1Z-2

無線センサネットワークにおけるセキュリティ向上の検討

三石 広樹† 宮保 憲治† 鈴木 男人† 鈴木 貴之†

†東京電機大学大学院 情報環境学研究科

1. はじめに

近年，無線通信機を備えたセンサノードが自律的に動作するアドホックセンサネットワーク(ASN : Ad Hoc Sensor Network)が注目されている．ASN は，センサノードを複数箇所に配置し，情報収集・分析を行うことにより周辺環境の監視が迅速にできるため，防犯や軍事等の幅広い分野で活用できる。センサノードは電池駆動である場合が多く，収集情報を安全にデータ配送先へ送信するためには，センサノードの低電力化に配慮した高速暗号演算処理機構の検討が必要である．

本稿では，センサノードが収集した情報に対して高速暗号処理を実施した後に，暗号文を複数のデータパケットに分割して配送する方式を提案する．以下に，攻撃者による収集情報の盗聴や改竄を防ぐための高速暗号演算処理機構について，IRIS MOTE[1]を用いて実装評価した結果を述べる．

2. アドホックセンサネットワーク

ASN の基本構成例を図 1 に示す．センサノードは周辺の情報を収集するためのセンサボードと無線通信機を備える．各センサノードはグローバルネットワークへのゲートウェイとなる基地局ノードへ収集したデータ情報を配信する．ネットワーク管理者は ASN 内の情報の定期的に監視する．

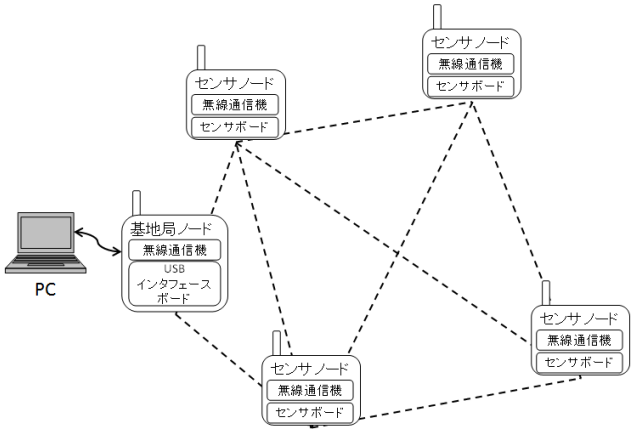

図 1. ASN の基本構成例

Improvement of wireless sensor network security
Kouki Mitsuishi†, Noriharu Miyaho†, Nanto Suzuki†, Takayuki Suzuki†
†Graduate School of Information Environment, Tokyo Denki University

3. 高速暗号演算処理機構

センサノードは一般的に安価なので，限られた演算能力しかもたない．従って，収集情報に暗号処理を行う場合には，センサノードの仕様上の制限に配慮した高速暗号演算処理機構の実装が必要である．センサノードに実装した高速暗号演算処理機構を図 2 に示す．

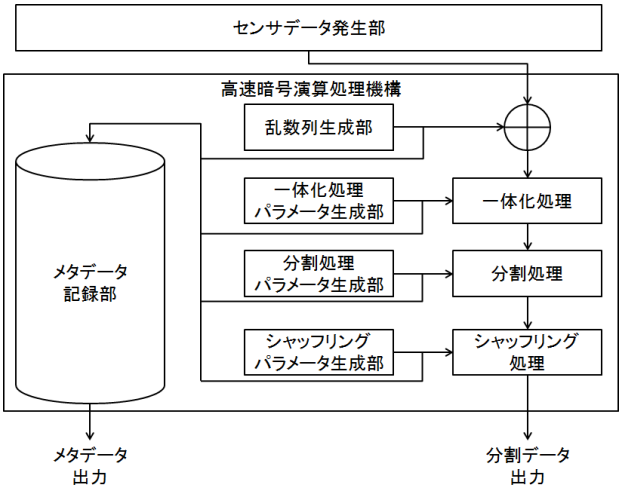

図 2. センサノードの高速暗号演算処理機構

センサデータ発生部では，収集されたセンサデータと同じ長さの乱数列で排他的論理和演算を実施する．当該の演算処理が行われたセンサデータは，一体化処理[2]後に、N 個の断片データに分割処理される．この分割されたデータを送信する順番は，シャッフリング処理を実施して順不同にする．上述した一連の処理において，乱数列や演算処理に関わるパラメータは，センサデータ発生部でセンサデータを収集する度に生成する．この乱数列とパラメータは，暗号解読のために必要な暗号鍵に相当し，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．メタデータ記録部に保存されたメタデータは，上記の分割データの送信に先立って送信される必要がある．

データ配信先ノードは，このメタデータの情報を用いて，高速暗号演算処理機構の処理手順を逆の順序で実施し，センサデータを復号化する．

高速暗号演算処理機構は，センサデータを適切なサイズに分割して多経路に転送することにより，データ配信先以外の第３者による分割データ

の回収が困難になるため，セキュリティ強度を，一層向上できる．

4. 実験内容

高速暗号演算処理機構を実装したセンサノードにおける，分割データ数とホップ数による，復元可能なパケット到達率の変化を，IRIS MOTE を用いて測定した．実験パラメータを表 1 に示す．実験ネットワーク構成を図 4 に示す．

センサノードは直線上に 4 個配置した．ノード間距離は，先行研究[3]より，ホップ数が増加しても安定した通信が可能である 10[m]に設定し，データ分割数によるパケット到達率の影響を検証した．

表 1. 実験パラメータ

センサノード	IRIS MOTE
センサノード数	4
ソフトウェア	XMesh[4]
無線周波数帯域	2.4 [GHz]
ネットワークトポロジ	リニア型
パケット送信間隔	5 [sec]
ノード間距離	10 [m]
一体化処理回数	7 [回]
分割データ数	2,4,8,16 [分割]

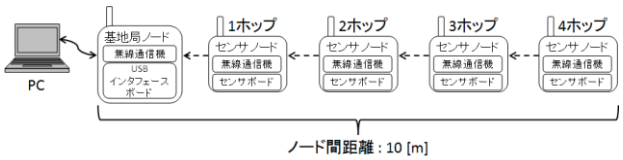

図 4. 実験ネットワーク構成

5. 実験結果

図 4 に示した実験ネットワーク構成にて測定したビットエラー率を図 5 に，パケット到達率を図 6 に示す．ビットエラー率は，受信したパケットの内，ビット誤りを検出した割合を示す．パケット到達率は，センサデータを正常に復号化できた割合を示す．

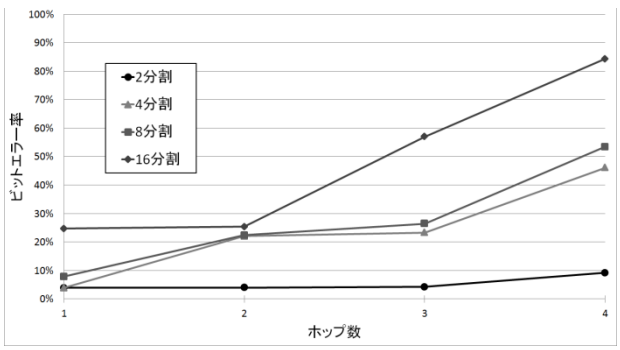

図 5. ビットエラー率

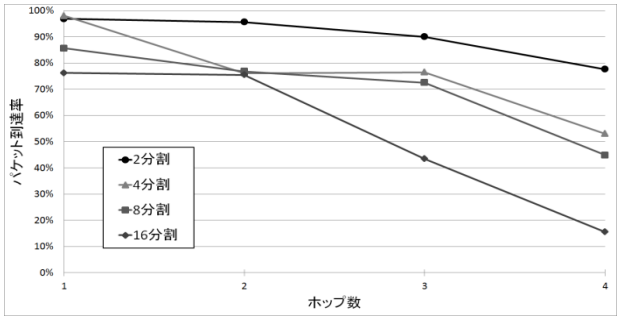

図 6. パケット到達率

6. 考察

図 5，図 6 で得られた実験結果より，ホップ数とデータ分割数の増加に伴って，ビットエラー率は上昇し，パケット到達率は低下することを定量的に検証できた．この実験結果は，すでに先行研究で報告されているように，ホップ数を増加させて通信距離を長くすると，周辺端末からの電波干渉の影響が強くなる現象を裏付けている．データ分割数の増加により通信トラフィック量も漸増するため，電波干渉の影響は通常の場合より大きくなることが想定できる．これらの要因が組み合わされることにより，パケット同士の衝突頻度が上昇し，パケット到達率が低下したと考えられる．

7. まとめ

高速暗号演算処理機構をセンサノードへ実装することにより，ASN におけるセキュリティ強度を向上化できる可能性を示すと共に，データ分割数の増減によるパケット到達率を評価した．

今後は，メッシュ型ネットワークにおける高速暗号演算処理機構の性能評価を進める．またパケット到達率の一層の向上化のために，分割データを複製して送信するパケット複製方式，パケット衝突頻度を低下させるためのチャネル制御方式の検討を進める予定である．

参考文献

[1] MOTE 仕様,住友精密工業株式会社, 2014 年 1 月 11 日, http://www.xbow.jp/

[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

[3] 石川, 山本, 山東, 三石, 宮保, “アドホックセンサネットワークを構成するセンサノードの性能評価”, 平成 24 年度電子情報通信学会東京支部学生会研究発表会,講演番号 119,2013 年 3 月

[4] 住友精密工業, “MoteWorks センサネット統合ソフトウェア - クロスボー”, 2014 年 1 月 11 日, http://www.xbow.jp/moteworks.html