Hybrid Clustering Mechanisms for High-Efficiency Intrusion Prevention

Pin-Shan Lin, Yi-Cheng Lai, Man-Ling Liao, Shih-Ping Chiu and Jiann-Liang Chen

Department of Electrical Engineering, National Taiwan University of Science and Technology
Taipei, Taiwan

m11107510@mail.ntust.edu.tw, m11007505@mail.ntust.edu.tw, m11007502@mail.ntust.edu.tw, spchiu@mail.ntust.edu.tw, lchen@mail.ntust.edu.tw

***Abstract*—With the advancement of information and communication technology, cyberattack techniques have evolved into increasingly complex trends. Malicious network traffic attacks have become one of the information security problems for all organizations. This study is aimed to combat malicious network traffic attacks by actively collecting commands from attackers using honeypots. It involves pre-processing the raw network traffic data, employing a K-means algorithm to group the payloads, and label payloads using the MITRE ATT&CK framework. To improve the accuracy of the generated snort rules, the system utilizes Locality-Sensitive Hashing (LSH) method for secondary clustering, combined with snort rule generation, to form a comprehensive intrusion prevention system. In addition, to speed up the experimental process, this study adapted a script for this system to simulate an attacker's attack automatically. Through experimentation, it can be observed that hybrid clustering techniques such as K-means and LSH mechanisms can yield a defensive effectiveness of up to 93% for malicious payloads. This result proves the system's ability to identify and prevent different packet attacks effectively.ttom of this column.**

***Keyword*—K-means Algorithm, MITRE ATT&CK, Snort, Locality Sensitive Hashing (LSH), Malicious Packet**

Pin-Shan Lin was born in Hsinchu, Taiwan, in 2000. She received her B.S. degree in 2022. She is pursuing an M.S. degree in electrical engineering from the National Taiwan University of Science and Technology, Taipei. Her main research interests include data analysis, machine learning, and cyber threat intelligence.

Yi-Cheng Lai was born in Taipei, Taiwan, in 1998. He received his B.S. degree in 2021. He is pursuing an M.S. degree in electrical engineering from the National Taiwan University of Science and Technology, Taipei. His main research interests include cyber security, vulnerability research, and defense.

Man-Ling Liao was born in Tainan, Taiwan, in 1998. She received her B.S. degree in 2021. She is pursuing an M.S. degree in electrical engineering from the National Taiwan University of Science and Technology, Taipei. Her main research interests include data analysis, machine learning, and cyber threat intelligence.

Shih-Ping Chiu was born in Taipei, Taiwan, in 1984. She received the B.S. degree in 2007. She is a research assistant in electrical engineering from the National Taiwan University of Science and Technology, Taipei. Her main research interests include data analysis and the Internet of Things (IoT)

JIANN-LIANG CHEN (Senior Member, IEEE) was born in Taiwan in December 1963. He received a Ph.D. in electrical engineering from the National Taiwan University, Taipei, Taiwan, in 1989. Since August 1997, he has been with the Department of Computer Science and Information Engineering, National Dong Hwa University, where he is a Professor and the Vice Dean of the Science and Engineering College. He joins the Department of Electrical Engineering, National Taiwan University of Scienceand Technology, as a Distinguished Professor. His current research interests include cellular mobility management, cyber security, personal communication systems, and the Internet of Things (IoT).