# 論　文　要　旨
# Thesis Abstract

（yyyy/mm/dd）　2021 年　01 月　11 日

| ※報告番号 | 甲第　286　号 | 氏　名 (Name) | NGUYEN AN HUNG |
|---|---|---|---|

主論文題名　（Title）

Traffic Modeling and Anomaly Detection for Internet of Things

内容の要旨　（Abstract）

The development of the Internet of Things (IoT) has made significant changes to people's lives now and in the future. With the development of the Internet, smartphones, and especially sensor devices, IoT is becoming the new trend of the world. IoT is defined as objects that can connect to the Internet. We enter the house, unlock the door, the lights will automatically light up where we stand, the air conditioner will automatically adjust the temperature, the music will automatically turn on to welcome us, and so on. These things are becoming familiar in everyday life with IoT technology. However, accompanied by the explosion of IoT because its utilities will increase security risks, the more connections are created, the more widely shared data, the more many security vulnerabilities. As in the past, we studied Internet traffic when it became popular, so understanding, modeling, and classifying IoT traffic is now more necessary than ever. The main objectives of this research were to solve the problem of IoT traffic understanding by using a traffic generator dedicated to the IoT environment as well as identify smart devices and detect anomaly in an IoT network. In this dissertation, I designed a novel IoT traffic generator called IoTTGen. I generate synthetic traffic for smart home and bio-medical IoT environments. Simultaneously, I also build a smart home testbed to validate and compare with generated traffic from IoTTGen. Then, I have a visual observation of IoT traffic properties by Behavior Shapes. My generator succeeds in capturing the characteristics of the IoT traffic. Additionally, I also proposed a new method to identify IoT devices based on traffic entropy. I compute the entropy values of traffic features and I rely on Machine Learning algorithms to classify the traffic. My method succeeds in identifying devices under various network conditions with performances up to 94% in all cases. My method is also robust to unpredictable network behavior with anomalies spreading into the network. In my future research, I intend to experiment with more distinct environments. I will also consider other scenarios and cybersecurity threats.

※official use only