論 文 内 容 の 要 旨

博士論文題目　Deep learning-based cyberattacks behaviour analysis for IoT ecosystem

氏　名　Enkhtur Tsogbaatar

（論文内容の要旨）

The proliferation of the Internet of Things (IoT) and the evolution of technologies enable us to create multitudes of personal applications and services to make our daily life more comfortable and easier by adopting automation in daily operations. This growth boosts explosively for vulnerabilities and emerging attacks in parallel, which are for both IoT devices and applications. Most IoT devices are inherently vulnerable due to insecure design, implementation, and configuration. On the other hand, IoT applications are more vulnerable than devices during service time because attackers can exploit those vulnerabilities to compromise a secure system in milliseconds. One of such attacks is a low-rate and economic Distributed Denial of Service (DDoS) attack that targets to deteriorate users Quality of Service (QoS). Deep learning (DL) has a notable capability to assist, analyze user behaviours in complicated IoT ecosystems. DL can learn complex behavioral patterns of IoT devices and applications more effectively than conventional learning techniques, and it can detect attacks in IoT with maximum accuracy. Additionally, Software-Defined Networking (SDN) has appealing features such as flexibility, dynamicity in network operations, and resource management to support detection systems.

This thesis aims to design, develop, and implement comprehensive approaches to detect and predict cyberattacks in IoT devices and applications by integrating DL with SDN infrastructures. The major contributions of this thesis are in two folds. Firstly, we focus on IoT devices to address problems such as class imbalance, dynamic attack detection, and data heterogeneity. We propose a deep ensemble learning framework known as DeL-IoT to uncover and predict anomalies in IoT devices by integrating SDN. The DeL-IoT employs deep and stacked autoencoders to extract handy features for stacking into an ensemble learning model. Moreover, this framework yields efficient detection of anomalies, manages traffic flows dynamically, and forecasts both short and long-term device status for early action(s). Our experimental analysis proved that DeL-IoT performs well even in an 1% imbalanced dataset and outperforms 2%-3% when comparing F1 and MCC scores with single models. Secondly, several IoT applications are latency-sensitive and mission-critical when providing services over edge-clouds. However, attackers attempt to interrupt services deployed in edge-clouds by imitating legitimate behaviour

of users, one such attack is Very Short Intermittent DDoS (VSI-DDoS) attack that targets services to degrade users QoS. These attacks send intermittent bursts (in tens of milliseconds) of legitimate HTTP requests to the target services for degrading users QoS. Because of the stealthy nature of VSI-DDoS, it is challenging to pinpoint the root-cause when the system resource usage remains at a moderate level. Therefore, we propose a 1D-CNN-based (Convolutional Neural Network) DL method for detecting VSI-DDoS attacks in IoT applications. The experimental results on both testbed and benchmark datasets proved that our proposed method achieves maximum detection accuracy of 99.3% and 100% which gives improvement by 33.15%-0.01% detection in comparison to baseline approaches, respectively.

氏　名	Enkhtur Tsogbaatar

（論文審査結果の要旨）

本論文は、深層学習と SDN インフラストラクチャを統合することで、IoT デバイスやアプリケーションにおけるサイバー攻撃を検知・予測する包括的なアプローチを設計・開発・実装することを目的としている。本論文の主な貢献は以下の 2 点である。まず、IoT デバイスに着目し、クラスの不均衡、動的な攻撃検知、データの不均質性などの問題に対処している。SDN を統合して IoT デバイスの異常を発見・予測するために、DeL-IoT と呼ばれる深層アンサンブル学習フレームワークを提案している。本フレームワークは、異常の効率的な検出、トラフィックフローの動的な管理、早期対処のための短期および長期のデバイス状態の予測を実現している。実験では、不均衡なデータセットにおいても提案方式が良好なパフォーマンスを示すことを確認している。

次に本論文では、エッジクラウド上でサービスを提供するミッションクリティカルな IoT アプリケーションにおける QoS 低下問題を取り扱っている。具体的には、間欠的に（数十ミリ秒単位で）正当な HTTP リクエストを送信する VSI-DDoS (Very Short Intermittent DDoS) を対象として、1D-CNN (Convolutional Neural Network)を用いた検知手法を提案している。テストベッドとベンチマークの両データセットに対する実験結果から、提案手法はそれぞれ最大検知精度 99.3%と 100%を達成し、ベースラインアプローチと比較してそれぞれ 33.15%-0.01%の検出率の向上を実現することを確認している。

以上のように、IoT デバイスやアプリケーションのセキュリティ向上に資する検知・対処方式を提案し、テストベッドを用いた実験とデータセットを用いた性能評価によってその有効性を検証している。それぞれの成果は2編の学術論文（うち１本は投稿中）と2編の査読付き国際会議論文として発表されており、研究成果の有効性を見ることができる。よって本論文は、博士（工学）の学位論文としての価値があるものと認める。