Dimensional Feature Reduction for Detecting Botnet Activities

Muhammad Aidiel Rachman Putra*, Tohari Ahmad*, Dandy Pramana Hostiadi**

*Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

** Department of Informatics, Institut Teknologi dan Bisnis STIKOM Bali, Bali, Indonesia

6025211020@mhs.its.ac.id, tohari@if.its.ac.id, dandy@stikom-bali.ac.id

***Abstract*— Rising number of devices linked to the internet has made computer network security crucial. Those devices may be compromised, forming botnets, one of the most severe threats to network security due to their unique characteristics. An in-depth analysis of various processes, including feature extraction, is required to develop a botnet detection model with reliable performance. In this system, feature extraction is one of feature engineering, which is part of the data pre-processing. To find the best approach, we analyze the impact of feature extraction using dimensional reduction with four techniques: Principal Component Analysis, Truncate Singular Value Decomposition, Factor Analysis, and Fast Independent Component Analysis. The feature extraction results are brought to the classification stage to analyze their impact using several machine learning algorithms such as k-NN, Decision Tree, Random Forest, Naive Bayes, and Logistic Regression. Using the CTU-13, NCC-1, and NCC-2 datasets, it is found that dimensional reduction is suitable with k-NN but not recommended for a tree-based machine learning algorithm.**

***Keyword*— botnet detection, intrusion detection system, network infrastructure, network security, dimensional reduction**

Muhammad Aidiel Rachman Putra received the bachelor's degree in information technology from Universitas Sumatera Utara (USU), Indonesia. He is currently a Ph.D student at Institut Teknologi Sepuluh Nopember (ITS), Indonesia. His research interests include network security, computer network, botnet detection and intrusion detection system.

Tohari Ahmad received the Bachelor degree in computer science from Institut Teknologi Sepuluh Nopember (ITS), Indonesia, the master degree in information technology from Monash University, Australia, and the Ph.D degree in computer science from RMIT University, Australia. He was a consultant for some international companies. In 2003, he moved to ITS, where he is now a professor. His research interests include network security, information security, data hiding and computer network. He is a reviewer of a number of journals. Prof. Ahmad's awards and honors include the Hitachi Research Fellowship, and JICA Research Program to conduct research in Japan.

Dandy Pramana Hostiadi received the bachelor's degree from STMIK STIKOM Bali, master's degree from Udayana University, and the Ph.D degree from Institut Teknologi Sepuluh Nopember (ITS), Indonesia, all in Computer Science. He also as Lecturer in Institut Teknologi dan Bisnis STIKOM Bali, Indonesia. His scientific interests include network security and network forensics.