論 文 内 容 の 要 旨

博士論文題目
センサネットワークを利用したサービスにおける情報セキュリティとフィジカルセキュリティに関する研究

氏 名　野田 潤

（論文内容の要旨）
センサネットワークにおいてはプライバシ保護が大きな問題となるため，新サービスの実現にあたっては，センサネットワークに適応可能な情報セキュリティ技術の導入を検討する必要がある．一方で，センサが実空間上に配備されることにより，センサ自体への攻撃や盗難等への配慮もこれまで以上に必要となる．このような背景をふまえ，本論文では，センサネットワークの安全性確保のための新しい鍵共有・鍵管理方式が提案されているとともに，センサネットワークにおける機能そのものを安全かつ有効に利用するためのフィジカルセキュリティに関する研究成果がまとめられている．

第 2 章ではセンサネットワークの応用の多くにおいて必要となるグループ通信の安全性強化に貢献するグループ鍵管理方式について論じられている．提案方式は，ノードの属性に紐つける管理情報を用いて，個々のグループ鍵の管理の仕組みを互いに連携させる．実用的な評価も交えて，一台のノードが複数の大規模グループに所属する場合に，従来に比べ，ノードのメモリ負荷の 64%～88%を，通信負荷の 46%～97%を削減できることが示されている．

第 3 章では，初見の端末同士でアドホックな通信路を安全に開設するために有効な，動的な鍵生成法について論じられている．外部情報のセンシング時においては，センサ単体で処理が完結することもあるが，センサ間やユーザの備える機器を含む機器間での通信が求められることも多い．この時，必要になる全ての通信路を予見し，暗号の鍵を用意することは困難である．提案方式は，センサが取得するユーザ状況，特にユーザの動作に関する情報の類似度に応じて，センサ情報から直接強度の異なる鍵を生成し，似た状況の端末間で自動的に鍵を共有させる手法となっている．加速度センサを用いた歩行，自動車によ

る移動動作からの鍵生成性能評価の結果，高々2 分程度で，4 桁の PIN コード相当の強度を持つ共通鍵を共有できることが示されている．

第 4 章では，センサから取得する情報を有効利用するフィジカルセキュリティ，具体的に物理的なアクセス制御について論じられている．提案方式では，信用管理の新たなアーキテクチャとして，信用の確立に利用する情報に，ユーザが提示したディジタル証明書に加え，センサで取得可能なユーザのプレゼンス(存在位置）が導入されている．プレゼンスの導入に際しては，プレゼンスに信頼度というパラメータを与え，確率モデル(マクロ状態を持つ隠れマルコフモデル）に基づく信頼度評価によってプレゼンスの不確実性が考慮される．被験者と RFID センサを用いた評価実験を通じて,確率モデルを用いた提案法により，得られるプレゼンスの recall を約 1.8 倍(0.94 以上)に向上できることが実証されているおり，その結果，信用確立における利便性や安全性を向上できることが示されている．

氏　名	野田　潤

（論文審査結果の要旨）

本論文では，センサネットワークを利用したサービスにおける情報セキュリティとフィジカルセキュリティに関して，以下のような知見を得ている．

（１）センサネットワーク技術の実用化局面においては，複数のサービス事業者が同一のネットワーク基盤を共用し，その上に各サービスを実現するような形態が考えられる．この場合であっても，各サービスの独立性と機密性を保証する必要があるが，本研究で提案されているグループ鍵管理方式は，この問題に対する有力な解となり得るものである．従来研究の多くでは，システム全体で一個のグループ鍵を共有することを前提としており，管理すべきグループ数の増加は，そのまま鍵管理コストの増加に直結するという問題があった．これに対し本研究では，複数のグループから導かれるノード集合の包含関係を多角的・多次元的に利用し，多数の独立グループネットワーク内に存在する場合であっても，きわめて効率的に鍵更新等を実現することが可能となっている．

（２）ヘッドセット等個人利用のための機器間の接続や，街頭，イベント会場，災害時における通信には，基地局を介さないモバイルアドホックネットワーク(MANET)が有用である．MANET における安全な通信にも共通鍵暗号が用いられるが，それに先立つ鍵共有は一般のユーザにとっては煩わしい操作である．この問題への一つのアプローチとして人間の動作から共通鍵を自動生成する研究が注目されている．本研究では，人間の動作の類似度に応じて強度の異なる鍵生成法を自動選択し，極めて類似度の高い動作対に対しては周波数領域上の特徴に基づいて（高いレートで）鍵を生成し，また，中程度の類似度をもつ動作対からは時間領域上の特徴（加速度分散値の時系列データ）に基づいて鍵を生成する手法が提案されている．これにより，歩行のように特徴量の小さい動作からでも false positive（類似度の低い動作から誤って同一の鍵を生成すること）を低く抑えることに成功している．

（３）モバイル機器等の使用において，例えば「外部研究員は，正社員と同室にいる場合に限りシステムへ正社員用パスワードなしにログインできる」等，ユーザのプレゼンス（ユーザがどこに存在し周囲はどのような状況か）に基づくアクセス制御をきめ細かく行うことができれば，システムの安全性とユーザの利便性を高いレベルで両立させることができる．本研究ではまず，従来のロールベースアクセス制御，公開鍵基盤(PKI)，センサに基づくユーザプレゼンスのすべてを同じ枠組みで表現できるアクセス制御モデルが提案されている．次に，電波状況等の影響で必ずしも信頼性の高くないセンサからのユーザプレゼンス情報を，隠れマルコフモデルを応用して自動修正する手法が開発されている．被験者と RFID センサを用いた評価実験により，プレゼンスの precision を低下させることなく recall を 0.94 以上に向上できることが示されている．

以上の通り，本論文で提案する手法と得られた結果は，情報セキュリティ，とりわけ，今後益々重要性を増すセンサネットワークにおける暗号通信やアクセス制御において，安全性と効率を高いトレードオフ点で実現するための新しい手法を提案しており，博士（工学）の学位論文として価値あるものと認める．