無線センサネットワークにおける近隣信用度を用いた統計的経路フィルタリングに関する一考察

渡邊 裕司† 田村 知嗣†

†名古屋市立大学大学院システム自然科学研究科
467-8501 愛知県名古屋市瑞穂区瑞穂町山の畑 1
yuji@nsc.nagoya-cu.ac.jp

あらまし 無線センサネットワークにおいて攻撃者が危殆化ノードを用いて偽イベントを送信する偽造データ挿入攻撃に対して，統計的経路フィルタリングでは，大規模ネットワークにおけるノードの高密度配置を仮定し，基地局に届く前の転送段階で偽造データを確率的に破棄する．筆者らは，既存手法に対して，各転送ノードにその近隣ノードに対する「信用度」パラメータを導入し，偽造データのより早い転送段階での破棄を計ってきた。本論文では，より実用的な環境でシミュレーションを行い，提案手法が既存手法より短い転送段階で偽造データを破棄できる一方で提案手法の問題点を確認した．

A study of statistical en-route filtering using neighbors credibility in wireless sensor networks

Yuji Watanabe† Tomotsugu Tamura‡

†Graduate School of Natural Sciences, Nagoya City University
1 Yamanohata, Mizuho-cho, Mizuho-ku, Nagoya 467-8501, JAPAN
yuji@nsc.nagoya-cu.ac.jp

Abstract In wireless sensor networks, attackers can compromise sensor nodes and then inject false data reports of bogus events using the compromised nodes. To overcome such attacks called false data injection attack, the statistical en-route filtering scheme can probabilistically filter out false reports en-route. In our previous studies, we proposed an immunity-based approach, where each node assigns credibility to its neighboring nodes, to achieve earlier detection of false reports. In this paper, simulation result in more practical environment showed that our scheme outperformed the original one, but .it had a problem that the performance of our scheme declines.

1 はじめに

多数の小型で安価なセンサノードからなる無線センサネットワークは，攻撃者が様々な脅威を与えうる潜在的に敵意ある環境に配備されうる．例えば，攻撃者はセンサノードを不正に取得することで通信に使われるアルゴリズムや鍵などのセキュリティ情報を入手し，その乗っ取った危殆化ノードを使って偽のイベントデータを基地局に向けて送信することができる．この攻撃は「偽造データ挿入攻撃（False Data Injection Attack）」と呼ばれ

[1]，誤報を引き起こすだけでなく，基地局にデータを転送する中間ノードのエネルギーも浪費させる．

この攻撃への対策として，統計的経路フィルタリング(Statistical En-route Filtering, 以下 SEF と略す) [2]と多くの改良手法[1, 3-9]が提案されている．SEF では，大規模センサネットワークにおけるセンサノードの高密度配置を仮定し，イベントを検出した複数ノードによる集合的合議と転送ノードによる分散的検出によって，基地局に届く前の転送段階で偽造データを破棄する．

筆者らも「免疫型統計的経路フィルタリング(Immunity-based SEF, 以下 ImSEF と略す)」と呼ばれる改良手法を提案した[10]．本手法では，免疫細胞の相互作用から着想を得た免疫型診断モデル[11]で使われたノードの「信用度」というパラメータを使用する．具体的には，各ノードが近隣ノードに対して信用度を割り当て，経路フィルタリングと通信の成否をもとに信用度を更新し，さらに更新された信用度を次回通信時の受信確率として使用する．シミュレーションおよび数学的解析により，転送経路上において ImSEF が偽造データをより早い段階で破棄できることを確認した[12]．しかし，環境設定が危殆化ノードだけからの単一転送ルートであり，より実用的な環境でのシミュレーションが必要であった．

そこで本論文では，複数の転送ルートがあり，正当データと偽造データが混在する環境での追加シミュレーションを行う．その結果，文献[12]と同様に提案手法が既存手法より短い転送段階で偽造データを破棄できることを確認した．その一方で提案手法の性能の悪化も観測された．

2 関連研究

ノード間のメッセージ認証によって，ネットワーク内のセキュリティメカニズムを知らない外部攻撃者によるなりすましや偽造データを防ぐことは可能である．しかし，通信のアルゴリズムや鍵を不正取得された内部の危殆化ノードによる攻撃は防御できない．そこで，危殆化ノードからの偽造データを検出・破棄するために，統計的経路フィルタリング SEF[2]と多くの改良手法[1, 3-9]が提案されている．SEF では，大規模ネットワークにおけるノードの高密度配置を仮定し，同一イベントを検出した複数ノードによる集合的合議と転送ノードによる分散的検出によって，基地局に届く前の転送段階で偽造データを確率的に破棄する．SEF は，センサの有限な計算や通信コストを無駄に消費することなく，早い段階で偽造データを検出できる．SEF の改良手法として，センサネットワークの動的なトポロジーに対処できる動的経路フィルタリング[3]や正当データを転送しない非検知攻撃（False Negative Attack）を扱ったマルチパス経路フィルタリング[4]などがある．SEF も含めてこれらの手法は，各ノードに対して鍵をランダムに配備するランダム鍵配備方式であるため，攻撃者があるしきい値 T 個以上の鍵を不正入手した場合，経路上では偽造データを検出できない．そこで，地理制約鍵配備方式[5-8]や固定パス鍵配備方式[1, 9]などが提案され，T 個以上の鍵が流出しても偽のイベントの発生地点を狭い領域に限定することができる．

これらの既存研究では，偽造データを送信する危殆化ノードの特定までは行っていない．もし危殆化ノードをうまく特定できれば，その近隣ノードがより早い段階で偽造データを検出できる．最も簡単な方法として，偽造データがたどった経路をトレースバックすることが挙げられる．しかし，危殆化ノードは，ネットワーク内のセキュリティメカニズムを知っているため，トレースバックの問い合わせに対して嘘の証言（例えば偽造データは自分からではなく別のノードから送信されてきた）をすることができ，危殆化ノードを特定できない．

一方，ネットワーク上の異常ノードの検出

方法として，免疫型診断モデル[11]は一つの見込みのあるアプローチである．この診断モデルでは，各ノードは近隣ノードと相互にテストし，そのテスト結果をもとに各ノードは自分の「信用度」を更新して正常・異常を判定する．しかし，危殆化ノードは，偽のテスト結果を出力するだけでなく，でたらめに自分の信用度を更新するかもしれない．そこで筆者らは，各ノードが自分ではなく近隣ノードに対して信用度を割り当てた免疫型統計的経路フィルタリング ImSEF を考案した[10]．次節以降では，想定環境と ImSEF について詳しく説明する．

3 想定環境

3.1 センサネットワークのモデル

本研究では，既存研究と同様に，多数の小型センサノードが高密度かつ広範囲に配備され，1 台の基地局（Base Station，以下 BS と略す）によって管理されるセンサネットワークを想定する．高密度な配置により，複数ノードが 1 つのイベントを検知できるとする．これは，複数センサが協調することで検知精度を高めるためや，ノードの故障にも対応するために必要である．しかし，イベントを検知した複数ノードそれぞれがイベントデータを基地局に向けて送ることは無駄であるため，検知したノード群からクラスターヘッド（Cluster Head，以下 CH と略す）を選出する．CH は，周囲ノードの検知データを集めて要約したイベントレポートを BS に向けて送信する．一方，広範囲な配置により，イベントレポートはいくつかの転送ノードを経由するマルチホップ通信によって BS まで届けられるとする．

3.2 攻撃モデル

攻撃者は，1 個以上のノードを物理的または遠隔操作で乗っ取ることによって，そのノードに含まれている秘密鍵や使用アルゴリズムなどのセキュリティ情報を不正入手できるとする．攻撃者は，この乗っ取った危殆化ノードを使って実在しない偽造イベントレポートを BS に向けて送信することができる．この偽造データは，誤報をもたらすだけでなく，転送ノードの限られたエネルギーを浪費させる．また，多くの偽造データにより正当データの送信が妨げられることにもなる．なお，BS は，センサノードと異なり，高度なセキュリティを有するため，攻撃者による BS への攻撃は困難であるとする．また，危殆化ノードによる他の攻撃（正当データの破棄や Dos 攻撃など）は，ここでは取り上げない．

4 免疫型統計的経路フィルタリング ImSEF

SEF および ImSEF は，3.1 節で想定するセンサネットワークにおいて複数の検出ノードによる集合的合議と転送ノードによる分散的検出によって転送段階で偽造データを確率的に破棄する．SEF は，三つの主要要素(1)鍵の割り当てとレポート生成，(2)経路フィルタリング，(3)BS での検証から成る．さらに ImSEF では，信用度更新と信用度に基づく通信が追加される．以下の各節でその要素を詳述する．

4.1 鍵の割り当てとレポート生成

鍵の割り当てとレポート生成は，次の手順である．

1) BS は N 個の秘密鍵のプール $\{K_i, 0 \le i \le N-1\}$ を保持し，その鍵プールは重複しない n 個のパーティションに分割される．各パーティションには m 個の鍵があるとする（つまり $N = n\,m$）．鍵プールの単純な分割方法は，$P_j = \{K_i | jm \le i \le (j+1)m - 1\}$ である．
2) 各センサノードは，配備される前に，鍵プールからランダムに 1 つのパーテ

ィションを選び，そのパーティションからランダムに選んだk個（$k<m$）の鍵を格納する．

3) 全ノードは配備後に1ホップ内の近隣ノードに自身の ID をブロードキャストする．そのメッセージを受け取った各ノードは，近隣ノードのリストを作成し，各近隣ノードに対して近隣信用度$R(t) \in [0,1]$を割り当てる．各信用度の初期値 $R(0)$は1とする．

4) あるイベントが発生すると，複数の周辺ノードがそのイベントを検出し，検出したノード群から CH を選出する．

5) 各検出ノードは，イベントレポート E と格納されている k 個の鍵からランダムに選ばれた1つの鍵 K_i を用いて，メッセージ認証コード（Message Authentication Code: MAC）M_i を生成する．そして各検出ノードは，使用した鍵のインデックスと生成された MAC の対$\{i, M_i\}$を CH に送る．鍵 K_i は秘匿であり，M_i は公開である．

6) CH は，全ての検出ノードから$\{i, M_i\}$を収集し，その中から異なるパーティションに属する鍵から作られた T 個の MAC を選ぶ．そして CH は，$\{E, i_1, M_{i1}, i_2, M_{i2}, \ldots, i_T, M_{iT}\}$のようにイベントレポート E に T 個の鍵のインデックスと T 個の MAC をつけて，BS に向けて送信する．T 個の MAC から成るこの集合がイベントレポートの正当さを示す証拠として働く．

図1に SEF および ImSEF における鍵の割り当てとレポート生成の具体例を示す．同図において，BS は $N=12$ 個の鍵のプールを保持し，鍵プールはそれぞれ $m=3$ 個の鍵から成る $n=4$ 個のパーティションに分割されている．各ノードは，鍵プールの任意の1つのパーティションから $k=2$ 個の秘密鍵をランダムに選ぶ．そしてイベントが起こると，例えば秘密鍵 K_1 と K_2 を格納するノードは，イベントレポート E と鍵の1つ K_2 を用いて M_2 を作成する．CH は，自分を含めて4個の検出ノードから鍵のインデックスと MAC の対を集めて，その中から $T=3$ 個の MAC としてランダムに M_2, M_9, M_{10} を選ぶ．ただし，3 個の MAC のパーティションは異ならなければならないため，同じパーティションに属する鍵から生成された M_7 と M_9 はどちらかが選ばれる．最後に CH はイベントレポート E に3個の鍵のインデックスと3個の MAC をつけて送信する．

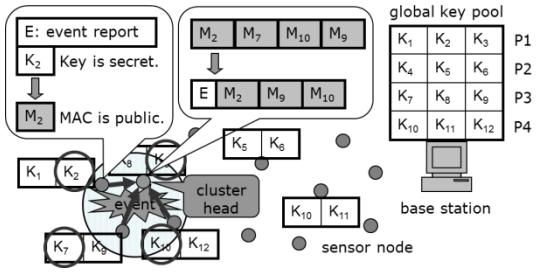


図1:SEF および ImSEF における鍵の割り当てとレポート生成の例[10]

4.2 経路フィルタリングと信用度更新

経路フィルタリングでは，中間の転送ノードがレポートに付属の MAC の正しさを確率的に検証し，偽造された MAC を持つレポートを破棄する．さらに ImSEF では，信用度更新と信用度に基づく通信も実行される．具体的には以下の手順で行われる．

1) 転送ノード j は，送信元の近隣ノード i からのレポートを信用度 $R_{ji}(t)$ に比例して受信する．換言すれば，ノード j は，ノード i からのレポートを確率 $(1 - R_{ji}(t))$ で無条件で破棄し，フィルタリング処理を終了する．

2) 正当レポートは異なるパーティションの T 個の鍵で作成されたちょうど T 個の MAC を持っているため，T 個未満の MAC しかないイベントレポートや同じパーティションから2個以上の鍵が使われたレポートは破棄される．もしノード i から受信したノード j が上記理由でレポートを破棄したら，ノード i

の信用度 $R_{ji}(t)$を減らし，フィルタリングを終了する．

3) ランダムな鍵の割り当てのため，転送ノード j は，レポートに含まれる鍵のインデックスが示す鍵と同じものをある確率で格納しうる．そこで，ノード j はレポートに付属の T 個の鍵のインデックスを調べ，同じ鍵を持っている場合は，イベントレポート E と格納している秘密鍵から MAC を再生成し，その MAC とレポートにつけられた MAC を比較する．もし再生成された MAC とレポートに添付された MAC が異なれば，そのレポートを破棄し，転送元のノード i の信用度 $R_{ji}(t)$を減らし，フィルタリングを終了する．

4) 手順3)で再生成したMACがレポートのMAC と一致した場合あるいはノード j が T 個の鍵のどれも持っていない場合，次のノード k にレポートを転送し，レポートを受理し転送したという返答メッセージを転送元ノード i に送る．ただし，ノード j がレポートを破棄した場合には，ノード i に返答しない．

5) ノード j は転送先ノード k からの返答を待ち，もし返答があれば転送元ノード i の信用度 $R_{ji}(t)$を増やし，返答がなければ $R_{ji}(t)$を減らす．

信用度更新をまとめると，ノード j は転送元ノード i のステップ t での信用度 $R_{ji}(t)$を，(1)自身が行ったフィルタリングの結果と(2)転送先ノード k からの返答の有無によって以下のように更新する：

$$R_{ji}(t+1) = \begin{cases} R_{ji}(t) + \Delta_s & \text{if node } j \text{ receives the reply from next node } k \\ R_{ji}(t) - \Delta_f & \text{if node } j \text{ does not receives the reply from next node } k \\ R_{ji}(t) - \Delta_d & \text{if node } j \text{ drops the report} \end{cases}$$

もし $R_{ji}(t)$が 1 を超えた（0 を下回った）ときは 1(0)とする．上式のパラメータ Δ_s，Δ_f，Δ_d の値は，数学的解析やシミュレーションによって決める必要がある．

例えば図 2 において，ノード i は，転送先の近隣ノード j から返答を受け取っているため，転送元の近隣ノード h の信用度 R_{ih} を増やす．しかし，ノード j は，転送先ノード k がレポート破棄により返答をしなかったため，転送元ノード i の信用度 R_{ji} を減らす．ノード k は，自身がレポートを破棄したため，転送元ノード j の信用度 R_{kj} を減らす．

信用度の更新だけでは，危殆化ノードにより近い転送段階での破棄ができない．例えば図 2 でもしノード h が危殆化されているとすると，このノードからの偽造レポートはノード k まで転送され続ける．そこで経路フィルタリングの手順 1)で述べた信用度に基づく通信が重要となる．先の例において，ノード i は，次回通信時には信用度 R_{ih} の増加により，危殆化ノード h から逆により高い確率で偽造レポートを受信してしまう．しかし，信用度 R_{ji}の減少によりノード j がノード i から受信する確率が低くなるため，次回通信時にはノード i とノード j の通信が失敗するかもしれない．その場合，ノード j からの返答がないため，ノード i は転送元の危殆化ノード h の信用度 R_{ih} を減らすことにつながる．なお，減らしてしまった信用度 R_{ji} と R_{kj} は，危殆化ノード以外の近隣ノードからの正当レポートを転送することによって回復することができる．このように信用度更新と信用度に基づく通信を繰り返すことによって，ImSEF では危殆化ノードの近隣ノードがより早い段階で偽造データを破棄できることが期待される．

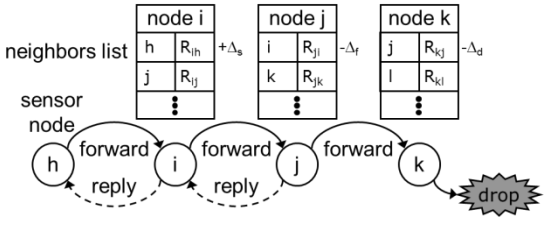


図 2：ImSEF における信用度更新の例[10]

4.3　BS での検証

上述の検出メカニズムは確率的であるため，不正 MAC を持つ偽造レポートのいくつかは，経路フィルタリングをすり抜けて，BS に達するかもしれない．しかし，BS には全ての秘密鍵が保持されているため，BS での最終検証として，レポート内の全 MAC の正しさを検証して，経路フィルタリングをすり抜けた偽造レポートを破棄する．

5　シミュレーション

文献[12]における ImSEF のシミュレーションおよび数学的解析においては，既存研究にならったシミュレーション環境としたが，攻撃者がイベント付近のノードを乗っ取り，1000 個の偽造レポートを単一転送ルートで送信した場合の結果であった．より実用的な環境として，複数の転送ルートがあり，正当レポートと偽造レポートが混在する場合を調べる必要がある．

そこで，図 4 に示すような 9×100 個のノードが配備された 2 次元格子フィールドでシミュレーションを行う．BS と 9 個のデータ発生ノードはフィールドの両端にあり，それらの間には 100 ホップある．そして，データ発生ノードの一つが危殆化され 1000 個の偽造レポートを複数のルートへ向けて送信し，残りの8個はそれぞれ1000個の正当レポートを送信する（文献[12]ではデータ発生ノードは危殆化ノードだけ）．他の設定条件は文献[12]と同じとした．つまりBS は 1000 個の秘密鍵のプールを保持し，その鍵プールは 10 個のパーティションに分割され，各パーティションには 100 個の鍵があるとする．また，各ノードには 50 個の鍵を格納し，イベントレポートには 5 個の MAC を添付する．さらに ImSEF の Δ_s，Δ_f，Δ_dは 0.02 とする．

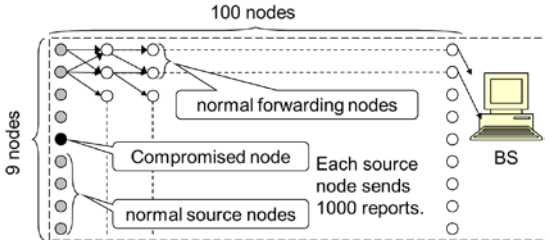
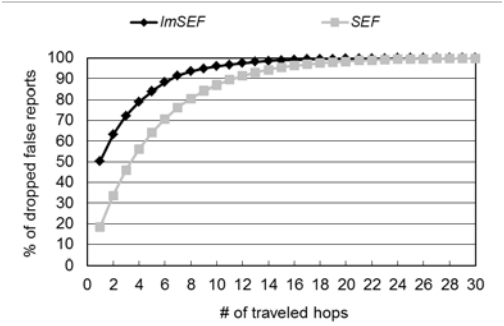
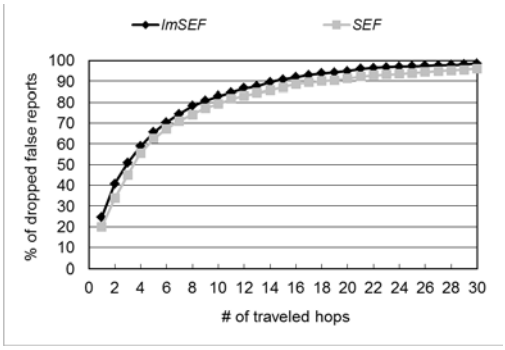


図 4：シミュレーション環境

図 5 の(a)に文献[12]の ImSEF と SEF の比較結果，(b)に今回の環境における結果を示す．同図において，横軸はレポートが転送されたホップ数，縦軸は破棄された偽造レポートの割合である．結果からレポートが転送されるにつれて，より多くの偽造レポートが検知されて棄却される．図 5 の(a)において，両手法とも 20 個のノードを経由すれば，ほぼ 100%の偽造ノードが破棄される．さらに，5 個の転送ノードによって SEF では約 64%の偽造レポートが検知されるのに対して，免疫的アプローチでは約 84%が破棄される．つまり，ImSEF が SEF よりも早い段階で偽造データを破棄できることを確認できる．一方，図 5 の(b)では，両手法とも偽造レポートの破棄率が悪くなり，特に ImSEF での悪化が顕著である．5 個の転送ノードによる破棄率は，SEF では約 63%，ImSEF では約 66%である．これは，複数ルートでそれぞれ信用度を更新する必要があるため，信用度更新が十分に行われていないと考えられる．しかし，若干ではあるもののより実用的な環境でも ImSEF が SEF よりも早い段階で偽造データを破棄できるといえる．



(a) 文献[12]の結果



(b) 図 4 の環境における結果

図 5: シミュレーション結果

6 おわりに

本論文では，無線センサネットワークにおける偽造データ挿入攻撃に対して，筆者らが提案してきた免疫型統計的経路フィルタリングの性能をより実用的な環境で評価した．その結果，よりも早い段階で偽造データを破棄できることが確認できたものの，性能の悪化も観測された．今後は，今回の結果の詳細な解析を行い，信用度更新の改良を検討する必要がある．

謝辞 本研究の一部は，科研費基盤研究(C)(22500063)の支援を受けて行われた．

参考文献

[1] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks,” *IEEE Symposium on Security and Privacy*, pp.259-271, 2004.

[2] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical En-Route Filtering of Injected False Data in Sensor Networks,” *IEEE Journal on Selected Areas in Communications*, 23(4), pp.839-850, 2005.

[3] Z. Yu and Y. Guan, “A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks,” *Proceedings of the 25th IEEE Conference on Computer Communications (INFOCOM)*, pp.1-12, 2006.

[4] M. S. Kim and T. H. Cho, “A Multipath En-Route Filtering Method for Dropping Reports in Sensor Networks,” *IEICE Transactions on Information and Systems*, E90-D(12), pp.2108-2109, 2007.

[5] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, “Toward Resilient Security in Wireless Sensor Networks,” *ACM MobiHoc*, pp.34-45, 2005.

[6] F. Li and J. Wu, “A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks,” *Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing (IWCMC)*, pp.27-32, 2006.

[7] K. Ren, W. Lou, and Y. Zhang, “LEDS: Providing Location-aware End-to-end Data Security in Wireless Sensor Networks,” *IEEE Transactions on Mobile Computing*, 7(5), pp.585-598, 2008.

[8] 清雄一，本位田真一，“多数のノード取得攻撃に対応した無線センサネットワークにおける不正イベントの検知”，信学論 B

J92-B(4), pp.678-688, 2009.

[9] C. Krauß, M. Schneider, K. Bayarou, and C. Eckert, "STEF: A Secure Ticket-Based En-route Filtering Scheme for Wireless Sensor Networks," *2nd IEEE International Conference on Availability, Reliability and Security (ARES)*, pp.310-317 2007.

[10] Y. Watanabe, "An Immunity-based Scheme for Statistical En-route Filtering in Wireless Sensor Networks," *Knowledge-Based Intelligent Information and Engineering Systems, LNCS* 6278, pp.660-665, 2010.

[11] Y. Ishida, "Fully Distributed Diagnosis by PDP Learning Algorithm: Towards Immune Network PDP Model," *Proceedings of International Joint Conference on Neural Networks (IJCNN)*, pp.777-782, 1990.

[12] Y. Watanabe, "An Analysis of Immunity-based Statistical En-route Filtering in Wireless Sensor Networks," The International Conference on Management of Emergent Digital EcoSystems (MEDES'11), pp.250-256, 2011.