A Model for Network Traffic Anomaly Detection

Nguyen Ha Duong*, Hoang Dang Hai**

**Faculty of Information and Technology, National University of Civil Engineering,*
55 Giai Phong, Hanoi, Vietnam
*** Posts and Telecommunications Institute of Technology, Ministry of Information and Communication,*
Nguyen Trai, Hanoi, Vietnam
duongnh@nuce.edu.vn, hdhai@mic.gov.vn

***Abstract*—Network traffic anomaly detection can find unusual events cause by hacker activity. Most research in this area focus on supervised and unsupervised model. In this work, we proposed a semi-supervised model based on combination of Mahalanobis distance and principal component analysis for network traffic anomaly detection. We also experiment clustering technique with suitable features to remove noise in training data along with some enhanced detection technique. With the approach of combining anomaly detection and misuse detection system, we believe the quality of normal dataset will greatly improve.**

***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.