Evolving Neural Network Intrusion Detection System for MCPS

Nishat Mowla*, Inshil Doh**, Kijoon Chae*

**Department of Computer Science and Engineering*

***Department of Cyber Security*

Ewha Womans University, 52, Ewhayeodae-gil, Seodaemun-gu, Seoul, 120750, Korea

nishat.i.mowla@gmail.com, isdoh1@ewha.ac.kr, kjchae@ewha.ac.kr

***Abstract*— Medical Cyber Physical Systems (MCPS) are some of the most promising next generation technologies so far. Like many other systems connected to a wider network such as internet, MCPS are also vulnerable to various forms of network attacks. For detecting such diverse forms of attack, we need smart and efficient mechanisms. Human intelligence is good enough to track such attacks but when it is a huge number of traffic it is no more a feasible process to detect them manually as it is time consuming and computationally intensive. Machine learning techniques embracing artificial intelligence are emerging as powerful tools to detect abnormalities in the network data. Supervised Neural Networks are some of the most efficient techniques to perform such classification. In this paper, we propose an evolving neural network technique that evolves based on classification, elimination and prioritization while focusing on time, space and accuracy to efficiently classify the four major types of network attack traffic found in an effectively pruned KDD dataset. We also show a leap of performance with hyper-parameter optimization which highly enhances the benefit of our proposed mechanism. Finally, the new performance gain is compared with a boosted Decision Tree. We believe our proposed mechanism can be adopted to new forms of attack categories and sub-categories.**

***Keyword*— MCPS, Machine Learning, Neural Networks, Intrusion Detection System**

Nishat Mowla received the B.S degree in Computer Science from Asian University for Women, Chittagong, Bangladesh in 2013, an M.S. degree in Computer Science and Engineering from Ewha Womans University, Seoul, Korea in 2016. She is currently a PhD student at Ewha Womans University, Seoul, Korea. Her research interests include next generation network security, IoT network security and network traffic analysis.

Inshil Doh received the B.S. and M.S. degrees in Computer Science at Ewha Womans University, Korea, in 1993 and 1995, respectively, and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2007. From 1995-1998, she worked in Samsung SDS of Korea to develop a marketing system. She was a research professor of Ewha Womans University in 2009~2010 and of Sungkyunkwan University in 2011. She is currently an assistant professor of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. Her research interests include wireless network, sensor network security, and M2M network security.

Prof. Chae received the B.S. degree in mathematics from Yonsei University in 1982, an M.S. degree in computer science from Syracuse University in 1984, and a Ph.D. degree in electrical and computer engineering from North Carolina State University in 1990. He is currently a professor in Department of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. His research interests include sensor network, smart grid, CDN, SDN and IoT, network protocol design and performance evaluation.