L-033

ルーティングアルゴリズムによるセンサネットワークのセキュリティ強化手法
A Routing-based Approach to Enhancing Sensor Network Security

孟　南† Nan Meng　王 家宏‡ Jiahong Wang　児玉　英一郎‡ Eiichiro Kodama　高田　豊雄‡ Toyoo Takata

1．まえがき

近年，センサネットワークが様々な分野に広く応用されるようになっている。通常の情報システムと同じように，センサネットワークにおいても，情報漏洩の問題が存在する。本研究はセンサネットワークのセキュリティを向上させることを目的とする。

センサネットワークでは基地局へ観測情報を送信するために，自律的にマルチホップ無線ネットワークを構築する。マルチホップ通信は，電波が直接届かないノードへデータを送信するときに，宛先との間に存在するノートがバケツリレー形式でデータを中継する。図 1 にセンサネットワークの応用例を示す。この例では，センサネットワークが食品や衣服，銃，爆弾などの軍事用品を保管する軍用倉庫の，温度や湿度などの保管環境の管理，品物の種類や数量などの在庫状況の把握，入出庫や点検作業などの監視などのために利用されている。

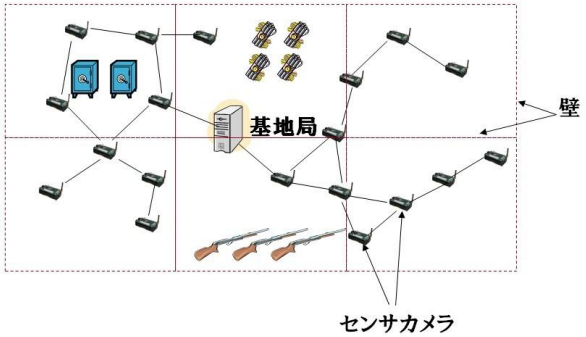

図1：センサネットワークを利用した軍用倉庫

本研究で想定したセンサネットワークの応用環境は，例えば，建物の内部と外部との境界が柵や金網などで隔たれた敷地など，部外者が容易に立ち入ることが困難な領域である。このような境界線で囲まれ閉じられた環境のなかで，センサノードが機密性の高い観測データを送受信する。図 2 に想定環境におけるセンサネットワークのセキュリティ問題を示す。図内の点線は境界線を示す。境界線に近いノードからの電波が境界外に届く可能性がある。もし攻撃者のアンテナがその範囲内に設置された場合，センサネットワークの情報を盗聴することが可能となり，セキュリティ上の問題が発生する。特に，データ転送はマルチホップ通信で行われるため，送受信ノードだけではなく，中継ノードにおいても電波漏洩の可能性がある。中継回数が多いノードほど，電波の送信回数が多くなり，盗聴される可能性が高くなる。

本研究では，センサノードから発信される電波が領域外へ漏洩してしまうことをできるだけ抑えることにより，センサネットワークのセキュリティを向上させることを目的としており，そのための新しいルーティングアルゴリズムを提案する。

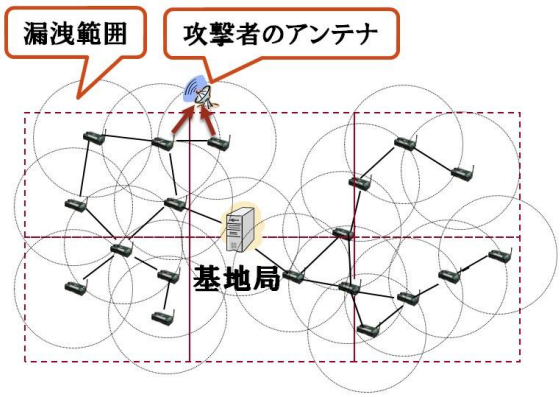

図 2：センサネットワークにおけるセキュリティ問題

2．関連研究

Chris KarlofとDavid Wagner [1] は，センサネットワークのルーティングに対するHELLOフラッド攻撃，Wormholes 攻撃，選択転送攻撃など様々な攻撃手法を示した。H. Luo[2]は公開鍵暗号を利用し，アドホックネットワークに対する攻撃の可能性を軽減する手法を提案している。ノード間でデータを送受信する際に，送信パケットに認証子を付加し，受信ノードがパケットの認証子を確認することで，認証を行うものである。この方法は理論上，効果が期待されるが，センサノードはバッテリーで駆動するものであることから，負荷が大きく，このような高い処理能力を必要とするセキュリティ対策を施すことは事実上困難である。これらのアルゴリズムを利用して，セキュリティ向上を図ることも考えられるが，電力問題を考慮すると，想定環境における電波漏洩問題に対しては，適切な手法ではないと考えられる。

3.　電波の漏洩を抑える手法の提案

本節では，電波の漏洩を抑えるためのセキュアルーティングアルゴリズムを提案する。提案するセキュアルーティングアルゴリズムは 2 ステップであり，通信バックボーンの構築，ルーティングアルゴリズムの適用に分け示す。

3.1.　基地局の設置場所について

センサネットワークにおいては，基地局（BS, ベーステーション）は特別な役割を果たすことから，その配置場所は必要に応じて決める必要がある。本研究では，セキュリティを確保する観点から，図 2 に示すように，領域内の相対的な中心に設置されているとする。攻撃者のアンテナが領域外のどの場所にも設置される可能性があることから，より中心に近い場所が安全である。

3.2　通信バックボーンの構築

まず，BS をルートノードとして Spanning Tree（ST）を

†岩手県立大学大学院ソフトウェア情報学研究科
‡岩手県立大学ソフトウェア情報学部

構築する。そして，通信バックボーンの構築は以下に示す手順で構築を行う。Level_LastN は，ST の最終のレベルからルート方向に N レベル分のすべてのノードの集合である。

Input ： ST を構築したセンサネットワーク
Output： バックボーンを構築したセンサネットワーク

1. BS を Black でマークし，Level_LastN を除く他の全てのノードを White でマークする。
2. BS は Pa をブロードキャストする。
3. White ノードがはじめて Black ノードからの Pa を受信した場合，Grey になり，Pb をブロードキャストする。
4. White ノードが全ての優先ノード（レベルがより低いか，同じレベルで ID 番号がより小さいノード）の Pb を受信した後，Black に変わり，Pa をブロードキャストする。
5. Grey ノードがはじめて P_b をまだ送信していない子ノードから Pa を受信した場合は，その Grey ノードは Black に変わり，Pa をブロードキャストする。

3.3 ルーティングアルゴリズムの適用

本ルーティングアルゴリズムの適用を以下に示す。

Case 1： Black ノードが目的ノードを探す
まず自分をルートとしたツリーと隣接ノードのなかから目的ノードを探す。
(a) 目的ノードがある場合は，ルートを構築し，データを転送する。
(b) 目的ノードがない場合は，レベルが低く，ID 番号の小さい Black ノードにデータを転送し，Case 1 に戻る。

Case 2： Grey ノードが目的ノードを探す
まず自分をルートとしたツリーと隣接ノードのなかから目的ノードを探す。
(a) 目的ノードがある場合は，ルートを構築し，データを転送する。
(b) 目的ノードがない場合は，レベルが低く，ID 番号の小さい Black ノードにデータを転送し，Case 1 に移る。

Case 3： Level_ LastN ノードが目的ノードを探す
まず自分をルートとしたツリーと隣接ノードのなかから目的ノードを探す。目的ノードがない場合は
(a) Black ノードが隣接ノードである場合，レベルの低く，ID 番号の小さい Black ノードにデータを転送し，Case 1 に移る。
(b) 隣接ノードに Black ノードがなく、Grey ノードしかない場合，レベルの低く，ID 番号の小さい Grey ノードにデータを転送し，Case 2 に移る。
(c) レベルの低いノードが Level_ LastN ノードしかない場合，レベルの低く，ID 番号の小さい Level_ LastN ノードにデータを転送し，Case 3 に移る。

4. 性能評価

第 3 節で述べた提案手法を実装し，性能評価を行った。本節では実験環境及び実験結果を示し，その考察を行う。本評価における比較対象は AODV[3]とした。

4.1. 評価環境と評価項目

本シミュレーション環境を表 1 に示す。

表1： シミュレーション環境

項目	設定値
シミュレーション時間	300 秒
基地局	1 個（ID 番号： 0）
ノード数	80 個, 100 個, 120 個
ノードの電波半径	40 メートル
領域	300×300 メートル

評価基準は，漏洩率を使った。漏洩率は，センサノードがパケットを送信するときに発生した電波が領域外へ漏洩した回数と，パケットの総送信回数の比率である。

4.2. 評価結果と考察

前述の評価環境にて実験を行った。実験ではランダムに選んだ 10 組の境界に近い 2 つのノード間で 1 秒ごとにデータの送受信を行った。

実験から得た漏洩率を図 3 に示す。AODV の漏洩率がおよそ 35%から 52%までであり，提案手法の漏洩率が 20%程度であった。

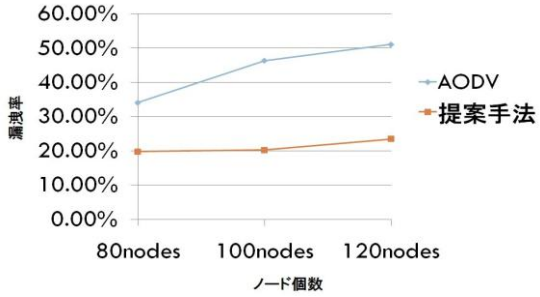

図 3 漏洩率

実験結果から，提案手法が AODV より漏洩率が低く，性能がよいことが分かる。また，提案手法を用いることにより，境界に近いノードの中継回数を最小限に抑えることができ，最終的に攻撃者に察知される可能性を減らすことが可能となる。

5. まとめ

本研究では，センサネットワークのセキュリティ向上を目的として，センサノードからの電波が領域外へ漏洩することを抑える新たなルーティングアルゴリズムを提案した。また，シミュレーション実験により，既存手法の AODV と比較し，本提案手法の優位性を確認した。

参考文献

[1] Chris Karlof, David Wagner: Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks, pp.293－315 (2003).
[2] H. Luo, P. Zefros, J. Kong, S. Lu, L. Zhang: Self-Securing Ad Hoc Wireless Networks, Proc. of Seventh IEEE Symposium on Computers and Communications (ISCC ’02) (2002).
[3] C.E. Perkins, E.M. Royer, S. Das: Ad Hoc On Demand Distance Vector (AODV) Routing, IETF Internet draft, draft-ietf-manet-aodv-08.txt (2001).