Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/110202

An Advanced Security Event Visualization Method for Identifying Real Cyber Attacks

Jungsuk Song[1], *Takayuki Itoh*[2], *GilHa Park*[3] *and Hiroki Takakura*[4,*]

[1] Korea Institute of Science and Technology Information, Daejeon, Korea
[2] Ochanomizu University, Tokyo, Japan
[3] Chungnam National University Hospital, Daejeon, Korea
[4] National Institute of Informatics, Tokyo, Japan

Received: 23 Jun. 2016, Revised: 2 Dec. 2016, Accepted: 7 Dec. 2016
Published online: 1 Mar. 2017

Abstract: Most organizations deploy and operate intrusion detection system (IDS) on their networks in order to defend their vital computer and network resources from malicious cyber attackers. Although IDS has been contributed to the improvement of network security, there is a fatal problem in that it records the tremendous amount of alerts, so that security operators are unable to deal with all of them and it is inevitable to miss real cyber attacks from the recorded IDS alerts. Many visualization methods of IDS alerts have been proposed in order to cope with this issue, but their main objective is to better understand only overall attack situations, not to detect real cyber attacks. In this paper, we propose an advanced visualization method of IDS alerts based on machine learning and statistical features derived from IDS alerts. The proposed visualization method can be contributed to the reduction of IDS alerts that must be analyzed by security operators and to effectively identify real cyber attacks from IDS alerts.

Keywords: Visualization, security event, machine learning, statistical features, real cyber attacks

1 Introduction

Most organizations deploy and operate intrusion detection system (IDS) [1] on their networks in order to defend their vital computer and network resources from malicious cyber attackers. Although IDS has been contributed to the improvement of network security, there is a fatal problem in that it records the tremendous amount of alerts, so that security operators are unable to deal with all of them and it is inevitable to miss real cyber attacks from the recorded IDS alerts [2,3].

There are mainly two types of approaches in order to cope with the issue of unmanageable IDS alerts. One is to apply machine learning to IDS alerts [2,3,4,5,6,7,8,9,22,23,24]. This approach is able to analyze IDS alerts automatically and is aiming at identifying unusual IDS alerts or filtering out false positives, i.e., meaningless IDS alerts. This approach can be contributed to the reduction of false positives with an automated manner, but there is a practical shortcoming that it is not easy to intuitively identify real cyber attacks from the results of machine learning: additional analysis task should be carried out by security operators.

The other is to visualize IDS alerts using their basic information, e.g., IP addresses, port numbers, event names and so on [10,11,12,13,14,15,16,17]. The main objective of this type of approaches is to visualize IDS alerts so that security operators are able to analyze them more effectively and intuitively, and to better understand only overall attack situations, but there is a limitation in that it is not able to detect real cyber attacks from the visualization results.

In this paper, therefore, we propose an advanced visualization method of IDS alerts based on machine learning. The proposed method first extracts 7 statistical features from each of the original IDS alerts, which were proposed in our previous work [18]. It then applies one-class SVM [19] into the IDS alerts with 7 statistical features to identify significant (or unusual) IDS alerts automatically. Finally, in order to visualize IDS alerts, we adopt the concept of the hierarchical visualization method presented in our previous work [14]. The main difference is that in the proposed visualization, it finds out all the

* Corresponding author e-mail: takakura@nii.ac.jp

other IDS alerts that have the same source IP address of the significant IDS alerts extracted by machine learning, and visualizes them using not only their 7 statistical features, but also source and destination IP addresses, port numbers and the results of one-class SVM, so that the proposed visualization method can be contributed to the reduction of IDS alerts that must be analyzed by security operators and to effectively identify real cyber attacks from IDS alerts.

We evaluated our visualization method using the security events obtained from threat management systems (TMSs) which are being operated in the Korea Research Open Network (KREONET) [20] and the evaluation results demonstrated the effectiveness and the superiority of the proposed visualization method. Especially, it succeeded in detection of real cyber attacks which were not detected by security operators.

The rest of this paper is organized as follows. In Section 2, we give a brief description for existing visualization approaches of IDS alerts. In Section 3, we describe the proposed visualization method in detail. In Section 4, we provide experimental results. Finally, we present concluding remarks and suggestions for future work in Section 5.

2 Related Work

There are lots of visualization systems based on IDS alerts such as NVisionIP [10], RainStorm [11], IP Matrix [12], VizAlert [13], Hierarchical Visualization [14], SnortView [16], Visual [17], etc. In NVisionIP, it visualizes audit data based on a class-B network to enable analysts to quickly understand the current state of their network and to increase the security analysts situational awareness. In RainStorm, it visualizes alarm data to allow system administrators get a general sense of network activity and detect anomalies. It uses multiple y-axes to represent the location of alarms, i.e., IP addresses, the x-axis shows time information, and color information indicates the severity and the amount of alarms. IP Matrix proposed a visualization method based on 2-dimensional matrix representation of IP addresses. It is able to visualize a large number of IP addresses and logical proximity of IP addresses. Hierarchical Visualization is most similar to the proposed visualization method. It uses the rectangle-packing algorithm to group IDS alerts that have the same source or destination IP addresses. Also, it adopts color and height information to represent the number of IDS alerts and the low-high security incidents predefined, respectively. In this paper, the proposed visualization adopts the basic concept of the rectangle-packing algorithm, but the color and height information is used for indicating the attribute values of 7 statistical features, the results of one-class SVM, port numbers, IP addresses. Also, it visualizes only IDS alerts related to the significant IDS events identified from machine learning technique, i.e., one-class SVM, not all the IDS alerts.

Furthermore, since the traditional visualization systems have focused on visualizing only basic information such as IP addresses, port numbers, event names, transmitted bytes, etc and they are mainly aiming to provide security analyst to better understand the overview of current attack situations, it is not easy to detect real attacks by visualizing IDS alerts.

3 Proposed Method

3.1 Overall Procedure

As shown in figure 1, the proposed visualization method is composed of three main phases: Feature Extraction, Machine Learning and Visualization. In the Feature Extraction phase, 7 statistical features are extracted from each of IDS alerts [18]. In the Machine Learning phase, we use one-class SVM [19] as machine learning technique in order to find out significant or unusual IDS alerts automatically. Finally, in the Visualization phase, all the IDS alerts which have the same source IP address of the significant IDS alerts are visualized based on 7 statistical features.

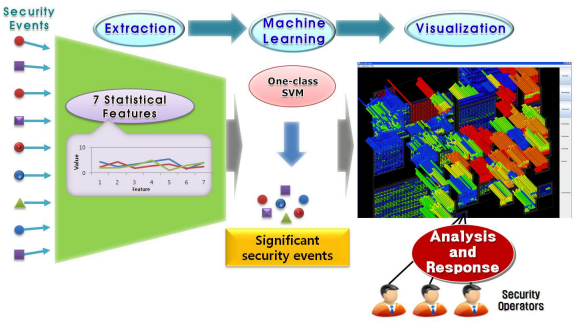

Fig. 1: Overall procedure of the proposed visualization method.

3.2 Feature Extraction

Our visualization method starts with the feature extraction phase and we adopt the 7 statistical features defined in our previous work [18], which are aiming at detecting suspicious IDS alerts to be related with unknown attacks, i.e., 0-day attacks. Table 1 shows the names of 7 statistical features and their description. Similar to our previous work, in this paper, we also extract the same 7 statistical feature from each IDS alert. We then feed IDS alerts with 7 statistical features to machine learning technique, i.e., one-class SVM.

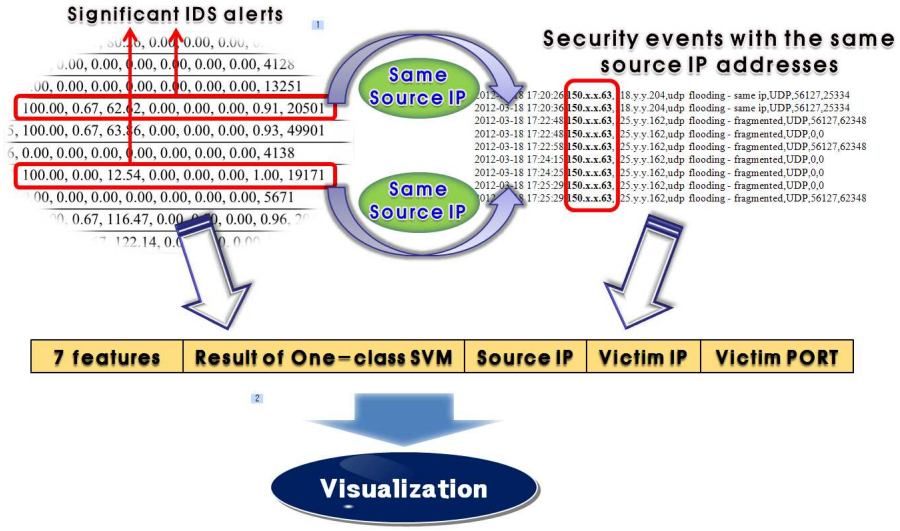

Fig. 2: Overall procedure of applying machine learning.

Table 1: Seven statistical features.

Feature Name	Description
NUM_SAME_SA_DA_DP	Among N alerts, the number of alerts whose destination address is the same to the current alert. We define them as *n* alerts.
RATE_DIFF_ALERT_SAME_SA_DA_DP	Rate of the number of alerts whose alert types are different from the current alert to *n*.
TIME_STDDEV_SAME_SA_DA_DP	Standard deviation of the time intervals . between each instance of *n* alerts . including the current alert.
NUM_SAME_SA_DP_DIFF_DA	Among N alerts, the number of alerts whose destination address is different from from the current alert; it becomes (*N* - *n*).
RATE_DIFF_ALERT_SAME_SA_DP_DIFF_DA	Rate of the number of alerts whose alert types are different from the current alert to (*N* - *n*).
TIME_STDDEV_SAME_SA_DP_DIFF_DA	Standard deviation of the time intervals between each instance of (*N* - *n*) alerts including the current alert.
RATE_REVERSE_SP_SAME_SA_DP	Rate of the number of the alerts whose source port is the same or larger than that of the current alert to *N*.

3.3 Applying Machine Learning

In this phase, we apply one-class SVM to the IDS alerts with 7 statistical features. Figure 2 shows the procedure of applying machine learning to IDS alerts. In this procedure, we first prepare training data which will be used for building a learning model to identify significant IDS alerts. We then feed testing data into the learning model built by the training phases so that we are able to extract the significant IDS alerts from the original IDS alerts. We then find out all the IDS alerts which have the same source IP addresses of the significant IDS alerts. Finally, we visualize them using 7 statistical features, the result of one-class SVM, source IP addresses, victim IP addresses and victim port numbers in the visualization phase.

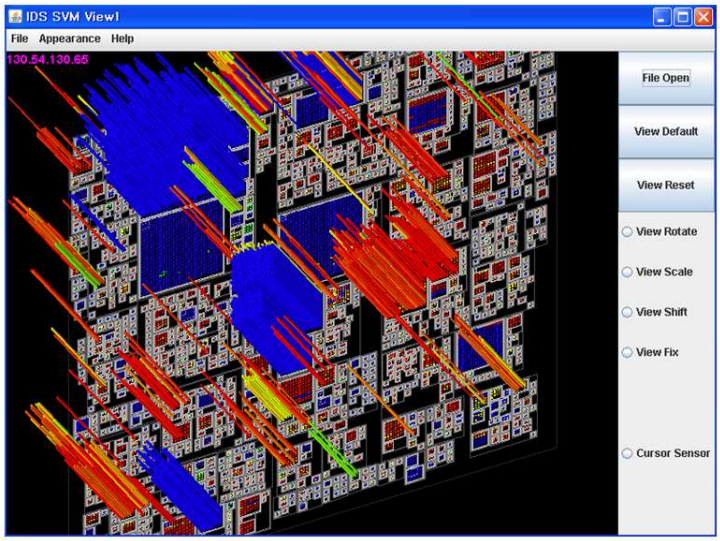

Fig. 3: Execution screen of the proposed visualization method.

3.4 Visualization Method

In this visualization phase, we adopt the hierarchical visualization method presented in our previous work. In the hierarchical visualization method, it groups IDS alerts into rectangles which consist of 4 layers, so that analyst is able to understand how many IDS alerts were caused by the same source and destination IP addresses that belong to the same rectangle. The main differences between the hierarchical visualization method and the proposed visualization method can be summarized as follows.

First, in the hierarchical visualization method, each leaf node represents a certain IP address associated with the corresponding IDS alerts while each IDS alert is depicted as a leaf node in the proposed visualization method. Second, the height of a leaf node is used for indicating the number of IDS alerts caused by a certain IP address and the low-high security incidents were distinguished by using different color information. In the proposed visualization method, however, the height and the color information of a lead node represent the values of 7 statistical features, the result of one-class SVM, source port numbers, and source and destination IP addresses. Figure 3 shows the execution screen of the proposed visualization method. In Figure 3, IDS alerts within each rectangle mean that all of them were caused by the same IP address. Also, the color information of each lead node is changed with respect to the selected items. In addition, the visualization system has user-friendly functions like view rotating, view scaling, view shifting and view fixing which can make analyst easy to use it.

Also, the proposed visualization system can represent IDS alerts from two viewpoints, i.e., source (or attackers) IP and destination (or victims) IP addresses. Figure 4 shows the selection view of either source or destination IP addresses.

Fig. 4: Selection view of source and destination IP addresses.

Figure 5 shows the attribute panel in that we can select what types of the attributes will be visualized in the proposed visualization system. In other words, the height and the color information of leaf nodes represent the values of the selected attributes. If we select RATE_DIFF_ALERT_SAME_SA_DP_DIFF_DA as height and RATE_DIFF_ALERT_SAME_SA_DP_DA as color, for example, the values of two statistical features that IDS alerts have are visualized. Also, in the attribute panel, when we click a certain leaf node, we are able to depict the actual information associated with the leaf node by selecting the name attribute. If we select Source Address as the name attribute, for instance, the actual source IP address that caused IDS alerts as shown in Figure 3.

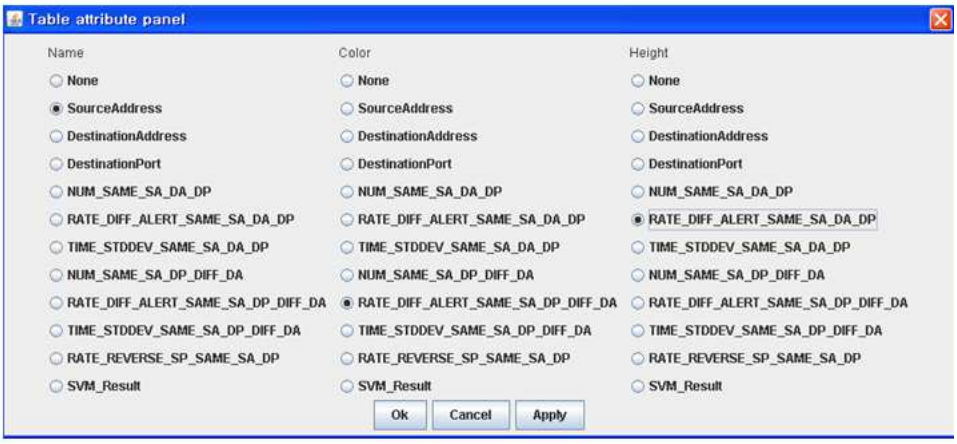

Fig. 5: Attribute panel of the proposed visualization method.

4 Experiment and Evaluation

4.1 Experimental Environment

Figure 6 shows the experimental environment where we collected security events detected by TMSs which are deployed on the boundary networks of 36 Korea national research institutes and their 38 branches that were connected to Korea Research Environment Open Network (KREONET). TMS is operated in the similar manner with IDS and triggers security events when packets contain the predefined intrusion signatures. Science and Technology Security Center (S&T-SEC) is providing security monitoring and response service for the 74 target organizations and all the TMS events are being sent to the collection sever of S&T-SEC. Security operators of S&T-SEC analyze the transmitted TMS events in real-time. For our evaluation, we used two days of TMS events as shown in Table 2.

Table 2: TMS events used for evaluation

Date	# of TMS events
Mar. 18th , 2012	77,959
Mar. 19th , 2012	116,003

This means that the reduction rate of the meaningless TMS events was about 38%.

We then visualized the reduced 48,216 and 71,245 TMS events using the proposed visualization system. Figures 7 and 8 show the results of visualization where we selected RATE_DIFF_ALERT_SAME_SA_DP_DIFF_DA as the height and color attributes. In this visualization, we visualized two days of TMS events in terms of two viewpoints: attack IP based visualization and victim IP based visualization. In case of the first evaluation data (i.e., TMS events on Mar. 18th), we observed that there were three remarkable attack and victim IP addresses, while five outstanding attack IP address and four victim IP addresses were detected from the second evaluation data. Table 3 shows the total 15 IP addresses. We sanitized the IP addresses due to the privacy problem.

Table 3: 15 IP addresses

Mar. 18th, 2012		Mar. 19th , 2012	
Attack IP	Victim IP	Attack IP	Victim IP
150.x.x.132	203.x.x.231	150.x.x.132	150.x.x.192
222.x.x.29	150.x.x.192	58.x.x.52	203.x.x.219
66.x.x.236	150.x.x.154	137.x.x.231	210.x.x.202
		220.x.x.100	210.x.x.37
		124.x.x.56	

4.2 Experimental Results

With respect to the original TMS events, we first extracted 7 statistical features, applied one-class SVM to the training data with them. From the result of the machine learning process, we obtained 48,216 and 71,245 TMS events associated with the significant TMS events.

In our further investigation, we recognized that there were eight attack scenarios of which 6 scenarios were related to real cyber attacks while 2 scenarios were not real cyber attacks, but the corresponding TMS events were caused by unusual communications between two Anti-DDoS security devices. In section 4.2.1 and 4.2.2,

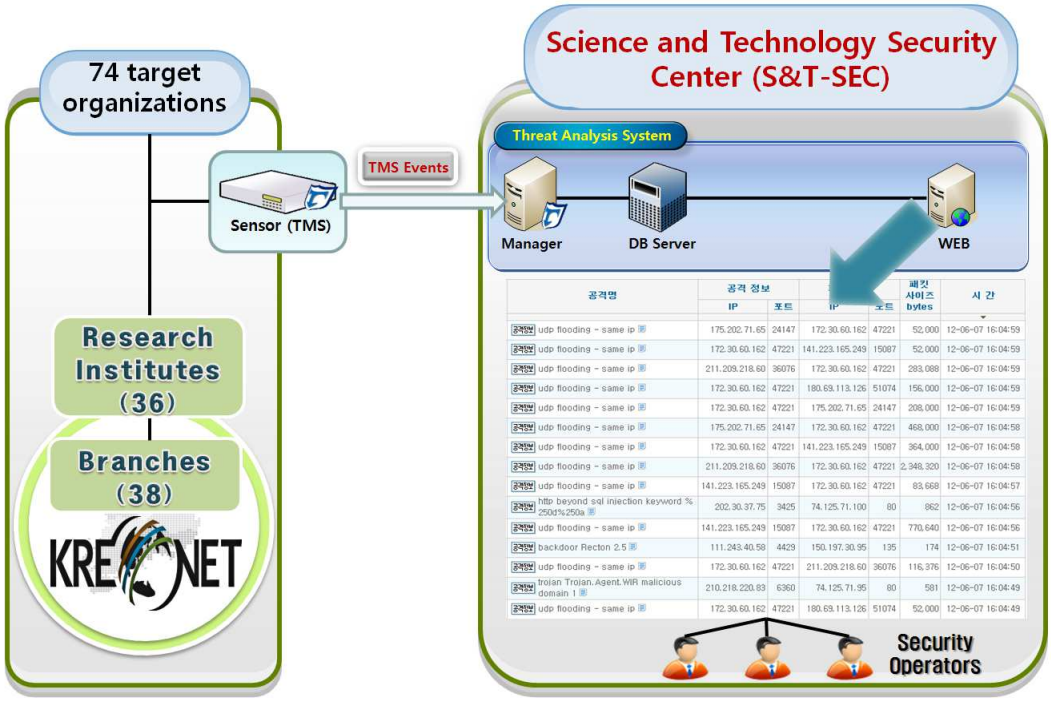

Fig. 6: Experimental environment.

we describe the detailed information of each attack scenario.

4.2.1 Six real cyber attacks

The six real cyber attacks detected by the proposed visualization system can be categorized into two types: one is P2P based attack and the other is RDP remote access attack. The former is corresponding to ②(Figure 7) and ②∼⑤(Figure 8) while the latter is corresponding to ③ in Figure 7. Tables 4 and 5 show the summary information of them.

In our further analysis, we observed that the P2P based attacks were caused by uTorrent P2P program in that the attackers sent their attack codes to the victims using it. TMSs detected attackers activities as the two types of events: udp flooding-fragmented and udp flooding. From Table 4, it can be easily seen that the attacks were caused during a short time interval (i.e., within 3 hours) and the target port number were 45,682, 11,024, 28,877 and 19,212.

In case of the RDP remote access attack, as shown in Table 5, we observed that it caused three different TMS events and the target port number was 3,398 that is used for providing MS remote terminal service. Figure 9 shows the actual attack process of this attack. In this attack, the attacker first tried to login the victim and this activity was detected as RDP login brute force event by the TMS. Also, the attacker tried to connect to his/her C&C server in order to download a new attack command because the TMS detected the attack activity using own DNS_ShinHole signature which triggers TMS events when the attacker connects to predefined malicious domains.

Table 4: Summary information of P2P based attacks

Time	Event Name	Volume	Destination Port
10:42 ∼ 11:21(②, Mar. 18th)	udp flooding -fragmented	16	45,682
	udp flooding	6	
03:36 ∼ 03:53(②, Mar. 19th)	udp flooding -fragmented	4	11,024
	udp flooding	6	
09:24 ∼ 12:03(③, Mar. 19th)	udp flooding -fragmented	31	28,877
	udp flooding	3	
11:16 ∼ 12:23(④, Mar. 19th)	udp flooding -fragmented	49	19,212
	udp flooding	6	
11:24 ∼ 11:52(⑤, Mar. 19th)	udp flooding -fragmented	22	19,212
	udp flooding	1	

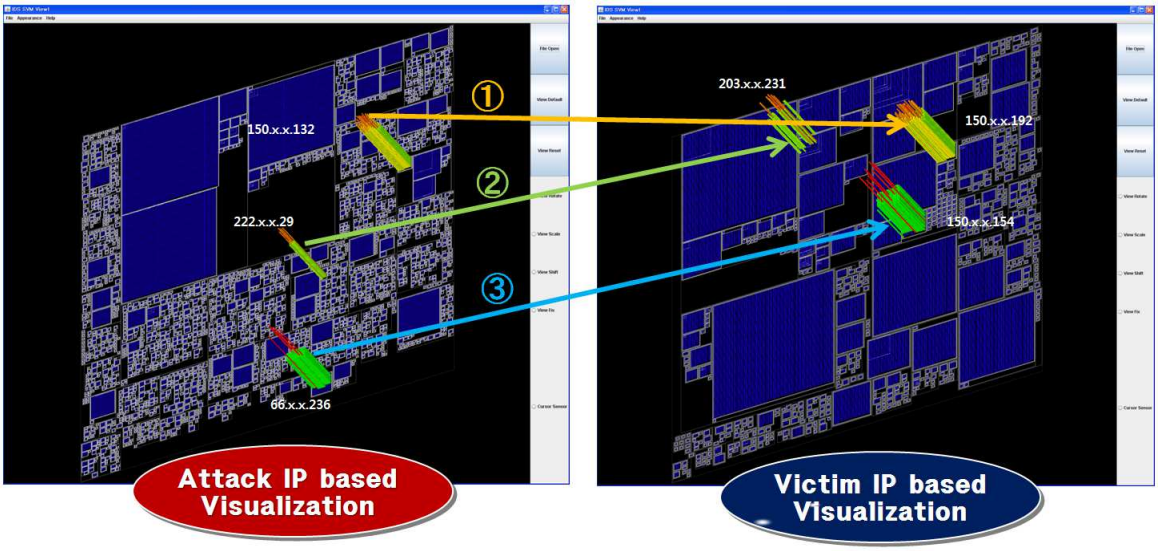

Fig. 7: Visualization results of TMS events on Mar. 18th, 2012.

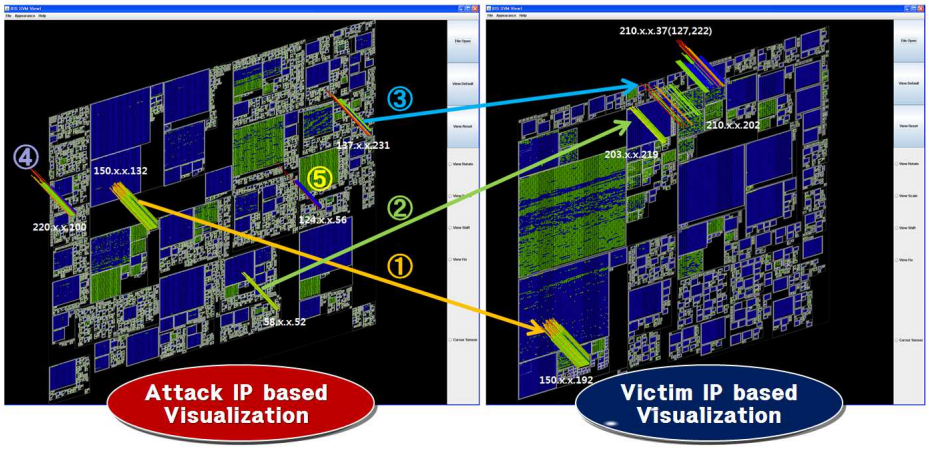

Fig. 8: Visualization results of TMS events on Mar. 19th, 2012.

Table 5: Summary information of RDP remote access attack

Time	Event Name	Volume	Destination Port
14:54 ∼ 20:31(③, Mar. 18th)	rdp login brute force	312	3,389
	[KISTI_100118_01] DNS SinkHole	2	
	tcp syn flooding	8	

4.2.2 Two unusual communicatoins

Table 6 shows the summary information of unusual communications between two Anti-DDoS security devices in that one is deployed in S&T-SEC and the other is deployed in one of the 74 target organizations. Since the communication between Anti-DDoS devices is different from usual communications by the general users, they were detected by the proposed visualization system. Therefore, although they were not real cyber attacks, this result means that the propose visualization system is useful to identify unusual attack activities.

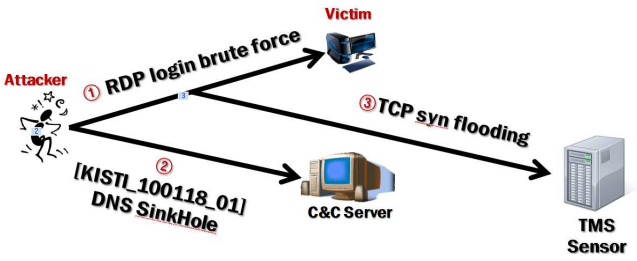

Fig. 9: Attack process of the RDP remote access attack.

Table 6: Summary information of unusual communications

Time	Event Name	Volume	Destination Port
00:06 ∼ 23:45(①, Mar. 18th)	udp flooding -fragmented	89	15,140
	udp flooding same ip	37	
00:01 ∼ 23:35(①, Mar. 19th)	udp flooding -fragmented	83	0
	udp flooding same ip	39	

5 Conclusion

We have proposed an advanced visualization method of IDS alerts based on machine learning. The proposed method consists of three main phases: feature extraction, applying machine learning and visualization. It extracts seven statistical features from each of the original IDS alerts during the feature extraction phase and applies one-class SVM into the IDS alerts with the 7 features in the phase of applying machine learning. The proposed visualization method visualizes all the IDS alerts related to only the significant IDS alerts extracted from the applying machine learning phase. We evaluated our visualization method using the security events obtained from TMSs. The evaluation results demonstrated that the proposed visualization method could detect real cyber attacks (6 real attack scenarios) as well as unusual attack activities (2 unusual communications between two Anti-DDoS security devices) from IDS alerts.

References

[1] D. E. Denning, An intrusion detection model, IEEE Transactions on Software Engineering, **SE-13:222-232**, (1987).
[2] Julisch, K., Clustering Intrusion Detection Alarms to Support Root Cause Analysis, ACM Transactions on Information and System Security **6(4)**, ACM Press, pp. 443-471, (2003).
[3] Manganaris, S., Christensen, M., Zerkle, D. and Hermiz, K., A Data Mining Analysis of RTID Alarms, Computer Networks **34 (4)**, Elsevier North-Holland, Inc, pp. 571-577, (2000).
[4] Yu, D. and Frincke, D., A Novel Framework for Alert Correlation and Understanding, Proc. on ACNS 2004, LNCS **3089**, pp. 452-466, (2004).
[5] Humphrey Waita Njogu, Luo Jiawei, Using Alert Cluster to reduce IDS alerts, ICCIT2010, IEEE, pp. 467-471, (2010).
[6] Fu Xiao, Shi Jin, Xie Li, A Novel Data Mining-Based Method for Alert Reduction and Analysis, Journal of Networks **5(1)**, pp. 88-97, (2010).
[7] A. Alharby, H. Imai, IDS False Alarm Reduction Using Continuous and Discontinuous Patterns, Proceedings of ACNS 2005, LNCS, pp. 192-205, (2005).
[8] Kwok Ho Law and Lam For Kwok, IDS False Alarm Filtering Using KNN Classifier, 5th International Workshop, WISA 2004, LNCS, pp. 114-121, (2004).
[9] Pietraszek, T., Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection, 7th International Symposium RAID 2004, LNCS, pp. 102-124, (2004).
[10] K. Lakkaraju, W. Yurcik, and A. Lee, NVisionIP: Netflow Visualizations of System State for Security Situational Awareness, Proc. of VizSEC 2004, ACM Press, pp.65-72, (2004).
[11] K. Abdullah, C. Lee, G. Conti, J. Copeland, and J. Stasko, IDS RainStorm: Visualizing IDS Alarms, VizSEC2005, pp. 1-10, (2005).
[12] H. Koike, K. Ohno, and K. Koizumi, Visualizing Cyber Attacks Using IP Matrix, VizSEC2005, (2005).
[13] Y. Livnat, J. Agutter, S. Moon, and S. Foresti, Visual Correlation for Situational Awareness, InfoVis2005, (2005).
[14] T. Itoh, H. Takakura, A. Sawada, and K. Koyamada, Hierarchical Visualization of Network Intrusion Detection Data in the IP Address Space, IEEE Computer Graphics and Applications, Vol. **26**, No. **2**, pp. 40-47, (2006).
[15] H. Koike and K. Ohno, Snortview: Visualization System of Snort Logs, VizSEC/DMSEC04, ACM, Washington DC, USA, (2004).
[16] R. Ball, G. Fink, and C. North, Home-centric Visualization of Network Traffic for Security Administration, ACM Conf. on Computer and Commun. Securitys Workshop on Visualization and Data Mining for Computer Security (VizSEC), pp.55-64, (2004).
[17] J. McPherson, K. Ma, P. Krystosek, T. Bartoletti, and M. Christensen, PortVis: A Tool for Port-Based Detection of Security Events, Proc. of VizSEC 2004, ACM Press, pp.73-81, New York, NY, USA, (2004).
[18] J. Song, H. Takakura, and Y. Kwon, A Generalized Feature Extraction Scheme to Detect 0-Day Attacks via IDS Alerts, SAINT2008, IEEE CS Press, pp. 51-56, (2008).
[19] Scholkopf, B., Platt, J., Shawe-Taylor, J., Smola, A., and Williamson, R., Estimating the support of a high-dimensional distribution, Neural Computation, **13(7)**:1443-1471, (2001).
[20] http://www.kreonet.net/en/
[21] H.M. Jung, K.S. Han, G.S. Lee, and S.J. Jang, A role-based access analysis for the cyber security management, The Journal of Future Game Technology, Vol.**2**, Issue **1**, pp.147-152, (2012).
[22] Lina, W.C., Keb, S.W., Tsai, C.F., CANN: An intrusion detection system based on combining cluster centers and nearest neighbors, Knowledge-Based Systems, Vol.78, pp. 13-21, (2015)

[23] Elhaga, S., Fernndezb, A., Bawakidc, A., Alshomranic, S., Herrera, F., On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems, Expert Systems with Applications, Vol.42, No.1, pp. 193202, (2015)

[24] Hu, W., Gao, J., Wang, Y., Wu, O., Maybank, S., Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection, IEEE Transactions on Cybernetics, Vol.44, No.1, pp. 66-82, (2014)

Jungsuk Song received his B.S. and M.S. degrees in Information and Telecommunication Eng. from Korea Aerospace University, Korea in 2003 and 2005, respectively. He received his Ph.D. degree in the Graduate School of Informatics, Kyoto University, Japan in 2009. He is a senior researcher at Korea Institute of Science and Technology Information. His research interests include network security, data mining, machine learning, security issues on IPv6, spam analysis, and cryptography theory.

Takayuki Itoh is a professor of Ochanomizu University. He received B.S., M.S., and Ph.D. degrees from Waseda university in 1990, 1992, and 1997, respectively. He worked for IBM Tokyo Research Laboratory as a researcher during 1992 to 2005, and then moved to Ochanomizu University. His research interest includes information and scientific visualization, computer graphics, multimedia, and user interface.

GilHa Park received his M.S. degrees in Computer Engineering from Hannam University, Korea in 2003 respectively. He received his Ph.D. degree in the Computer and Information Security, Daejeon University, Korea in 2009. He is a team leader at Chungnam National University Hospital, Korea. His research interests include Hospital Information System, u-Hospital System, Information Security.

Hiroki Takakura received his B.S. and M.S. degrees from Kyushu University in 1990, and 1992, and D.Eng degree from Kyoto University in 1995. He was research fellow of Japan Society for Promotion of Science since 1994 to 1995 (visiting scholar at University Illinois at Urbana Champaign), research associate at Nara Institute of Science andTechnology since 1995 to 1997, lecturer at Kyoto University since 1997 to 2000, associate professor at Kyoto University since 2000 to 2009, and professor at Nagoya University since 2010 to 2015. He is a professor at National Institute of Informatics since 2015. His research interests include network security, databases, and geographic information system. He is a member of Information Processing Society, Japan; Geographic Information Systems in Japan; The Institute of Systems, Control and Information Engineers and ACM.