複数ゲートウェイを有する無線センサネットワークにおける能動的攻撃を検知するデータ転送手法について

On the Detection Method of Active Attacks
in Wireless Sensor Networks with Multiple Gateways

越道涼太 [1] 浅井聡太 [2] 河野英太郎 [2] 角田良明 [2]
Ryota Koshimichi Sota Asai Eitaro Kohno Yoshiaki Kakuda

広島市立大学情報科学部 [1]
Faculty of Information Sciences, Hiroshima City University
広島市立大学院情報科学研究科 [2]
Graduate School of Information Sciences, Hiroshima City University

1 はじめに

無線センサネットワーク (以降，WSN) において中継センサ端末 (以降，ノード) またはその周辺のノードによるデータパケットの窃取，盗聴などのセキュリティ上の問題に対し，秘密分散法を用いたセキュア分散データ転送 (以降，セキュア分散データ転送) [1] を利用する複数ゲートウェイ (以降，GW) によるデータ転送手法が提案されている [2](以降，従来法)．この従来法では，各送信元ノードが複数の GW に対し経路の構築を行い，シェアを送信する．しかし，構築した経路上に故障ノードや能動的攻撃をおこなう悪意ノードが同時に存在する場合の回避は想定されていない．本稿では，そうした故障を回避し悪意ノードを検知する経路構築手法を提案する．また，提案手法の効果についてシミュレーション実験により性能を評価する．

2 従来法

2.1 WSN におけるノード故障とセキュリティ

WSN では，各ノードはフィールド内の観測すべき情報を測定するためのデバイスと，データを転送するための無線通信機能を持つ．一般に WSN では対象フィールド内に多数のノードを配置し，一定期間動作するように電池等で駆動される．そのため，各ノードの計算資源やバッテリ容量については，大きな制約がある．したがって，有線のネットワーク接続を行い，電源に常時接続する PC などと比較すると端末の故障，ならびに計算資源を要求する暗号化手法などは適用できない場合がある．また，バッテリ容量の枯渇についても考慮する必要がある．

伝統的に，WSN の多くの研究はノードの大きな制約があるバッテリ容量をいかに節約するかを考えて，様々な手法が提案されてきた．また，文献 [3] では，ノードが転送データを中継する際などに悪意のあるノードや攻撃者によって窃取や盗聴などを行う受動的攻撃や悪意のあるノードがネットワーク内の情報を改竄したり不正な情報を発信する能動的攻撃について述べられている．

2.2 概要

従来法 [2] は複数ゲートウェイとセキュア分散データ転送を用いることでゲートウェイが単一障害点になることと転送データの窃取や盗聴という受動攻撃による脆弱性に対応する手法として提案されている．また，従来法ではノードの観測情報を利用するユーザが，WSN にいることを想定している．従来法では，図 1 に示す通り GW 候補をフィールドに内接する円を分割した扇形の重心に配置する．

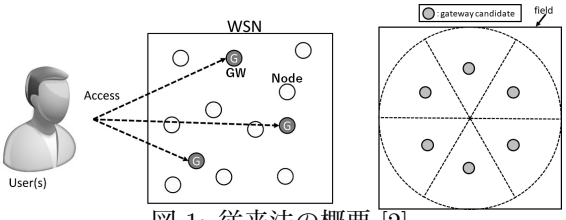

図 1: 従来法の概要 [2]

2.3 従来法の問題点

従来法は，2.1 で述べた問題のうち GW の故障と受動的攻撃を 2.2 で説明した構成法を用いて対応している．しかし，中継ノードの故障やノードの能動的攻撃を行う手法には対応していない．

3 提案法

本稿では，2.1 で挙げられた問題のうち，2.3 で述べた従来法で対応できていない中継ノードの故障とノードこの能動的攻撃に対応するための手法を提案する．提案法は，(1) 既に文献 [4] で述べられた中継ノードの故障に対応する迂回経路作成手法を導入し，(2) ノードの能動的攻撃に対応するため，セキュア分散データ転送で取り入れられている，秘密分散法によるチェックコードの復号化に基づくデータの改竄検知手法を文献 [2] の仕組みで取り扱うための手法を含む．

故障ノード発生時の迂回経路作成法

転送データの中継をノードが行っている際，経路表にある次ホップノードにデータが送信できない場合，従来法にて経路作成を行っている SRIDR[5] と同様の手法を用いて故障ノードを迂回する経路を作成しデータ転送を行う．

中継ノードにおける能動的攻撃対応手法

提案法では，データの転送にセキュア分散データ転送を用いている．そのため，転送すべき暗号化データ (以降　シェア) が改竄されているかどうかはしきい値分のシェアを複数の宛先 GW から入手して復号することで確認できる．もし，転送されたデータに改竄が認められた場合，送信元ノードと GW 間の元の経路とは異なる代替経路を改めて再構成しデータ転送を行う．そのために宛先 GW から送信元ノードに代替経路作成指示のための制御メッセージを導入し，代替経路が再構築され正しいデータが転送されるまで，次のデータ転送を待機させる．

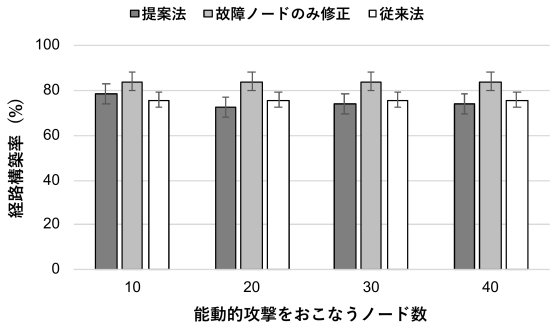

図 2: 経路構築率

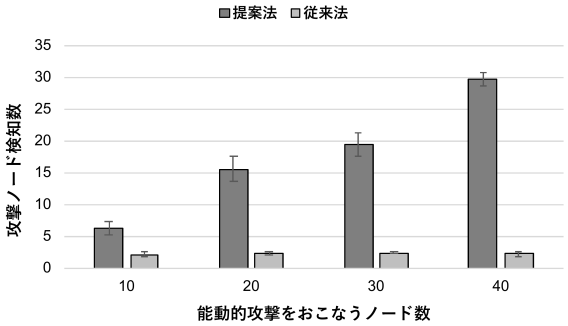

図 3: 攻撃ノード検知数

4　シミュレーション実験

4.1　実験概要

提案法をシミュレータ，QualNet ver 5.0[6] に実装し，シミュレーション実験により，転送データを改竄し能動的攻撃をおこなうノード (以降，攻撃ノード) がある場合の攻撃ノード検知数を測定した．実験環境は次の通りである．攻撃ノード数を 10，20，30，40，送受信ペア数を 10 組，各送信元ノードからのデータ数を 10 とし，故障ノード数を 10 とした．また，無線 LAN の規格は IEEE.802.11b を使用し，最大通信帯域を 11[Mbps]，ノード数を 400 とし各故障ノード数ごとに 50 回試行した．GW 候補の配置数は 6 として，GW グループは 3 つの GW で構成した．なお，セキュア分散データ転送のパラメータはシェア数を 3，しきい値を 2 とした．

また送信元ノードと GW 間の経路構築には整数倍程度の時間がかかるため，各送信元ノードのシェアの送信間隔は提案法が 3[s], 従来法が 1[s] となっている．

実験ではシェアの送信中に経路のノードが故障することを想定しており，ある送信元ノードのシェアの送信開始から 1[s] 後に故障ノードを発生させる．1 つの送信元ノードからのシェアの送信が終了後，故障ノードを復帰させ，次の送信元ノードでも同様に動作する．このようにして，シェアの送信中のみ故障ノードを発生させる．また，攻撃ノードは常に転送データを改竄する．また，送信元ノードと GW グループの間で必要な経路が 2 本以上構築された場合，1 組の送受信ペア間で経路が構築できたとする．比較項目として，経路構築率と攻撃ノード検知数を測定した．比較項目の定義はそれぞれ次の通りである．

経路構築率

ある送信元ノードと GW グループとの間で必要とされる経路が構築される割合

攻撃ノード検知数

各手法によって経路上に攻撃ノードが検知できた試行回数

4.2　実験結果

図 2 にノード数 400 の経路構築率を，図 3 にノード数 400 のデータ到達率を示す．図 2 中のエラーバーはいずれも 95% 信頼区間を示す．

実験結果より，従来法の攻撃ノード検知数は攻撃ノードの数によらずほとんど一定であるが，提案法の攻撃ノード検知数は一定でなく，シェアの改竄に対して検知できていることがわかる．また，提案法の攻撃ノード検知数は攻撃ノードの増加に伴い増加している．なお現状では提案法の経路構築率の低下について，攻撃ノードを検知した際に送信元ノードから代替経路を構築するため，その構築に時間がかかる場合があり失敗することが原因である．

5　まとめ

本研究では，複数 GW を持つ WSN においてセキュア分散データ転送を用いる際に，故障ノードと攻撃ノードに対する経路再構築法を提案し，その効果について実験により評価した．実験結果より，提案法は故障ノードや攻撃ノードを検知できることを確認した．今後の課題としては，経路構築率などを向上させる手法の開発がある．

謝辞

本研究の一部は日本学術振興会科学研究費補助金（基盤研究（C）課題番号 17K00130, 17K00131, 20K11775）のもとに実施したものである．ここに記して謝意を表す．

参考文献

[1] E.Kohno et al., ‘‘Improvement of dependability against node capture attacks for wireless sensor networks,” IEICE Transactions on Information and Systems, vol.E94-D, no.1, pp.19-26, Jan. 2011.

[2] 藤田，谷 他, “セキュア分散データ転送を用いる無線センサネットワークにおける経路構築率向上のための複数ゲートウェイの配置法ならびに経路制御手法，” 電子情報通信学会論文誌 B, vol.J102-B, no.8, pp.545-554, Aug. 2019.

[3] P.Sakarindr et al.,“Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks,” IEEE Wireless Communications, vol.14, no.5, pp.8–20, 2007.

[4] 浅井 他, ”複数ゲートウェイを持つセキュア分散データ転送を用いる無線センサネットワークにおける故障ノード発生時の経路再構築手法,” 2020 年電子情報通信学会総合大会, BS-2-9, Mar. 2020.

[5] T.Okazaki et al., “Improvement of assurance for wireless sensor networks using packet detouring and dispersed data transmission,” Proc. iThings/CPSCom 2011, pp.144-151, Oct. 2011.

[6] Scalable Network Technologies Inc., “Qualnet network simulator by scalable network technologies,” http://www.scalable-networks.com/.