \quad (k = 0,1,\ldots,N-1), \tag{7}$$

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

Table 1.Characteristics ofeachwindow function

	Good< -- >Bad
Frequency	Hamming window >Hanning window>Blackman window
Noise	Blackman window > Hanning window >Hamming window

4. EXPERIMENT

4.1. Kyoto2006+ dataset

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

Table 2.Features inKyoto2006+ dataset

14 conventional features	10 additional features
Duration	IDS detection
Service	Malware detection
Source bytes	Ashula detection
Destination bytes	Label
Count	Source IP address
Same srv rate	Source Port number
Serror rate	Destination IP address
Srv serror rate	Destination Port number
Dst host count	Start time
Dst host srv count	Duration
Dst host same src port rate	
Dst host serror rate	
Dst host srv serror rate	
Flag	

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 accordingto 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-Minto O-O. These sessions are also categorized depending onpayloads as follows.

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

According to the information of Label, rates of sessions of perday are summarized as Table 3.

Table3.Rateofclassified sessionper-day

	2008/1/10		2008/1/20		2008/1/30	
	Ordinary session	Attack session	Ordinary session	Attack session	Ordinary session	Attack session
O-O-F (Number of sessions)	12.0% (1694)	2.8% (398)	7.8% (1375)	8.5% (1492)	9.7% (1492)	2.6% (407)
O-O-V (Number of sessions)	51.6% (7255)	1.9% (266)	33.6% (5898)	8.5% (1496)	44.9% (6917)	2.7% (408)
O-M-F (Number of sessions)	0.0% (0)	0.0% (0)	2.6% (464)	2.8% (491)	0.0% (0)	5.8% (890)
O-M-V (Number of sessions)	29.7% (4177)	0.0% (0)	33.2% (5816)	3.0% (504)	28.8% (4428)	5.5% (852)
M-O-F (Number of sessions)	0.0% (0)	2.0% (278)	0.0% (0)	0.0% (0)	0.0% (0)	0.0% (0)
M-O-V (Number of sessions)	0.0% (0)	0.0% (0)	0.0% (0)	0.0% (0)	0.0% (0)	0.0% (0)

4.3. Procedure of experiment

Preparation: We classify ordinary sessions according to classificationshown in section 4.2. We derive each standard spectrum from discrete waveforms of average of ordinary sessions byapplying three window functions. As shown in Table3,there are cases that the number of ordinary sessions is toosmall to make the standard spectrum. Therefore, we omit M-O-Fand M-O-V. Also, we determine that type of F is all attacksessions. Because type of F is against our assumption, which is the behavior of ordinary session is random. Hence, wederive two types of standard spectrum from O-O-V and O-M-V.

Step-1: We classify sessions according to section4.2. Since Kyoto2006+ dataset has no information about time elapsed in each session, we assume thatμ=20and N=256. From the condition of μ=20, the network speed is estimated about 1[Gbps].There are 42 sessionswhose number of communication is greater than N=256 in the target data(17 sessions in 1/10, 10 sessions in 1/20, and 15sessions in 1/30). We omit these data in the experiment because they can be detected as attack session without using any IDS.

Step-2: We apply three types of window functions shownin section 3.2 to discrete waveforms in Step-1. We makespectrums by performing DFT in them. Frequency resolution in Step-1 becomes Δf (=μ/N)=0.078125 [Hz] regardingμ=20 as sampling frequency. It takes about 0.1 [sec] to make a spectrum pera session and we need about an hour to complete all of threedays 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 identificationis about 1.0 [sec]. Since we found many sessions, whichcanbe decided ordinary session or attack one without comparing with the standard spectrum, we execute visual identification againstrandom chosen 600 sessions in each day. We calculate false occurrencerate 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, typicaldetection results applying window functions for O-M-V areshown 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 thatour proposal methods suppress the noise spectrums by the effectiveness of window functions. Therefore, we can conclude thatwindow functions realize more effective detection in visualidentifications. Then, the choice of the most suitable windowfunction is next problem.

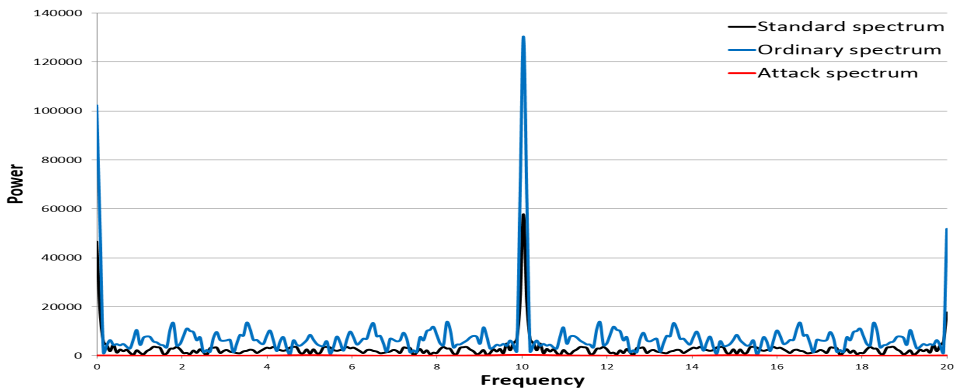

Figure 3. O-O-V（Hanning window）

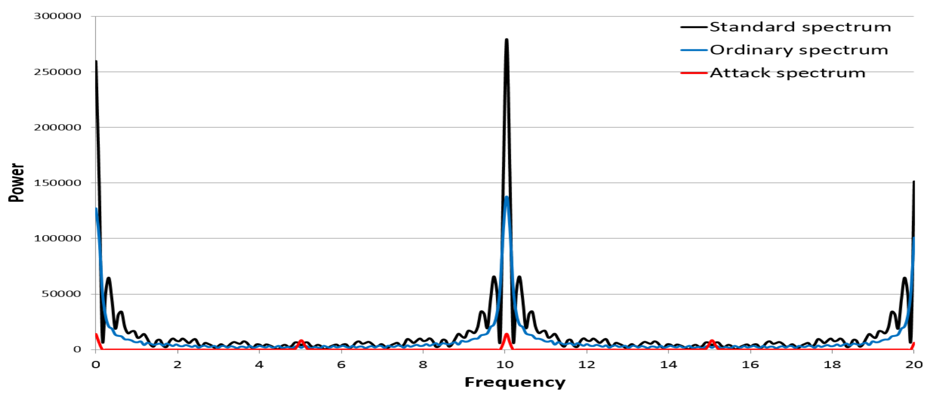

Figure 4. O-O-V（Hamming window）

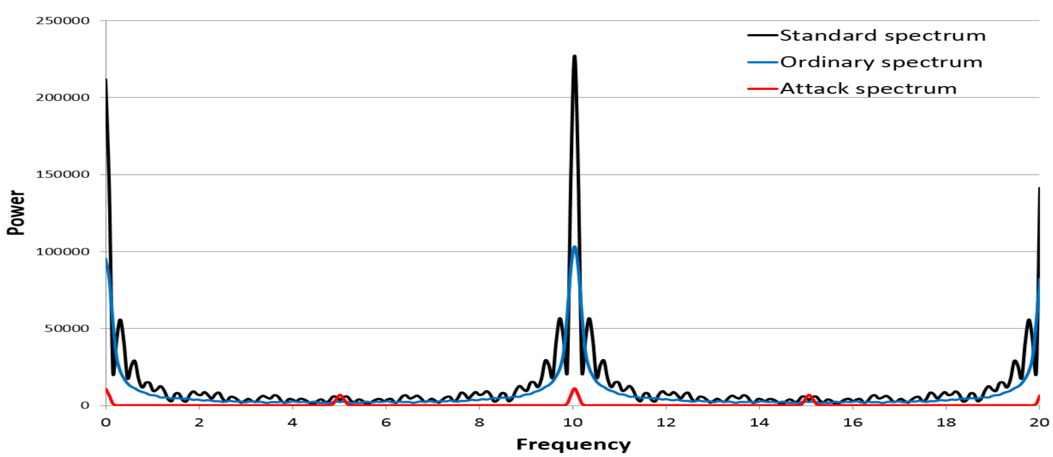

Figure 5. O-O-V（Blackman window）

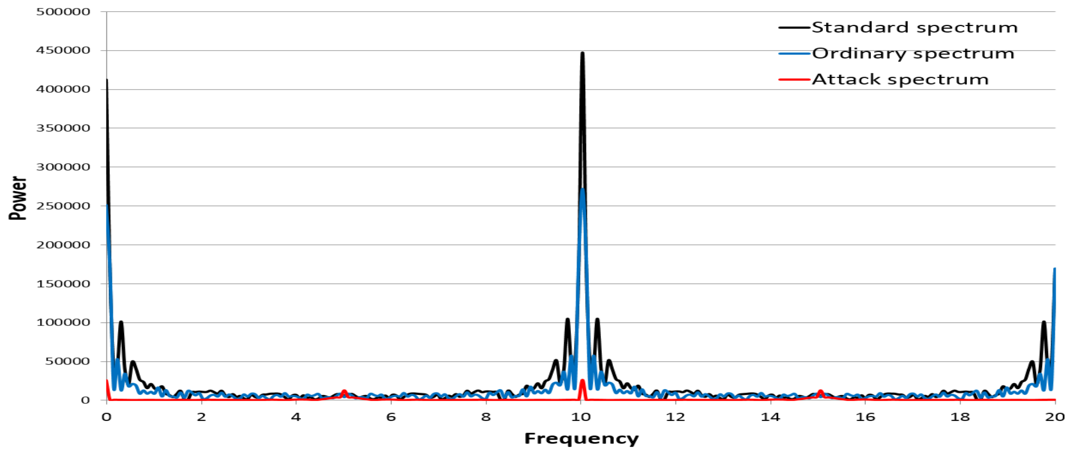

Figure 6. O-O-V（No window）

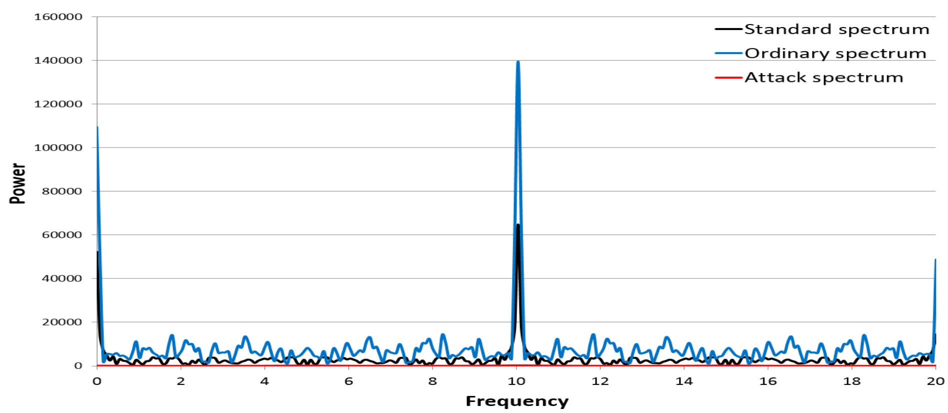

Figure 7. O-M-V（Hanning window）

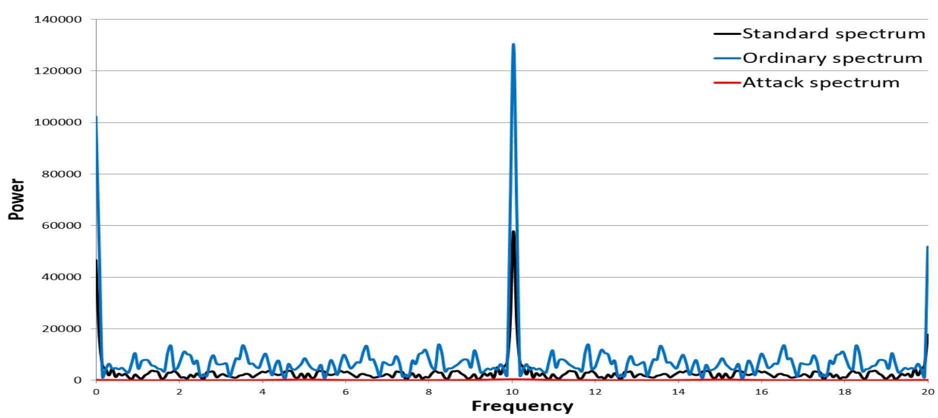

Figure 8. O-M-V（Hamming window）

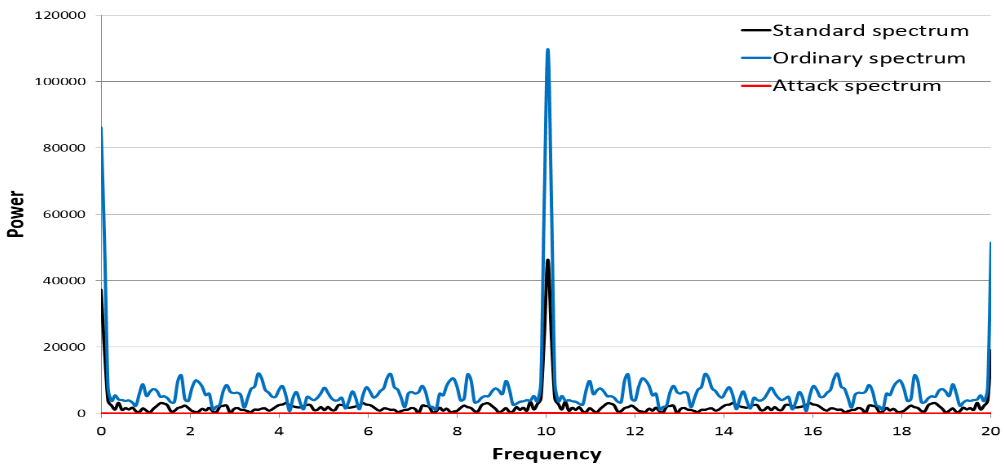

Figure 9.　O-M-V（Blackman window）

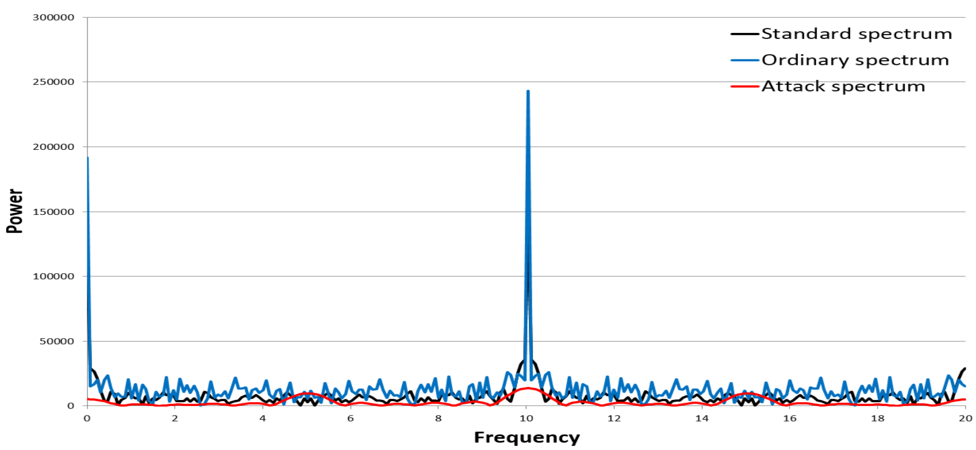

Figure 10.　O-M-V（No window）

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 betweenthe standard spectrumand ordinary spectrums among window functions. On the otherhand, we can find remarkable difference in attack spectrumsamong them. In particular, there are significant differencesin O-M-V sessions. In Figure 7 ～Figure 9, powers of attackspectrums seem to be almost constant. When we compare onlyattack spectrums among them, we can find there aredifferences in noise powers (Figure 11). From Figure 11, we can find thatspectrums, which do not apply window functions, have largenoise. Also, when we apply a Hamming window, noise is stilllarge. Therefore, we expect that the effective window function is Hanning window or Blackman window.Figure 12 shows the detailed comparison of Hanning windowandBlackman window. From this figure, we can see thatboth of them have same effectiveness in noise suppression.However, the characteristic of peaks is well displayed inHanning window because of its better frequency resolution (see Table1). On the other hand, Blackman window makes characteristic ambiguous because of too effective noisesuppression. From these factsand features, we conclude thatHanning window is the most suitable for IDS using DFT.

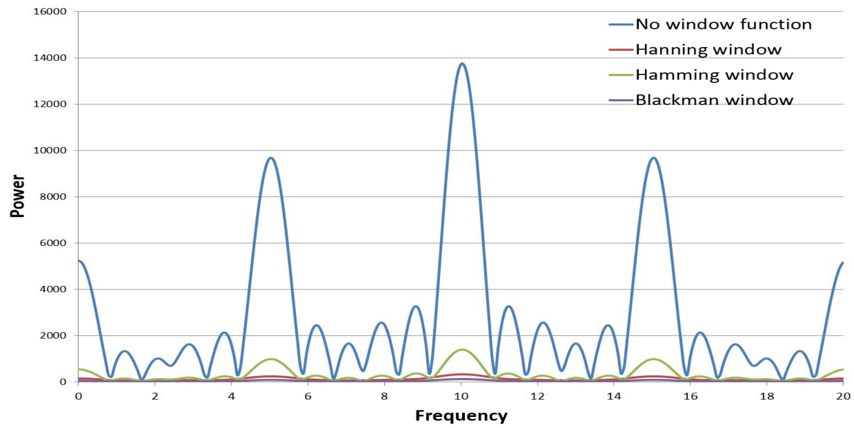

Figure. 11 Comparison of three types of window functions against attack session only

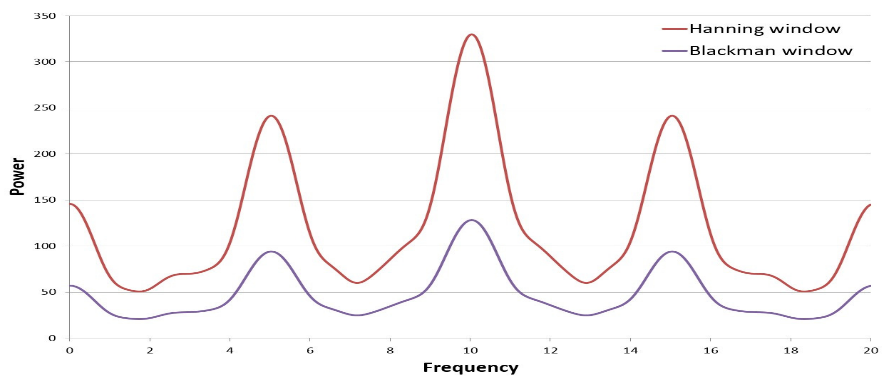

Figure. 12 Comparison of Hanning window and Blackman window

5. COMPARISON OF PERFORMANCE

We evaluate the performance of our proposal methodcomparing with Sato method [11]. Sato method detects abnormal sessions usingclustering process against statistical analysis of proceduralchanges in data process, protocol manner and so on.

Table 4 shows the detection result of our proposalmethod. 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}ofproposal method is obviously lower than Sato method. Onthe other hand, our proposal method has larger R_{FP}. Thisfact means that our proposal method may decrease quality ofservice. However, from the viewpoint of security in the criticalcommunication system, we can ignore such value ofR_{FP}.From these results, we can expect that our proposal method ismore effective than Sato method in the detection of unknownattacks.

Table 4. Detection resultof our proposal method

	2008/1/10	2008/1/20	2008/1/30
R_{FN}	0%	0%	0%
R_{FP}	12.0%	10.4%	9.7%

Table5. Detection result of Sato[11]

	2008/1/10	2008/1/20	2008/1/30
R_{FN}	14.4%	16.2%	12.3%
R_{FP}	2.8%	3.6%	4.6%

6. CONCLUSION

In this paper, we propose a new method of IDS usingDFT with window function. Our experimental results showHanning window is the most suitable for the method. Thecomparison without window function, it is obvious that window function is effective in visual identification. Andthe comparison with Sato method, our method is expectedhigh detection of unknown attacks. This result satisfies therequirement for critical communication system, which is ourgoal.

Our method will become more effective by the followingimprovements.

(i) Improvement of the standard spectrum by weighted averagecalculation.

In particular, we omit type of F session because of too smallrate (see Table3). The standard spectrum will be improved byusing the distribution with weight of payload. Then, it can beexpected that R_{FP} improved.

(ii) Derivation of discrete waveform using time elapsedsession.

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

In this paper and almost method of anomaly-based IDS,detection is made by visual identification. Therefore, successfuldecision is depended on the acquirement level of staff, andit is the disadvantageous point that there is no objectivity. Foranomaly-based IDS, the evolution to the method, which can bedecided objectively, is our future work.

REFERENCES

[1] Mohammad A. Alia, Adnan A. Hnaif, Hayam K. Al-Anie, Khulood Abu Maria, Ahmed M. Manasrah and M. Imran Sarwar,"A novel header matching algorithm for intrusion detectionsystems,"*International Journal of Network Security and Its Applications*,vol.3, No.4, 2011

[2] AlfredV. Aho and Margaret J. Corasick,"Efficient string matching: An aid to bibliographicsearch,"*Communications of the ACM*, vol.18(6), pp.333-340, 1975

[3] Paul Barford, Jeffery Kline, David Plonka and Amos Ron, "A signal analysis of network traffic anomalies," *Proceedings ofInternet Measurement Workshop*, pp.71-82, 2002

[4] Beate Commentz-Walter, "A string matching algorithm fast on the average,"*Proceedings of ICALP*, pp.118-132, 1979

[5] Traffic Data from Kyoto University's Honeypots, http://www.takakura.com/Kyoto_data/ (last access 2016/Mar/20)

[6] Enkhbold Chimedtseren, Keisuke Iwai, Hidema Tanaka and Takakazu Kurokawa, "Intrusion detection system using Discrete Fourier Transform," *Seventh IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA2014), Proceedings of CISDA 2014*, pp.1-5, 2014

[7] FredericJ. Harris, "On the use of windows for harmonic analysis with thediscrete Fourier transform," *Proceedings of the IEEE*, vol. 66, no. 1, pp.51–83, 1978

[8] Sharmila Kishor Wagh, Vinod K. Pachghare and Satish R. Kolhe, "Survey: Learning techniquesfor intrusion detection system", *International Journal of Advance Foundationand Research in Computer*, vol.1,issue 2, pp.21-28, 2014

[9] Seong Soo Kim, A.L.Narasimha Reddy and Marina Vannucci, "Detecting traffic anomaliesthrough aggregate analysis of packet header data,"*Networking 2004,Springer Lecture Notes in Computer Science 3042*, pp.1057-1059, 2004.

[10] Christian Kreibich and Jon Crowcroft, "Honeycomb: Creating intrusion detectionsignatures using honeypots," *ACM SIGCOMM Computer CommunicationReview*, vol.34(1), pp.51-56, 2004.

[11] Masaaki Sato, Hirofumi Yamaki and Hiroaki Takakura, "Unknown attacks detection usingfeature extraction from anomaly-based ids alerts," *Applications andthe Internet (SAINT), 2012 IEEE/IPSJ 12th International Symposium onIEEE*, 2012, pp. 273–277.

[12] Keith Skinner and Alfonso Valdes,"Adaptive model based monitoring for cyber-attack detection," *Recent Advances in Intrusion Detection 2000, Springer Lecture Notes in Computer Science 1907*, pp.80-92, 2000.

[13] Mian Zhou and Sheau Dong Lang, "A frequency-based approach to intrusiondetection,"*Proceedings of the Workshop on Network Security Threats andCountermeasures*, 2003.

[14] Sun Wu and Udi Manber,"A fast algorithm for multi-pattern searching,"*Tech.Rep.TR-94-17*, Dept. of Comp.Science, Univ of Arizona, 1994.

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 ofNational Defense Academy Japan. His main research area is analysis of cryptographic algorithm, code theory, information security and cyber warfare and its domesticlaws.