講演番号： 50

アドホックネットワークにおけるセキュリティ向上化の検討

B－18 Study of security enhancement in the ad hoc sensor network

吉本 涼† 石川 真也† 宮保 憲治†

Ryo YOSHIMOTO† Shinya ISHIKAWA† Noriharu MIYAHO†

†東京電機大学大学院 情報環境学専攻

† Graduate School of Information Environment, Tokyo Denki University

1. はじめに

近年，無線ノードが自律的にネットワークを構築するアドホックネットワークが注目されている．アドホックネットワークは，環境モニタリング[1] や生体情報を活用したセンサネットワーク[2] への応用が進みつつある．無線ノードは電池駆動で使用する場合が多く，収集情報を安全にデータ配送先へ送信するためには，無線ノードの低電力化に配慮することが必要である．本稿では，センサデータに対して暗号処理を実施した後に，暗号文を分割・複製・シャッフリングする高速暗号演算処理機構[3]を活用し，複数の周波数を用いてマルチパス上にパケット化されたセンサデータを送信する手法を提案する．また，ネットワークシミュレータ QualNet[4]を用いパケット復元率を評価した結果を述べる．

2. マルチパス手法

高速暗号演算処理機構によって生成されたメタデータと断片データは,盗聴や改竄を防ぐため，異なる周波数で異なる経路（パス）を用いて送信する方法がセキュリティ上，安全である．複数の周波数を使用し，マルチパスを利用し，メタデータと断片データを送信する．複数の周波数とマルチパスを利用する方法はアドホックネットワークのルーティングプロトコルである AODV[5]方式を改良して実現した．

3. シミュレーション実験

高速暗号演算処理機構を実装した無線ノードにおける AODV 方式に，複数の周波数とマルチパス手法を適用した時のセンサデータの復元率をネットワークシミュレータ QualNet を活用して測定した．実験で使用したパラメータを表 1 に示す．無線ノードは 2 [s]毎にセンシングを行い，暗号化後にメタデータと断片データを 0.1 [s]間隔で送信する．中継ノードに，単一の周波数を用いる方式（提案方式 1）と複数の周波数を用いる方式（提案方式 2）に対して，断片データ数の変化に伴うセンサデータの復元率を図 2 に示す．

表 1． 評価パラメータ

項目	パラメータ
シミュレータ	OualNet
無線通信規格	IEEE802.15.4
周波数帯	2.4GHz 帯
センサデータサイズ	64 [Byte]
断片データ数	2,4,8,16
距離	300 [m]

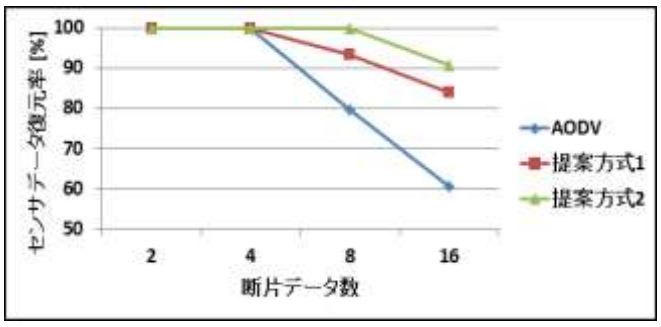

図 2 断片データ数の変化に伴うセンサデータの復元率

図 2 より，複数の周波数を利用したマルチパス手法は，断片データ数が増えても，電波干渉が少なくなるため，センサデータの復元率の低下を抑えることが出来る．中継ノードに複数の周波数を対応させるとセンサデータの復元率の低下を更に抑えることが出来る．すなわち，既存プロトコルの AODV 方式よりも複数の周波数を利用したマルチパス通信は，セキュリティの強度を向上させ，同時にセンサデータの復元率を高くできる有効な手段と考えられる．

4. 今後の課題

センサデータの復元を確実に行うためには，メタデータのロスを極力，抑える必要がある．そのため，複数の経路の中でパケットロス率の最も低い経路を用いたメタデータの転送を実現するための手法を検討する予定である．

参考文献

[1] 山東剛，冬爪成人,宮保憲治，“センサネットワークを応用した放射能拡散予測用の防災システムの一検討”，平成 23 年度電子情報通信学会東京支部学生会研究発表会

[2] 中村達郎，後藤啓太，今野紀子，島田尊正，宮保憲治,“セキュリティを考慮したセンサネットワークにおける優先制御方式の検討” 2010 年電子情報通信学会講演論文集,S.94-S.95, 2010.

[3] M.Kouki, N.Miyaho 電子情報通信学会総合大会,ISS-SP-P186,” センサネットワークにおけるセキュリティ向上化の検討”,2015

[4] QualNet，構造計画研究所，2015, http://network.kke.co.jp/products/qualnet/

[5] C.E. Perkins, E.M. Belding −Royer, S.R. Das,"Ad hoc On-Demand Distance Vector(AODV)Routing," RFC3561, 2003.