A semi-supervised model for network traffic anomaly detection

Nguyen Ha Duong*, Hoang Dang Hai**

*Faculty of Information and Technology, National University of Civil Engineering, Vietnam

** Ministry of Information and Communication, Vietnam

nghaduong@gmail.com, hdhai.hn@gmail.com

Abstract— **Network traffic anomaly detection can help to early detect network attacks because hacker's activities may result in unusual changes of network traffic, that are significant fluctuations compared to normal traffic of the network. Among various anomaly detection approaches, principal component analysis (PCA) has been seen as an effective solution. Until now, PCA is basically applied to dimension reduction method. Several issues remain including: how effective can PCA be applied to semi-supervised models with a small training dataset, which components are significant for anomaly detection. This paper proposes a semi-supervised model using a modified Mahanalobis distance based on PCA for network traffic anomaly detection. We propose a K-means clustering method to build normal profile of traffic to improve the training dataset and propose to give weights to choose principal components of PCA.**

Keyword— **Network traffic anomaly, anomaly detection, semi-supervised model, intrusion detection, network security**

Nguyen Ha Duong was born in Ha noi, Vietnam, in 1978. He received the B.E. degree in electronic and telecommunication engineering from the Ha Noi University of Technology, Vietnam, in 2001, and the Msc. degree in electronic and telecommunication engineering from the Ha Noi University of Technology, Vietnam, in 2003.
In 2001, he joined the Department of Network and System Engineering, IT Faculty, National University of Civil Engineering as a lecturer. His current research interests include network security, network protocol, routing, data mining and machine learning.

Hoang Dang Hai, was born in Vietnam in 1960. He received the Diplom-Ing. degree in Technical Cybernetics from the TechnicalUniversity Ilmenau (Germany) in 1984, Dr.-Ing. degree in Telematics and Dr.-Ing.habil. degree from the Technical University Ilmenau (Germany) in 1999 and 2003, respectively.
He is currently an Associate Professor at the Post and Telecommunication Institute of Technology (PTIT), Ministry of Information and Communications of Vietnam since 2010. His current research interests include information security, wireless sensor networks, network security and network traffic management.