Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/110209

A Fusion Framework of IDS Alerts and Darknet Traffic for Effective Incident Monitoring and Response

Sang-Soo Choi[1], *Seok-Hun Kim*[2] *and Hark-Soo Park*[1,*]

[1] Korea Institute of Science and Technology Information, Daejeon, Korea
[2] Department of Electronic Commerce, Paichai University, Daejeon, Korea

Received: 7 Jun. 2016, Revised: 21 Dec. 2016, Accepted: 23 Dec. 2016
Published online: 1 Mar. 2017

Abstract: Most organizations deploy and operate intrusion detection systems (IDSs) in order to cope with cyber attacks. However, in many cases, it is very difficult to not only analyze IDS alerts in real-time, but also identify real cyber attacks with a high detection accuracy because IDSs record the tremendous amount of alerts and most of them are false positives. Many approaches have been proposed to solve this issue, but there is a limitation in that they have focused on dealing with only IDS alerts. Therefore, in this paper, we propose a fusion framework of IDS alerts and darknet traffic, which is aiming at improving the effectiveness of the incident monitoring and response process. The experimental results show that the proposed framework could detect real cyber attacks that were not detected by IDSs and to identify more dangerous IDS alerts related to real cyber attacks.

Keywords: IDS Alerts, darknet traffic, fusion framework, incident monitoring and response

1 Introduction

With the rapid development of the Internet, cyber threats (e.g., DDoS, computer viruses, Internet worms, Trojan horses) are also increasing constantly and they give fatal damages to our crucial computer systems, networks and services. Most organizations deploy and operate intrusion detection systems (IDSs) [1] in order to cope with cyber attacks. However, in many cases, it is very difficult to not only analyze all of the IDS alerts in real-time, but also identify real cyber attacks with a high detection accuracy because IDSs record the tremendous amount of alerts and most of them are false positives [2,3].

Many approaches have been proposed to solve the issue [4,5,6,7,8,9,10,11,12,25,26,27], but there is a limitation in that they have focused on dealing with only IDS alerts. Since most IDSs adopt misuse detection mechanism and detect intrusions using the predefined signatures, they are unable to detect unknown attacks (i.e., 0-day attacks) that were not defined as signatures. Anomaly detection based machine learning and data mining techniques enables us to detect unknown attacks, but it is not easy to apply the techniques to the real environment because their detection accuracy is very low and it is time-consuming to build anomaly detection models.

On the other hand, many researchers also proposed the reduction methods of IDS alerts that were not related to real cyber attacks or false positives [13,14,15,16,17,18,19,20,21]. However, considering more than 99% of IDS alerts are false positives, it is not easy to filter out all of the meaningless IDS alerts which do not affect any damage to real systems or services. Because of this, many organizations suffer from carrying out incident monitoring and response based on IDSs.

Therefore, in this paper, we propose a fusion framework of IDS alerts and darknet traffic, which is aiming at improving the effectiveness of the incident monitoring and response process. The darknet means a set of unused IP addresses where no real systems are operated with them and thus we are unable to observe any packets on it. In many cases, we can regard the darknet traffic as potential attacks because attackers or infected hosts try to send their attack codes to the victims at random. The main idea of the proposed framework is to compare the IDS alerts with the darknet traffic and regards the darknet traffic that was not detected by IDSs as unknown cyber attacks and the darknet traffic that was detected by IDSs as known cyber attacks.

* Corresponding author e-mail: hspark@kisti.re.kr

We already proposed a similar framework in the previous work [23], we expand the framework and provide more practical experimental results that show the effectiveness and the superiority of the proposed framework. The experimental results show that the proposed framework could detect real cyber attacks that were not detected by IDSs and to identify more dangerous IDS alerts related to real cyber attacks.

The rest of this paper is organized as follows. In Section 2, we give a brief description the existing approaches for analyzing of IDS alerts. In Section 3, we describe the proposed fusion framework in detail. In Section 4, we provide experimental results obtained from Science and Technology Security Center(S&T-SEC). Finally, we present concluding remarks and suggestions for future work in Section 5.

2 Related Work

Many approaches have been proposed to remove meaningless IDS alerts or false positives. T.Bass proposed data fusion techniques in military applications for improving performance of next-generation IDS [19]. Yu, et al. presented a framework for conducting correlation analysis and better understanding using IDS alerts [13] and for contributing to the reduction of false positives, and for providing better understanding of the intrusion progress by introducing confidence scores. Giacinto, et al. proposed a clustering method to group IDS alerts so that it is able to produce unified description of attacks and attain a high-level description of cyber threats [20]. Treinen, et al. adopted meta-alarms to identify known attack patterns in alarm streams, and used a data mining technique, i.e., association rule, to reduce the training time [21]. Song, et al. proposed a clustering method and a generalized feature extraction scheme to detect unknown attacks from IDS alerts [22]. Also, they performed a correlation analysis between raw traffic data captured from honeypots and IDS alerts to reduce the false positives.

Although there are many approaches to effectively reduce and detect real cyber attacks from IDS alerts, they have two main limitations [2,3]. One is that they only focused on dealing with only IDS alerts, not other audit data. This means that the analysis accuracy heavily depends on IDS alerts themselves. The other is that the time complexity for analyzing IDS alerts is very high due to the large amount of IDS alerts. Thus, it is not so easy to apply the existing methods of analyzing IDS alerts into the real environment.

3 Proposed Method

3.1 Overall Architecture

Figure 1 shows the overall architecture of the proposed fusion framework for carrying out effective incident monitoring and response. The proposed fusion framework uses three types of audit data: darknet traffic, IDS alerts and connection information to real systems. It first observes the darknet traffic arriving to the internal and the external darknets from real systems. It then investigates whether the darknet traffic caused any IDS alerts or not. Since the darknet traffic can be regarded as malicious traffic, security operates can use the darknet traffic that was undetected by IDSs as unknown attacks. Also, the darknet traffic that was detected by IDSs can be regarded as known attacks. In addition, the proposed framework checks whether the darknet traffic was observed at the real system or not. For example, if an internal real system sent attack codes to the darknets and they were detected by IDS, they can be regarded as known attacks. Otherwise, they can be regarded as unknown attacks that must be analyzed by security operators.

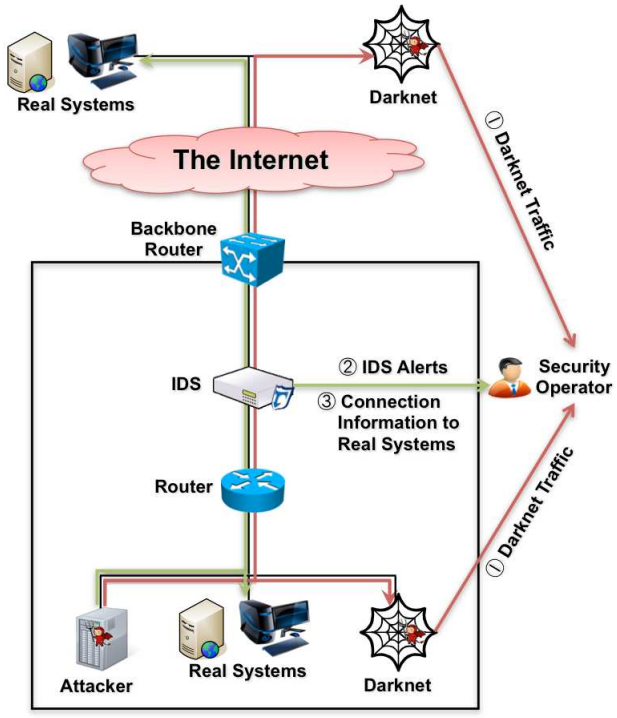


Fig. 1: Overall architecture of the proposed fusion framework.

3.2 Monitoring and Response Process

Figure 2 shows the decision process of the proposed framework to identify known and unknown cyber attacks. The process is as follows.

① It first checks if attackers sent packets to the darknet.

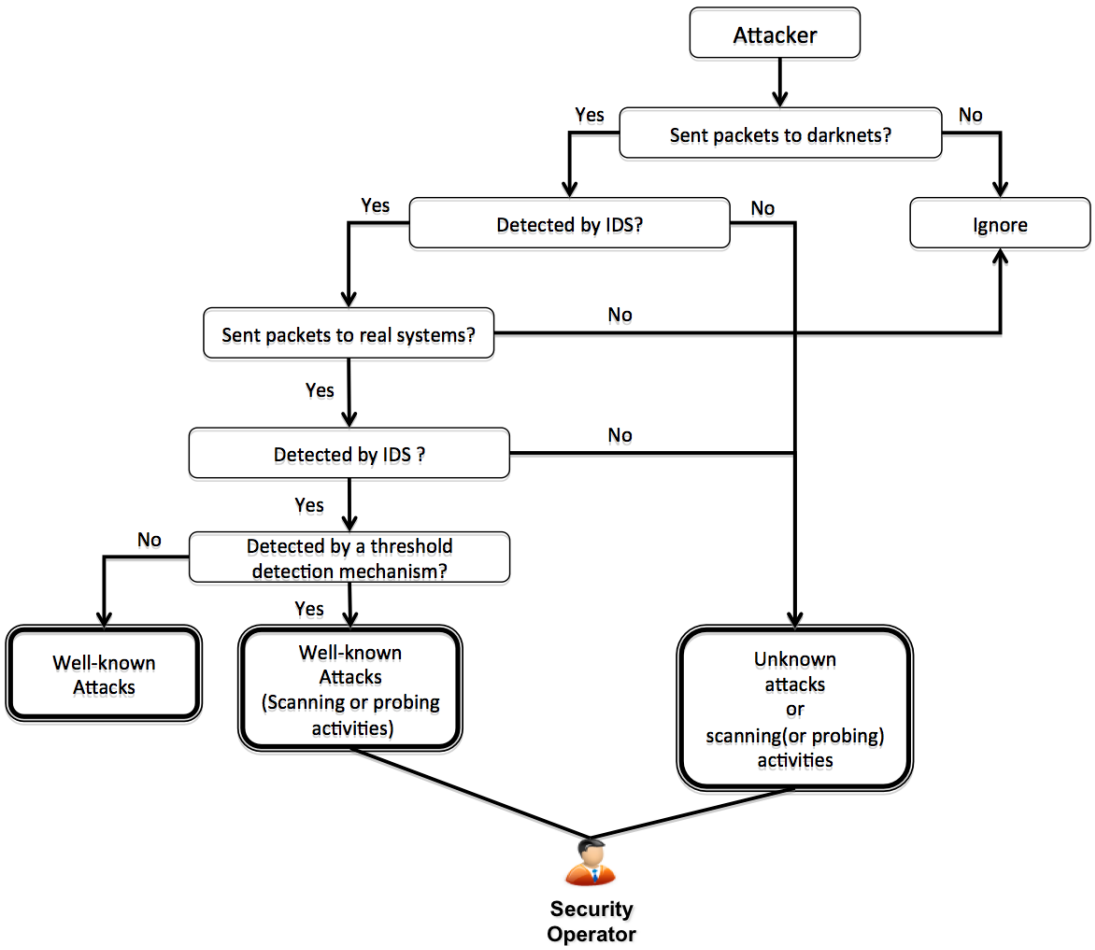


Fig. 2: Decision process of the proposed framework.

② If attackers did not send any packets to the darknet, then we ignore them.
③ It checks whether the incoming darknet packets were detected by IDS or not.
④ If the incoming darknet packets were not detected by IDS, then we regard them as potential cyber attacks such unknown attacks or scanning activities.
⑤ If IDS succeeded in detecting the incoming darknet packets, then we check whether the attackers also sent packets to the real systems or not.
⑥ If the attackers did not send any packets to the real systems, then we ignore them because they do not give any damage to the victims.
⑦ It checks if the outgoing packets to the real systems were detected by IDS or not.
⑧ If they were not detected by IDS, then we regard them as unknown attacks or scanning activities.
⑨ If IDS detected them as attacks, then we regard them as known attacks.
⑩ It checks if the known attacks were detected by a threshold detection mechanism (e.g., if the number of the attack packets that were sent by a certain host exceeds 10 within 1 second, then IDS records an alerts against them) by IDS or not.
⑪ If the known attacks were detected by the threshold detection mechanism, then we regard them as known scanning or probing activities.
⑫ If the known attack were undetected by the threshold detection mechanism, then we regard them as usual known attacks such as remote exploits, viruses, etc.

4 Experiments

4.1 Experimental Environment

Figure 3 shows the experimental environment for evaluating the proposed fusion framework. We prepared eight /24 darknets (i.e., 2,040 IP addresses) space on the Korea Research Open Network (KREONET) [24] where about 200 organizations such as university, research

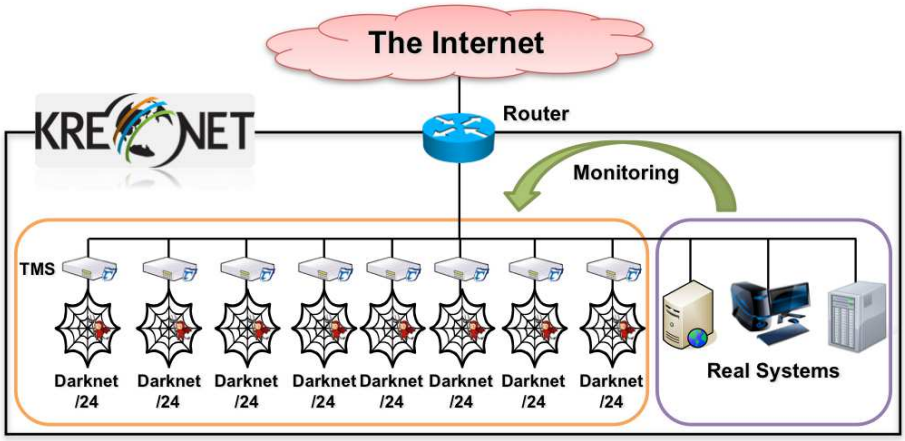


Fig. 3: Experimental environment.

institutes have been connected to it. We collected all the traffic arriving to the eight darknets during one month (Aug. 24th, 2012 ∼ Sep. 24th, 2012). Also, we deployed a dedicated security appliance, i.e., threat management systems (TMSs) into the boundary network of the eight /24 darknet IP addresses. TMS is operated with a similar detection mechanism of the IDSs. All the incoming darknet packets were also inspected by the TMSs based on two detection modes. The first mode is that the TMSs only count the number of the incoming darknet taffic and do not apply any detection rules to them. The second mode is that the TMSs use all the built-in signatures to investigate which darknet packets were detected by TMMs and count the number of them. Furthermore, we also analyzed the darknet traffic based on the decision process described in section 3.2 and divide them into four categories: ignore, unknown attacks or scanning, well-known attacks of scanning activities and well-known attacks.

4.2 Evaluation Results

Table 1 shows summary information of all the incoming darknet packets. We sanitized the IP addresses due to the privacy problem. The total number of the incoming darknet packets was only 30, and in our further analysis all of them were not detected by the TMSs. Thus, we are able to regard them as unknown attacks. From Table 1, it can be easily seen that the incoming darknet packets were observed during only one week (Aug. 24th, 2012 ∼ Aug. 29th, 2012) and we did not observe any packets during the rest of three weeks. Also, we can see that five unique hosts (i.e., 172.x.x.91, 172.x.x.219, 172.x.x.150, 10.x.x.98, 203.x.x.138) sent only 2 or 4 packets to the darknets and they used 11 different source ports (i.e., 389, 3450, 1389, 1624, 4165, 4813, 4295, 4246, 4648, 3959 and 3649). Meanwhile, five attacking hosts sent packets to the 10 different destination darknet IP addresses (i.e., 134.x.x.18, 134.x.x.5, 134.x.x.112, 134.x.x.61, 134.x.x.97, 134.x.x.115, 134.x.x.230, 134.x.x.85, 134.x.x.99, 134.x.x.1103) and only two different destination ports, i.e., 445 and 8085. From these results, we can conclude the followings.

① The five attacking hosts were infected by two types of malwares because they sent attack packets to only two different destination ports.
② Since the darknet packets were only observed during one week, there is a high possibility that the two malwares were carefully controlled by the attackers or the five attacking hosts infected by the two malwares have been recovered by the owners or the administrators after the one week.
③ The five attacking hosts sent only 2 or 4 attack packets to only the specified 10 IP addresses and two destination ports, not the overall (or many) IP addresses on a certain network or the overall (or many) ports on a certain host. This means that the 30 darknet packets that were undetected by TMSs contain a well crafted exploit codes or shell codes to attack the target hosts. Because, in case of the scanning and probing activities, they tend to send packets in a sequence (or at random) against the entire hosts on the specified network or the entire ports on the specified host.

We also investigated whether the TMSs triggered alerts associated with the five attacking hosts or not. In the further investigation, we observed that among the five attacking hosts, only one attacking host (i.e., 172.x.x.219) was detected by the TMSs. Table 2 shows the summary information the TMS alert. This alert was detected in Sep. 11th, 2012 and its destination IP address and port number were 134.x.x.104 and 445, respectively. Also, the name of

Table 1: Summary information of the darknet traffic.

Time	Source IP:PORT	Destination IP:PORT	Count
2012-08-24	172.x.x.91:389	134.x.x.18:445	4
2012-08-24	172.x.x.219:3450	134.x.x.5:445	4
2012-08-25	172.x.x.219:1389	134.x.x.112:445	2
2012-08-26	172.x.x.150:1624	134.x.x.61:445	2
2012-08-27	10.x.x.98:4165	134.x.x.97:445	2
2012-08-28	203.x.x.138:4813	134.x.x.115:8085	2
2012-08-28	203.x.x.138:4295	134.x.x.230:8085	2
2012-08-28	203.x.x.138:4246	134.x.x.85:8085	2
2012-08-28	203.x.x.138:4648	134.x.x.99:8085	4
2012-08-29	203.x.x.138:3959	134.x.x.103:8085	4
2012-08-29	172.x.x.219:3649	134.x.x.103:445	2

Table 2: Summary information of the TMS alerts

Time	2012-09-11
Source IP	172.x.x.219
Source Port	4814
Destination IP	134.x.x.104
Destination Port	445
Event Name	tcp syn flooding
Number of packets	200

the TMS alert was “tcp syn flooding” and the number of the corresponding packets was 200. In this alert, we need to give an attention for the name of the TMS event; this means that the attacking host was used for DDoS attack. From these results, we can conclude that the attacking host was recovered after its first infection, but it has been compromised by some malwares again, and consequently it sent many packets for DDoS attack.

5 Conclusion

In this paper, we have proposed a fusion framework of IDS alerts and darknet traffic for carrying out the effective incident monitoring and response. The main idea of the proposed framework is to compare the IDS alerts with the darknet traffic and regards the darknet traffic that was not detected by IDSs as unknown cyber attacks and the darknet traffic that was detected by IDSs as known cyber attacks. The main contribution of the proposed framework is to expand our previous work proposed in [23], focusing on constructing the decision process more clearly and providing more practical experimental results that show its effectiveness and superiority.

We have evaluated the proposed framework using 8 /24 darknet IP addresses and TMS alerts that were obtained from TMSs deployed on the KREONET. The experimental results showed that the five attacking host sent 30 packets to the darknets and their activities were related to unknown attacks. In addition, we concluded that the darknet packets contain well crafted exploit codes or shell codes to attack the specified 10 victims. We also observed that one attacking host has been compromised by some malware again and it was used for carrying out DDoS attack.

In our future work, we need to evaluate the proposed framework with more large scale darknets. Also, we have a plan to collaborate with other research institutes which have many darknet IP addresses to provide more practical experimental results.

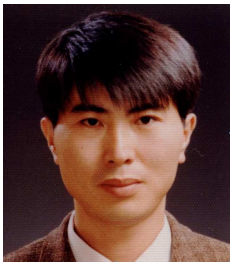
References

[1] D. E. Denning, An intrusion detection model, IEEE Transactions on Software Engineering, 1987, **SE-13:222-232**, (1987).
[2] K. Julisch, 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] S.S. Choi, S.H. Kim and H.S. Park, An Advanced Security Monitoring and Response Framework Using Darknet Traffic, 2012 International Workshop on INFORMATION & SECURITY, pp. 9-10, (2012).
[5] L. Portnoy, E. Eskin and S. Stolfo, Intrusion Detection with Unlabeled Data Using Clustering, In Proceedings of ACM CSS Workshop on Data Mining Applied to Security, (2001).
[6] E. Eskin, A. Arnold, M. Prerau, L. Portnoy and S. Stolfo, A Geometric Framework for Unsupervised Anomaly Detection : Intrusion Detection in Unlabeled Data, In Applications of Data Mining in Computer Security, (2002).
[7] Y. Guan, A. Ghorbani and N. Belacel, Y-means : A Clustering Method for Intrusion Detection, In IEEE Canadian Conference on Electrical and Computer Engineering, Proceedings, (2003).
[8] K.L. Li, H.K. Huang, S.F. Tian, and W. Xu, Improving one-class SVM for anomaly detection, International Conference on Machine Learning and Cybernetics, Vol. **5**, pp. 3077-3081, (2003).

[9] K. Leung, and C. Leckie, Unsupervised Anomaly Detection in Network Intrusion Detection Using Clusters, ACSC2005, (2005).
[10] J. Song, K. Ohira, H. Takakura, Y. Okabe and Y. Kwon, A Clustering Method for Improving Performance of Anomaly-based Intrusion Detection System, IEICE Transactions on Information and Communication System Security, Vol.**E91-D**, No.**5**, pp.1282-1291, (2008).
[11] Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A., Srivastava, J., A comparative study of anomaly detection schemes in network intrusion detection, In Proceedings of the Third SIAM International Conference on Data Mining, (2003).
[12] Reza Sadoddin and Ali A. Ghorbani, A Comparative Study of Unsupervised Machine Learning and Data Mining techniques for Intrusion Detection, MLDM 2007, LNAI **4571**, pp. 404–418, (2007).
[13] Yu, D. and Frincke, D., A Novel Framework for Alert Correlation and Understanding, Proc. on ACNS 2004, LNCS **3089**, pp. 452-466, (2004).
[14] Humphrey Waita Njogu, Luo Jiawei, Using Alert Cluster to reduce IDS alerts, ICCIT2010, IEEE, pp. 467-471, (2010).
[15] 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).
[16] A. Alharby, H. Imai, IDS False Alarm Reduction Using Continuous and Discontinuous Patterns, Proceedings of ACNS 2005, LNCS, pp. 192-205, (2005).
[17] Kwok Ho Law and Lam For Kwok, IDS False Alarm Filtering Using KNN Classifier, 5th International Workshop, WISA 2004, LNCS, pp. 114-121, (2004).
[18] Pietraszek, T., Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection, 7th International Symposium RAID 2004, LNCS, pp. 102-124, (2004).
[19] T. Bass, Intrusion detection systems and multisensor data fusion, Communications of the ACM, ACM Press, pp. 99-105, New York, NY, USA, (2000).
[20] G. Giacinto, R. Perdisci and F. Roli,Alarm Clustering for Intrusion Detection Systems in Computer Networks, MLDM 2005, LNAI **3587**, pp. 184-193, (2005).
[21] J.J. Treinen, R. Thurimella, A Framework for the Application of Association Rule Mining in Large Intrusion Detection Infrastructures, RAID 2006, LNCS **4219**, pp. 1-18, (2006).
[22] J. Song, H. Takakura, and Y. Kwon, A Generalized Feature Extraction Scheme to Detect 0-Day Attacks via IDS Alerts, The 2008 International Symposium on Applications and the Internet(SAINT2008), The IEEE CS Press, pp. 51-56, (2008).
[23] S.S. Choi, J.S. Song, H.S. Park, and J.K. Choi, An Advanced Incident Response Framework Based on Suspicious Traffic, The Journal of Future Game Technology, Vol.**2**, Issue **2**, pp.171-176, (2012).
[24] http://www.kreonet.net/en/
[25] 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)
[26] 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)
[27] 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)

Sang-Soo Choi received the B.S., M.S. and Ph.D. degrees in Computer Science from Hannam University, Daejeon, Korea, in 2001, 2003 and 2006, respectively. He is a senior engineer at Korea Institutes of Science and Technology Information, Korea. His research interests include information security and design of incident response process model.

Seok-Hun Kim is an assistant professor in the Electronic Commerce at Paichai University. He received the M.S and Ph.D. degree in Computer Engineering from Hannam University in 2003 and 2006, respectively. His teaching and research specialties are in the fields Mobile computing, Web-App programming, information security.



Hark-Soo Park received the B.S., M.S. and Ph.D. degrees in Computer Science from Hannam University, Daejeon, Korea, in 1989, 1991 and 2003, respectively. He is a general manager at Korea Institutes of Science and Technology Information, Korea. His research interests include network security and incident monitoring and response.