Detecting Anomalous Network Traffic in IoT Networks

Dang Hai Hoang*, Ha Duong Nguyen**

**Posts and Telecommunication Institute of Technology, Hanoi, Vietnam*

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

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

Abstract—**Network operators need effective tools to quickly detect anomalies in traffic data for identifying network attacks. In contrast to traditional Internet, detection of anomalous network traffic in IoT (Internet of Things) networks is becoming a challenge task due to limited network resources and performance. Comprehensive detection methods are no longer effective for IoT networks, calling for developing lightweight solutions. Principal Component Analysis (PCA) techniques can help to reduce computing complexity, thus, anomaly detection techniques based on PCA received a lot of attention in the past. However, PCA techniques could not be directly applied to IoT networks with constrained resources and limited performance. This paper investigates PCA techniques for detecting anomalous network traffic in IoT networks. We propose a novel detection scheme with two levels using PCA techniques. The first level is for quick detection with few principal components while the second level is for detailed detection with a number of principal components. We investigate the selection of parameters in a distance calculation formula using several experiments to show the feasibility of our proposed scheme.**

Keyword— **IoT Network Traffic Anomaly, Anomaly Detection, Principal Component Analysis, Information Security, Network Security**

Dang Hai Hoang, Associate Prof. Dr. Dsc., BSc (1984), PhD (1999), DSc (2002) at TU Ilmenau, Germany. Current institution: Posts and Telecommunication Institute of Technology. Research interests: Communication network, IoT networks, information security, network security.

Ha Duong Nguyen, BSc (2001), MSc (2003) at TU Hanoi, PhD (2017) at PTIT, Vietnam. Current institution: Faculty of Information Technology. Research interests: Communication network, telecommunication networks, information security, network security.