A Study on Security and Privacy for Ad-hoc Network, VoIP Service and RFID-enabled Supply Chains System

February 2016

Kentaroh Toyoda

主　論　文　要　旨

報告番号	㊙ 乙 第　　号	氏 名	豊田 健太郎

主 論 文 題 目 :
A Study on Security and Privacy for Ad-hoc Network, VoIP Service and RFID-enabled Supply Chains System
（アドホックネットワーク，VoIPサービス，およびRFIDサプライチェーンシステムにおけるセキュリティとプライバシに関する研究）

（内容の要旨）

パーソナルコンピュータや携帯電話によるインターネットの利用者増大に伴い，ネットワークを介した様々な攻撃が問題となっている．これまで，これらの攻撃を防止するために共通鍵および公開鍵暗号方式，認証，デジタル署名技術などのセキュリティ技術が確立されてきた．一方，無線センサデバイス，スマートフォン，RFID (Radio Frequency Identification)といった多様な無線通信可能なデバイスの技術的進歩に伴い，我々の生活をより豊かにするような新しいシステムおよびサービスが急速に普及し始めている．しかしながら，これらのデバイスを用いたシステムやサービスには，アドホックネットワークにおいて信頼できる第三者機関を用いた認証ができないこと，VoIP サービスでは格安な通話料金を悪用した迷惑電話を発信する行為，RFID に書き込まれた情報の不正読取によるプライバシ侵害などといった既存のセキュリティ技術だけでは対処できない問題が存在する．したがって，これらに対する対策および防御策を講じることは喫緊の課題となっている．

本論文では，より安全・安心なシステムおよびサービスの実現に向け，アドホックネットワークにおける認証，VoIP サービス，および RFID サプライチェーンシステムにおけるセキュリティおよびプライバシ保護手法を提案し，理論計算，計算機シミュレーションおよび実験によりその有効性を示す．本論文の構成を以下に示す．

第 1 章では，無線センサデバイス，スマートフォン，RFID を用いたシステムおよびサービス，またそれらに対する脅威および対策について概観し，本研究の目的および位置付けを明確にする．

第 2 章では，無線センサデバイスおよびスマートフォンがアドホックネットワークにおいて，端末間通信のひとつである FFS (Feige-Fiat-Shamir) プロトコルの演算量を低減する方法として，認証における検証時に 1,024 ビットの変数の乗算が演算の負荷となっていることに着目し，乗算回数を低減しつつも，従来求められている安全性を確保する方式を提案する．そして安全性証明，理論計算および Android デバイスを用いた実測により，計算時間を低減可能であることを示す．

第 3 章では, IP 電話を始めとする音声通話サービスにおいて, 複数の通話に関する特徴量を基に, 発信者を 2 つのクラスタに分類することで学習を必要としない迷惑電話発信者手法を提案する．そして実通話データセットおよび生成したデータセットを用いたシミュレーションにより本方式の有効性を示す．

第 4 章では，RFID を用いた物流管理システムにおいてタグに書き込まれた製品情報 (EPC: Electronic Product Code)を漏洩させることなく商品を配送する方法として，タグの EPC に乱数をマスクした上でその乱数を認証サーバに置き，認証が成功した場合に正しい EPC を復元できる仕組みを提案する．提案方式では認証に必要な情報を閾値秘密分散法により商品のタグに書き込んだ上で，ダミーの情報を付加したタグを一緒に配送することで安全な認証情報の配送を可能とする．そして安全性証明，理論計算および市販されている RFID デバイスを用いた実験により有効性を示す．

第 5 章は，結論であり，本論文の内容および今後の課題を総括している．

SUMMARY OF Ph.D. DISSERTATION

School	Student Identification Number	SURNAME, First name
School of Science for Open and Environmental Systems		TOYODA, Kentaroh

Title

A Study on Security and Privacy for Ad-hoc Network, VoIP Service and RFID-enabled Supply Chains System

Abstract

Attacks via network are big issues as many people heavily use the Internet with computers and mobile phones. To defend against the attacks, several security techniques have been developed. Recently, the situation has been changing with technology advances that more objects equip wireless communication modules, i.e., wireless sensor devices, smartphones, and RFID (Radio Frequency Identification). This technological advance yields new systems and services that enrich our life. However, emerging systems and services suffer from unprecedented security and privacy issues, e.g., the problem that a trusted third party is not available for authentication in ad-hoc network, voice-based spam in the VoIP (Voice over IP) service, and the privacy issue that the information in RFID tags is illegally interrogated. Therefore, it is an urgent demand to take an appropriate measure against them.

In this thesis, we propose security and privacy approaches for ad-hoc network, VoIP service, and RFID-enabled supply chains system. The effectiveness of the proposals is shown by theoretical calculation, computer simulation, and experiments with off-the-shelf devices. The outline of this dissertation is as follows:

Chapter 2 deals with a lightweight verification scheme in FFS (Feige-Fiat-Shamir) protocol in ad-hoc network. We point out that the heaviest calculation in the verification is to multiply many 1,024 bits variables and propose a scheme to reduce the number of multiplication without lowering the required security. We show that the proposal is provably secure, the number of multiplication can be theoretically decreased, and calculation time is also shortened with an Android device.

Chapter 3 deals with a SPITters (Spam over Internet Telephony callers) detection scheme in voice communication services including VoIP. We propose an unsupervised SPITters detection scheme with multiple call features and clustering algorithm. The effectiveness is shown by the computer simulation with real call logs and an artificial dataset.

Chapter 4 deals with a secure products distribution scheme in RFID-enabled supply chains. We propose to mask tags' EPC (Electronic Product Code) with random sequences, and put them on an authentication server so that only a legitimate party can recover genuine tags' EPC. The required authentication code is split into product tags with a secret sharing scheme and dummy tags that possess bogus code information are introduced to securely distribute an authentication code. We show the effectiveness of the proposal by security analysis, theoretical calculation, and experiments with off-the-shelf RFID devices.

Chapter 5 concludes this dissertation and summarizes the contribution of this work and future work.