【26】

氏名（本籍）	劉　永生（中　国）
学位の種類	博　士（工　学）
学位記番号	博甲第6302号
学位授与年月日	平成24年7月25日
学位授与の要件	学位規則第4条第1項該当
審査研究科	システム情報工学研究科
学位論文題目	**Efficient Broadcast Authentication for Wireless Senor Networks** （ワイヤレスセンサネットワークにおけるブロードキャスト認証方式に関する研究）

主　査	筑波大学教授	博士（工学）	李　頡
副　査	筑波大学教授	理学博士	北川博之
副　査	筑波大学教授	工学博士	岡本栄司
副　査	筑波大学教授	博士（理学）	加藤和彦
副　査	筑波大学准教授	博士（情報科学）	木村成伴

論文の内容の要旨

本論文では、ワイヤレスセンサネットワークにおける有効なブロードキャスト認証方式に関する研究を行っている。本論文の第1章では、研究の背景と位置付けを述べている。また、関連のワイヤレスセンサネットワークにおけるブロードキャスト認証方式とそれらの問題点について論じている。第2章では、共通鍵暗号方式、公開鍵暗号方式（PKC: Public Key Cryptography）、メッセージの認証などの本論文に関連している知識について概説している。第3章では、ワイヤレスセンサネットワークにおけるSignature Amortizationを用いたPKC basedブロードキャスト認証方式を新たに提案している。提案した認証方式では、署名の効率を向上させるために、楕円曲線デジタル署名を用いている。また、提案したブロードキャスト認証方式のオーバーヘッドと安全性について分析している。そして、実際にワイヤレスセンサネットワークのテストベッドを構築して評価実験を行い、提案した方式が既存の方式より有効であることを示している。第4章では、階層型キーチェーンを用いて、ワイヤレスセンサネットワークにおける長期間での認証に対応できる長期遅延型ブロードキャスト認証方式を新たに提案している。そのため、送り手側の階層型キーチェーンと受取手側の階層型キーチェーンの構造を導入した。ワイヤレスセンサネットワークのテストベッドで評価実験を行い、提案した認証方式が一段階キーチェーンを持つ遅延型ブロードキャスト認証方式より実行時間とメモリの両方で有効であることを明らかにしている。この遅延型ブロードキャスト認証方式を実現するには、送り手と受取手の間の時間同期を必要としている。第5章では、ワイヤレスセンサネットワークにおける軽量かつセキュアのグローバル時間同期プロトコルを新たに提案している。提案した時間同期プロトコルでは、ブロードキャスト同期パケットを用いて、ワイヤレスセンサネットワーク内の全てのセンサノードを信頼できるソースノードの時間に同期させる。そして、同期したセンサノードとソースノード間の時間の歪みの上限を定量的に見積もっている。シミュレーションにより、提案した時間同期プロトコルの有効性を確認している。第6章では、論文をまとめ、今後の課題について述べている。

審 査 の 結 果 の 要 旨

ワイヤレスセンサネットワークにおいては、ブロードキャストメッセージの認証（ブロードキャスト認証）は重要な情報サービスの一つである。また、ワイヤレスセンサネットワークの一つの特徴としては、計算と通信に用いられる資源は少ないことが上げられる。ワイヤレスセンサネットワークにおいて、如何に効率よくブロードキャスト認証を行うのかは重要な研究課題の一つである。

本論文では、ワイヤレスセンサネットワークにおける有効なブロードキャスト認証方式に関する研究を行っている。具体的には、幾つかのブロードキャストメッセージの認証を纏め、Signature Amortization を用いた PKC（PKC: Public Key Cryptography）based ブロードキャスト認証方式を新たに提案している。また、送り手側の階層型キーチェーンと受取手側の階層型キーチェーンの構造を導入し、ワイヤレスセンサネットワークにおける長期間での認証に対応できる長期遅延型ブロードキャスト認証方式を新たに提案している。さらに、遅延型ブロードキャスト認証方式を実現するための軽量かつセキュアのグローバル時間同期プロトコルを新たに提案している。理論的な分析とテストベッド上での評価実験により、提案した方式の有効性を示している。これらの研究成果は情報工学上貢献するところが大きいと判断される。今後は、提案した方式をより現実で大規模なワイヤレスセンサネットワーク環境上に実装し、その有効性を示すことが望まれる。

平成 24 年 6 月 4 日、システム情報工学研究科において、学位論文審査委員の全員出席のもと、著者に論文について説明を求め、関連事項につき質疑応答を行った。その結果、学位論文審査委員全員によって、合格と判定された。

上記の学位論文審査ならびに最終試験の結果に基づき、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。