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

三石 広樹† 宮保 憲治†
†東京電機大学大学院 情報環境学専攻

1. はじめに

近年，無線通信機能を備えたセンサノードが構築するセンサネットワークが注目されている．センサネットワークでは温度や湿度などの環境情報を収集・解析した結果を活用することにより，特定領域の監視システムとして利用できる．センサノードは電池駆動である場合が多く，情報を安全に送信するためには，センサノードの低電力化に配慮した暗号演算専用の処理機構の検討が必要である．

本論文では，環境情報に対して暗号処理を実施した後に，暗号文を複数の断片データに分割・複製して送信できる高速暗号演算処理機構を提案する．以下に，攻撃者による環境情報の盗聴や改竄を防ぐための，高速暗号演算処理機構ならびに，ネットワークシミュレータ QualNet[1]を用いて実装し，評価した結果を述べる．

2. 提案手法 高速暗号演算処理機構

センサノードは一般的に限られた演算能力しかもたない．センサノードの省電力化と演算コストに配慮した高速暗号演算処理機構を図 1 に示す．

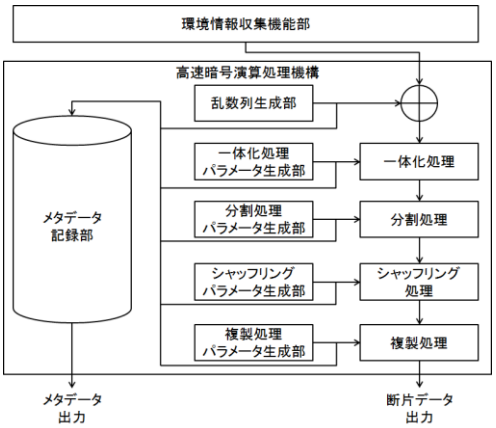

図 1 高速暗号演算処理機構

センサーが取得した環境情報は，排他的論理和演算と一体化処理[2]後に，N 個の断片データに高速に分割処理される．断片データを送信する順番は，シャッフリング処理により発生順とは無関係にする．断片データは，複製して送信できるようにする．これら一連の処理において，乱数列や演算に関わるパラメータは，環境情報の収集毎に生成する．使用パラメータは，暗号解読のために必要な暗号鍵に相当し，暗号解読用のメタデータとして時系列的にメタデータ記録部へ保存する．その後，断片データの送信に先立って,予め設定されたルートで宛先ノードへ送信する．

3. シミュレーション実験

提案手法を実装したセンサノードの通信システムで，ノード数と断片データ複製数をパラメータとした時のデータ復元率の変化をネットワークシミュレータ QualNet を用いて測定した．実験評価パラメータを表 1 に示す．センサノードは 30[s] 毎にセンシングを行い，暗号化実施後にメタデータと断片データを 50 [ms]間隔で送信する．断片データ損失率，センサデータ復元率を図 2，図 3 に示す．

表 1 実験評価パラメータ

シミュレーション領域	1500×1500 [m]
ノード数(基地局除く)	10, 20, 30, 40, 50 [個]
ノード配置	ランダム
シミュレーション試行回数	100 [回]
ルーティングプロトコル	AODV
無線通信規格	IEEE802.15.4
センサデータサイズ	64 [Byte]
断片データ数	8 [分割]
断片データ複製数	0, 1, 2, 3, 4, 5, 6 [個]

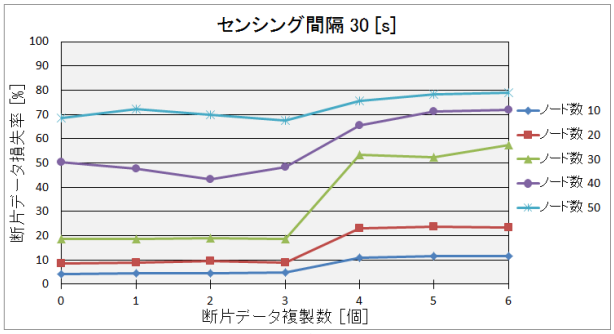

図 2 断片データ損失率

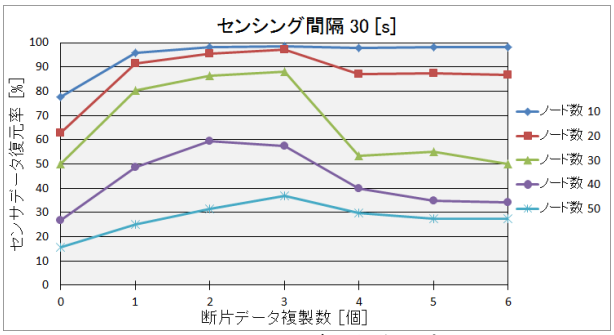

図 3 センサデータ復元率

図 2，図 3 より，断片データを複製した場合，複製がない場合と比較して，センサデータ復元率が向上することがわかる．理由は，一定数の断片データによって復号が可能になるからである．複製数が 4 個以上になると断片データ損失率が増加し，センサデータ復元率が減少した．この理由は複製数を増やしたことで断片データのパケットサイズが増え，断片データの送信時間増加による，端末間の電波干渉の影響が増大したためと考えられる．

4. 今後の課題

今後はメタデータと断片データを異経路分散するための最適ルーティングプロトコルの提案・実装を行う．

参考文献

[1] QualNet，構造計画研究所，2015 年 1 月 12 日，http://network.kke.co.jp/products/qualnet/
[2] N. Miyaho, Y. Ueno, S. Suzuki, K. Mori and K. Ichihara, “Study on a Disaster Recovery Network Mechanism by Using Widely Distributed Client Nodes”, ISCNC2009, pp.217-223, Sep.2,2009