DOI: 10.4218/etr2.12236

GUEST EDITORIAL

ETRI Journal WILEY

Special Issue on Cyber Security and AI

We are facing a big data world, embedded with interconnected IoT (Internet of Things) devices that generate large volumes of data. They pose a significant challenge to academia and industries focused on digital security: A variety of new malware and other threats are emerging at a fast pace, and existing preventive methods are struggling to deal with them within the golden time by depending solely on the known attack signature. Recently, there has been considerable advancement in computing, particularly in the field of Artificial Intelligence (AI). Advanced technologies such as Machine Learning and Deep Learning are being actively deployed in cyber security, and new results and issues have been reported.

In this special issue, we have selected five publications that represent the state-of-the-art research in AI-based cyber security ranging from theory to practice.

The first paper, entitled "Supervised learning-based DDoS attacks detection: Tuning hyperparameters" by Meejoung Kim investigates and analyzes Distributed Denial-of-Service (DDoS) attacks using Machine Learning-based approaches. She employs two different supervised Machine Learning-based Algorithms, namely Basic Neural Network and LSTM RNN.

Her study focuses on four aspects - 1) how various data preprocessing methods and values of hyperparameters can affect the performance of Machine Learning-based techniques, 2) which suboptimal values of hyperparameters enable feature extraction algorithms to work efficiently, 3) whether learning from the former traffic and a particular dataset can affect the sequential traffic and another dataset, respectively, especially in case of DDoS attacks, and 4) whether Machine Learning algorithms crafted for older attacks can be reused to detect recent attacks.

Her experiments incorporate three scenarios: 1) using mixed CAIDA and DARPA datasets, 2) using CAIDA dataset for training and DARPA dataset for testing and 3) using the more recent dataset for both training and testing. Besides this, she also considers different environments with different hyperparameter values, including but not limited to optimizers, learning rates, number of layers, hidden nodes, number of epochs, etc.

The key contributions of her study are: 1) an investigation of the joint effects of hyperparameters and preprocessing methods on the performance of Machine Learning-based techniques, 2) investigation of the effects of learning, previously conducted using former traffic and a particular dataset, on sequential traffic and a different dataset, 3) appraisal of the applicability of a Machine Learning-based algorithm, trained on old features, in the detection of DDoS attacks with new features, and 4) comparison of two optimizers, namely Gradient Descent and Adam, used in the Machine Learning-based models to detect DDoS attacks.

The next paper by Ili Ko, Desmond Chambers and Enda Barrett, entitled "Unsupervised learning with hierarchical feature selection for DDoS mitigation within the ISP domain" presents a DDoS attack mitigation framework.

Their proposed framework is an improved version of the previous system they had designed. The newly proposed framework comprises four improvements - 1) it has an extended horizontal expansion process for global feature extraction to enhance the separability of data, 2) it incorporates two logical controllers to avoid incorrect map generation by the system, 3) it consists of one additional layer of SOM, and 4) it is equipped with an additional model to select appropriate sets of features for each layer of SOM.

Further, they have also underlined some of the challenges that they faced while conducting their research. These include 1) reducing the size of the dataset without losing relevant information, 2) extraction of significant features without consuming too many resources, and 3) difficulty in evaluating the performance of the newly proposed framework on unlabeled datasets.

They have made three main contributions to the field via this research. First, they leveraged the data collected by an ISP, thereby enhancing data separability to improve the performance of the system. Second, they have proposed a two-layered SOM DDoS attack mitigation model deployed at an ISP domain. This model is capable of recognizing normal traffic and mitigating DDoS attacks more efficiently compared to their previously presented model. Third, their approach is not only capable of identifying 99% of the malicious traffic but also enables ISPs to resist

malicious traffic, thereby resulting in minimal consumption of resources.

In the third paper being considered, entitled "Honeypot game-theoretical model for defending against APT attacks with limited resources in cyber-physical systems" by Wen Tian et al., the authors propose a model to defend from APT attacks on CPSs. Due to limited resources and the honeypot classification, their model is not capable of tackling real attacks. Therefore, their study is aimed toward studying the various offensive and defensive interactions, and the processes of the CPSs. Their proposed model is a Honeypot Game Theoretical model which consists of two modes—low interaction mode and high interaction mode.

Through this study, the authors have proved that there exist several Bayesian-Nash equilibria for the different scenarios. They have also obtained an optimal defensive strategy. Furthermore, they have optimized the capture effect by appropriately allocating and distributing deployment resources and human analysis costs between low and high interaction modes.

The results of their numerical simulations show that their proposed model and approach can provide an effective and optimal defence with limited resources.

Two main contributions to the field have been made in this study. First, a model based on honeypots has been proposed to combat APT attacks on CPSs. In addition, the honeypots have been classified into two categories—low and high interaction modes, to improve the accuracy of the interaction process. Second, optimized allocation costs and human analysis costs in the honeypots have also been introduced.

The fourth paper, entitled "Concealment of iris features based on artificial noises" by Jiao Wenming et al., introduces privacy protection mechanisms based on Iris features. The authors adopt differential privacy to secure the Iris features, generally used in Biometric Verification Processes.

Their study employs two differential privacy methods: the Gaussian method and the Laplacian method. Via these methods, they are able to add an ample amount of random noise to the iris images, thereby making it difficult for an attacker to figure out the precise amount of noise present in the iris images. Their approach of hiding the iris features using differential privacy not only reduces privacy leakage but also outperforms other existing techniques. Their results show that the Gaussian mechanism performed slightly better than the Laplacian mechanism under the same noise parameters.

Further, they present a hash algorithm to evaluate the performances of their differential privacy protection mechanisms. It compares the iris images which were protected by the Gaussian noise and the Laplacian noise using differential privacy.

In the last paper entitled "Keyed learning: an adversarial learning framework – formalization, challenges, and anomaly detection applications", Francesco Bergadano has formalized and defined a more generalized notion of keyed learning, which is a type of Machine Learning where a secret key is used as an additional input to the learning systems. The proposed secret key can be used to manipulate learning algorithms and processes. The main purpose of proposing a secret key is to prevent an adversary from simulating the learning phase. The framework developed can affect any form of learning and use any kind of secret information. The author has followed Kirchhoff's principle and concentrated only on the precise and generalized methods of hiding information, needed during the learning process, in a secret key.

The same notation has been used to describe three alternative adversarial challenges and models, including 1) Passive Observer, 2) Active Data Selector, and 3) Active Data Modifier. The author has also defined possible adversary goals like Misclassification Mining, Classifier Disclosure, and Key Recovery. The framework developed has been applied to the more specific context of anomaly detection.

Further, the author has highlighted a variety of applications for his framework, namely network intrusion detection, continuous user authentication, and defacement response. Additional practical and experimental uses of this framework include integration with SIEM software and security monitoring systems to generate alarms.

ACKNOWLEDGMENTS

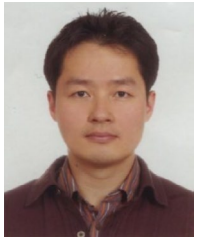
The Guest Editors thank all the authors, reviewers, and the editorial staff members of the *ETRI Journal* for making this special issue a success. We are most pleased to have been part of this effort and to have been able to ensure the timely publication of these high-quality technical articles.

Seong Oun Hwang[1]
Taekyoung Kwon[2]
Wei-Chuen Yau[3]
DaeHun Nyang[4]
[1]*Department of Software and Communications Engineering, Hongik University, Sejong, Rep. of Korea*
[2]*Graduate School of Information, Yonsei University, Seoul, Rep. of Korea*
[3]*School of Electrical and Computer Engineering, Xiamen University Malaysia, Sepang, Malaysia*
[4]*Department of Computer Engineering, Inha University, Incheon, Rep. of Korea*

Correspondence
Seong Oun Hwang,
Department of Software and Communications Engineering,
Hongik University, Sejong, Rep. of Korea
Email: sohwang@hongik.ac.kr

AUTHOR BIOGRAPHIES

Seong Oun Hwang received his BS degree in Mathematics in 1993 from Seoul National University, his MS degree in Computer and Communications Engineering in 1998 from Pohang University of Science and Technology (POSTECH), and his PhD degree in Computer Science from Korea Advanced Institute of Science and Technology (KAIST). He worked as a software engineer at LG-CNS Systems, Inc. from 1994 to 1996. He worked as a senior researcher at Electronics and Telecommunications Research Institute (ETRI) from 1998 to 2007. Since 2008, he has been working as a professor with the Department of Software and Communications Engineering of Hongik University, Rep. of Korea. He is a Senior Member of the IEEE and an editor of ETRI Journal. He is an executive director of the Institute of Electronics and Information Engineers (IEIE), Rep. of Korea. His research interests include cryptography, cyber security, blockchain, and artificial intelligence.



Taekyoung Kwon received his B.S, M.S., and Ph.D. degrees in Computer Science from Yonsei University, Seoul, Rep. of Korea, in 1992, 1995, and 1999, respectively. He is currently a professor of Information Security at Yonsei University, Seoul, Rep. of Korea, where he is a director of the Information Security Lab. From 1999 to 2000, he was a postdoctoral research fellow at the University of California, Berkeley. From 2001 to 2013, he was a professor of Computer Engineering at Sejong University, Seoul, Rep. of Korea. He is a member of the director board of the Korea Institute of Information Security and Cryptology (KIISC) and a member of the editorial committee of the Korean Institute of Information Scientists and Engineers (KIISE). He is also a member of IEEE, ACM, and Usenix. His research interests include authentication, cryptographic protocols, software and system security, usable security, and AI security.

Wei-Chuen Yau is an Associate Professor in School of Electrical and Computer Engineering at Xiamen University Malaysia. He received his BS and MS degrees from National Cheng Kung University, Taiwan, and his PhD degree from Multimedia University. He is also a Chartered Engineer (CEng) and a Certified Information Systems Security Professional (CISSP). He was the General Co-Chair of Mycrypt 2016. His research interests include cryptography, security protocols, intrusion detection, network security, blockchain, and machine learning.

DaeHun Nyang received a BEng degree in Electronic Engineering from Korea Advanced Institute of Science and Technology, and MS and PhD degrees in Computer Science from Yonsei University, Rep. of Korea, in 1994, 1996, and 2000, respectively. He has been a senior member of the engineering staff at the Electronics and Telecommunications Research Institute, Rep. of Korea, from 2000 to 2003. Since 2003, he has been a Full Professor in Department of Computer Science and Engineering at Inha University, Rep. of Korea, where he is also the founding director of the Information Security Research Laboratory. He is a member of the board of directors and editorial board of the Korean Institute of Information Security and Cryptology and a section editor of ETRI Journal. His research interests include AI-based security, cryptography, privacy, usable security, traffic measurement, network security, and system security. He is a member of the IEEE.