L-029

無線センサネットワークにおける免疫型統計的経路フィルタリングの高性能シミュレーターによる一検証

A Verification of Immunity-based Statistical En-route Filtering Using High-Performance Simulator in Wireless Sensor Networks

渡邊 裕司† 徐 英†
Yuji Watanabe Jyoei

1. はじめに

多く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において，攻撃者は容易にノードを乗っ取り，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不正入手することができる．そして，その乗っ取った危殆化ノードを用いて偽イベントを基地局に向けて送信することもできる．この攻撃は「偽造データ挿入攻撃」と呼ばれ，誤報をもたらすだけでなく，基地局にデータを転送する中間ノードのエネルギーを浪費させ，正当レポートの送信を妨げることにつながる．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: SEF）[1]と多くの改良手法が提案されている．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確率的に破棄する．

筆者らも，石田の免疫型診断モデル[2]で使用されたノードの「信用度」というパラメータを導入して，「免疫型統計的経路フィルタリング（Immunity-based SEF: ImSEF）」と呼ばれる改良手法を提案した[3]．提案手法では，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，ImSEF が SEF より早い転送段階で偽造データを破棄できることを確認した[4]．しかし，環境設定を危殆化ノードだけからの単一転送ルートとして自作シミュレーターで検証した．本提案手法で受信確率として用いる信用度により正当レポートが破棄されうるため，正当レポートと偽造レポートが混在するより実用的な環境でのシミュレーションが必要である．

本報告では，より実用的な環境を模した Scalable Network Technologies 社の高性能シミュレーターQualNet[5]を用いて提案手法の利点・欠点について検証する．

2. 想定環境

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: BS）によって管理されるセンサネットワークを想定する．高密度配置により，複数ノードが同一イベントを検出できる．これは，複数センサが協調して検出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，イベントを検出した複数ノードそれぞれがイベントデータを BS に向けて送ることは無駄であるため，検出したノード群からクラスターヘッド（Cluster Head: CH）を選出する．CH は，周囲ノードの検出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，その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．

一方，想定する攻撃者は，複数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る秘密鍵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．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．

3. 免疫型統計的経路フィルタリング ImSEF [3]

SEF および ImSEF は，前節の想定環境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しく説明する．

3.1 鍵の割り当てとレポート生成

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) 各ノードは，配備前に，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．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，そのイベントを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．

†名古屋市立大学システム自然科学研究科，Graduate School of Natural Sciences, Nagoya City University

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．

3.2 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Δ_dだけ減らし，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 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Δ_dだけ減らし，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Δ_sだけ増やし，返答がなければ $R_{ji}(t)$をΔ_fだけ減らす．

3.3 BS での検証

上述の検証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．

4. シミュレーション

3.2 節の手順 1)で述べたように信用度が受信確率として用いられるため，転送元ノードが危殆化ノードではなく単に偽造レポートを転送しているだけの正常ノードであった場合，その転送元からの正当レポートまでも破棄される恐れがある．より実用的な環境として，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，ZigBee に準拠した無線センサネットワークの高性能シミュレーションが行える QualNet[5]を用いてシナリオ作成を行った．まず ZigBee のため，物理層と MAC 層は IEEE 802.15.4 の規定に従い，2.4GHz で通信速度 250Kbps であり，ルーティングプロトコルは AODV（Ad hoc On-Demand Distance Vector）である．100 m×100 m のフィールドに 500 個のセンサノードを配備し，フィールド中央に BS を置く．データ発生ノードはランダムに選択されて，1000 個の正当レポートを 2 秒間隔で BS に向けて送信する．データ発生ノードのいくつかは乗っ取られて偽造レポート 1000 個を送信するとする．他の設定条件は文献[4]と同じとする．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，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．

まず偽造レポートに関して，文献[4]と同様にして，レポートが転送されたホップ数に対して破棄された偽造レポートの割合を調べたところ，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出され棄却された．20 個の転送ノードを経由すればほぼ 100%の偽造レポートが破棄される．また，ImSEF が SEF よりも早い段階で偽造データを破棄できることも確認した．一方，正当レポートが提案手法によって誤って破棄される割合は，正当レポートの発信源が危殆化ノードに近いかどうかに依存する．例えば，危殆化ノードのすぐ近くのノードから発信された 1000 個の正当レポートのうち，14 個が誤って破棄された（破棄率 1.4%）．現在これらの結果の解析を進めており，詳細な結果は発表時に報告予定である．

5. おわりに

本報告では，より実用的な環境を模した高性能シミュレーターを用いて提案手法の利点・欠点について検証した．

謝辞

本研究の一部は，科研費基盤研究(C) (22500063)および名古屋市立大学の平成 24 年度後期研究支援員制度の支援を受けて行われた．

参考文献

[1] 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, Vol.23, No.4, pp.839-850 (2005).
[2] Y. Ishida, “Fully Distributed Diagnosis by PDP Learning Algorithm: Towards Immune Network PDP Model,” Proceedings of International Joint Conference on Neural Networks, pp.777-782 (1990).
[3] 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).
[4] Y. Watanabe, “An Analysis of Immunity-based Statistical En-route Filtering in Wireless Sensor Networks,” The International Conference on Management of Emergent Digital EcoSystems, pp.250-256 (2011).
[5] QualNet, http://web.scalable-networks.com/content/qualnet