# A PCA-based Method for IoT Network Traffic Anomaly Detection

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@gmail.com**

*Abstract*— **Network operators need effective tools to quickly detect anomalies in traffic data for identifying network attacks. In contrast to traditional Internet, anomaly detection 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. Methods using Principal Component Analysis (PCA) is an attractive approach due to complexity reduction. Anomaly detection techniques based on PCA received a lot of attention in the past. However, there are remaining issues by applying PCA such as the choice of principal components for complexity reduction. This paper investigates PCA techniques used in previous typical research works and proposes a new general formula for distance calculation and a new detection method based on PCA for IoT networks. The paper investigates formula parameters using several experiments. Results indicated that our new method is suitable for quick detection of network traffic anomalies with lower complexity.**

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

**Dang Hai Hoang,** A/Prof. Dr. DSc., 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.