論文審査の要旨および学識確認結果

報告番号	甲／乙第　　号	氏　名	豊田 健太郎

論文審査担当者：				
	主査	慶應義塾大学教授	工学博士	笹瀬　巌
	副査	慶應義塾大学教授	工学博士	山中　直明
		慶應義塾大学教授	博士(工学)	大槻　知明
		慶應義塾大学教授	博士(工学)	眞田　幸俊
		アテネ大学教授	Ph.D.	MATHIOPOULOS　Panagiotis

(論文審査の要旨)

工学士、修士（工学)、豊田健太郎君提出の学位請求論文は、「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)」と題し、全 5 章から構成される。

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接続の普及に伴い、ネットワークを介した様々な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)等の無線通信可能なデバイスの技術的進歩に伴い、新たなシステムやサービスが急速に普及し始めている。しかしながら、アドホックネットワークでは信頼できる第三者機関を用いた認証が困難、VoIP サービスでは格安な通話料金を悪用した迷惑電話発信が増加、RFID では書き込まれた情報の不正読取によるプライバシ侵害等、既存のセキュリティ技術だけでは対処できない問題がある。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、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、提案方式の有効性を示している。

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におけるセキュリティとプライバシに対する課題を示し、本論文の目的と位置付けを述べている。

第 2 章では、無線センサデバイスやスマートフォンを用いるアドホックネットワークにおいて、端末間認証のひとつである Feige-Fiat-Shamir プロトコルの演算量を低減する方法として、検証時に 1024 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、要求される安全性を確保できる方式を提案している。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、提案方式が計算時間を低減可能であることを示している。

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により、学習を必要としない迷惑電話発信者検出手法を提案し、実際の通話履歴および生成したデータセットを用いて、提案方式の有効性を示している。

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している。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み、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している。そして、安全性証明、理論計算および市販 RFID デバイスを用いた実験により、提案方式の有効性を示している。

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。

以上、本論文の著者は、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、それらの有効性を明らかにしており、工学上、工業上寄与するところが少なくない。よって、本論文の著者は博士(工学)の学位を受ける資格があるものと認める。

学識確認結果	学位請求論文を中心にして関連学術について上記審査会委員で試問を行い、当該学術に関し広く深い学識を有することを確認した。 また、語学（英語）についても十分な学力を有することを確認した。