A Study on Energy-Efficient Security Schemes in Wireless Multi-Hop Networks

February 2021

Hiromu Asahina

別表５
⑶

主　論　文　要　旨

No.1

報告番号	㊙ 乙 第　　号	氏　名	朝比奈 啓

主 論 文 題 名：

A Study on Energy-Efficient Security Schemes in Wireless Multi-Hop Networks
(無線マルチホップネットワークにおける省電力化セキュリティ方式に関する研究)

（内容の要旨）

無線通信技術の進歩や端末の小型化に伴い，スマートフォンやセンサを含む様々な機器をネットワークに接続する Internet of Things (IoT) の導入が進む一方， これら IoT 機器を狙った攻撃は増加しており，対策が急務となっている．一般に，IoT 機器はバッテリー駆動であるため，セキュリティの省電力化は解決すべき重要課題の一つである．しかしながら，IoT のネットワーク技術は，無線マルチホップ通信を用いることで端末の移動の有無や接続の連続性などが異なる多様なネットワーク構成を許容しているおり，それぞれのネットワーク技術に適したセキュリティの仕組みの省電力化は十分に達成されていない．

本論文では，接続が恒常的で端末の移動が無いネットワークの代表例として無線センサネットワーク(WSN)を，接続が間欠的で端末の移動が有るネットワークの代表例として遅延耐性ネットワーク(DTN)を取り上げ，それぞれにおける最重要なセキュリティ手法の省電力化を扱う．

本論文の構成を以下に示す．第１章では，従来のネットワークとの差異を概観することで IoT のセキュリティ課題を述べ，本研究の目的と位置付けを明確にする．第２章では，本研究で扱う IoT のシステムモデル，本研究に関連する従来研究とその問題点を述べる．第３章では，WSN における省電力なアップデートコード配布方式を提案する．本提案では，個々の IoT 機器のセキュリティを維持する上で最も重要となるファームウェアアップデートに注目し，アップデートを必要とするセンサへコードを配信する際の電力消費量を低減する． 計算機シミュレーションにより，提案が従来提案されているアップデートコード配布方式より少ない電力でコードの配布が可能であることを示す．第４章では，DTN におけるメッセージフラッディング攻撃の省電力な検知法を提案する．本提案では，DTN の本質的なセキュリティ課題であるネットワーク全体の監視の困難さを悪用したメッセージフラッディング攻撃に注目し，既存の防御手法において攻撃者を特定するために端末間で交換される通信履歴が消費する電力量を低減する．計算機シミュレーションにより，提案方式が検知性能を維持しつつ通信履歴の送信による電力消費量を低減できることを示す．第５章は結論であり，本論文の内容を総括している．

別表６
（３）

Keio University

Thesis Abstract

No.

Registration Number	☑ "KOU" □ "OTSU" No. *Office use only	Name	Hiromu Asahina

Thesis Title

A Study on Energy-Efficient Security Schemes in Wireless Multi-Hop Networks

Thesis Summary

Although the recent growth in the field of wireless communication technologies has promoted the Internet of Things (IoT) where various devices such as smartphones and sensors connect to the Internet, cyber-attacks against those IoT devices are on the increase as well. Since, in general, the IoT devices draw operation power by a battery, the traditional security schemes, which typically work on computers with a power supply, cannot be applied. Thus, many energy-efficient security schemes for the IoT have been proposed so far. However, there is still room for improvement. The reason behind this is the diversity of network topologies in IoT, which is realized by the multi-hop wireless communication technology. Although this technology enables devices to organize various types of networks flexibly, this flexibility also incurs a new type of attack or complicates a security task. Therefore, it is required to deal with individual security issues in various types of networks with different characteristics.

In this dissertation, I focus on Wireless Sensor Networks (WSNs) and Delay Tolerant Networks (DTNs) as representative IoT networks with different characteristics and propose novel energy-efficient security schemes for an argent security issue in each of these networks.

The outline of this dissertation is as follows: Chapter 1 deals with the security issues in the IoT through summarizing differences from the security in the traditional networks to clarify the purpose and position of this dissertation. Chapter 2 deals with the system models under consideration and the related works of this research. In chapter 3, I deal with the firmware update as the most fundamental mechanism to maintain a security level of the WSNs and propose an energy-efficient code dissemination scheme, which aims at reducing the energy consumption during the dissemination of latest firmware codes. Various performance evaluation results obtained by means of computer simulations show that the proposed scheme can reduce the energy consumption as compared to another previously known code dissemination scheme. In chapter 4, I deal with the message flooding attacks as a threat that reflects the most fundamental security issue in the DTNs, which is the difficulty of traffic monitoring across the network. In order to solve this problem, I propose an energy-efficient defense against the message flooding attacks, which allows nodes to identify attackers by exchanging the minimum required amount of communication history. Extensive performance evaluation results obtained by means of computer simulations verify that the proposed scheme improves the overall energy efficiency while maintaining the same level of attack detection accuracy compared to a previously known similar defense scheme. Chapter 5 concludes this dissertation and summarizes the contribution of this work.