様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　６月１１日現在

機関番号：23903
研究種目：基盤研究（Ｃ）
研究期間：2010～2012
課題番号：22500063
研究課題名（和文）　免疫系に学んだモバイルセンサネットワークにおける異常検出・修復の研究
研究課題名（英文）　Anomaly Detection and Repair on Mobile Sensor Networks Using Immunity-based System
研究代表者
渡邊　裕司（WATANABE　YUJI）
名古屋市立大学・システム自然科学研究科・准教授
研究者番号：60314100

研究成果の概要（和文）：本研究では、無線センサネットワークにおいて免疫型システムの導入により効率的な異常検出とノード修復を目指す。そこで、各センサノードに近隣ノードに対する「信用度」変数を導入し、フィルタリングと通信の成否により更新された信用度を通信確率として用いる免疫型統計的経路フィルタリングを提案した。シミュレーション及び数学的解析により、提案手法が既存手法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。

研究成果の概要（英文）：The aim of this study is more efficient anomaly detection and node repair on wireless sensor network using an immunity-based system. We have proposed an immunity-based statistical en-route filtering, where each node assigns credibility to its neighboring nodes, updates the credibility based on the success or failure of filtering and communication, and then uses the updated credibility as the probability of the next communication. Simulation results and mathematical analysis showed that the proposed scheme could achieve earlier detection of false data than the original one.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	900,000	270,000	1,170,000
2011 年度	1,500,000	450,000	1,950,000
2012 年度	1,400,000	420,000	1,820,000
年度			
年度			
総　計	3,800,000	1,140,000	4,940,000

研究分野：知能情報学、情報ネットワーク
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：センサネットワーク、免疫型システム、統計的経路上フィルタリング、偽造データ送出攻撃、ノード修復

１．研究開始当初の背景

(1) 近年、活発な研究が行われている「無線センサネットワーク」において、センサノードに移動機能を付加した「モバイルセンサネットワーク」の研究分野がある。代表的な研究として南カリフォルニア大学のチームよる「Robomote」があり、動的配置、適応的サンプリング、ネットワーク修復などの利点が挙げられ、そのいくつかは実際に実験で示されている。最近の論文として Fagiolini らによるセンシング範囲を最適化する分散配置などはあるものの、異常検出や修復も含めてモバイルセンサネットワークにおけるセキュリティに関する研究はまだ乏しい。

(2) 一方、移動ノードを含まない静的なセン

サネットワークにおけるセキュリティに関しては、暗号化、公開鍵、メッセージ認証など数多くの研究が存在する。しかし、ほとんどの研究はいかに外部の攻撃者からネットワークを守るかを問題としている。これに対して、Ye らによる「統計的経路上フィルタリング」は、攻撃された後の内部の改ざんノードが送出する異常データを検出・破棄する。この手法では、基地局が全ての鍵のプールを持つ一方で各ノードは鍵の一部を所持し、異常データの転送過程において同じ鍵を有するノードによって異常データを破棄する。最近の論文としてファジィルールを用いた適応的鍵分割などはあるものの、このフィルタリングをモバイルセンサネットワークに適用した事例はまだ見当たらない。また、異常データの発信元である改ざんノードの検出・修復方法には触れられていない。

(3) 本研究者は、これまでに若手研究(B)や基盤研究(B)などで「免疫型診断モデル」に関する研究に携わった。この診断モデルは、免疫系の B 細胞間の相互認識のネットワークから着想を得たものであり、相互にテストしうるノードからなるシステムに対して、そのテスト結果ならびにノードの活性・非活性をもとに、ダイナミカルモデルによって各ノードの正常・異常を判定する。しかし、このモデルは相互診断によって異常ノードを検出するのみであり、異常ノードによる異常データのばら撒きは考慮していない。さらに、異常検出後の修復方法も検討課題である。

２．研究の目的

本研究では、これまで得られた免疫型診断モデルに関する多くの成果研究業績も踏まえて、未解決のモバイルセンサネットワークにおける以下の 2 課題に取り組む。

- 診断モデルとフィルタリングを組み合わせることでより効率的な異常検出が可能か？
- 異常検出後に故障センサや改ざんセンサをいかに修復するか？

具体的には、まずモバイルセンサネットワークに対して統計的経路上フィルタリングだけを適用し、異常データの検出率を調べる。そして、このフィルタリングと免疫型診断モデルを相補的に用いることにより、異常データ及び異常ノードの両方をより効率的に検出することを目指す。ここでは、鍵の個数と分割方法、移動ノードの割合と移動戦略も変更しながら検出性能を調べる。

次に、検出した故障ノードや改ざんノードに対して、移動ノードによってどれだけ修復できるかを明らかにする。故障ノードに対しては、移動ノードが代替することでセンシング領域を回復するが、その置換によって移動ノード自体のセンシング範囲がカバーされなくなるために、他の移動ノードとの協調によって適応的配置を行う免疫的手法を提案し、Fagiolini らなどの既存手法と比較する。一方、改ざんノードに対しては、改ざんされた鍵を移動ノードの鍵で書き換えることによって復旧する。ただし、移動ノードが改ざんされた場合、移動ノードの上書きによって逆に改ざんノードが増えるという「諸刃の剣」の側面があり、そのトレードオフとなる点も探る。

３．研究の方法

(1) 想定環境

まずは本研究で想定する環境を明確にしておく必要がある。センサネットワークのモデルとして、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環境を想定する。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。

攻撃モデルとして、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、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。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。

(2) 免疫型統計的経路フィルタリング

Ye らによる「統計的経路上フィルタリング」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、③BS での検証から成る。さらに本研究で提案する免

疫型統計的経路フィルタリングでは、信用度更新と信用度に基づく通信が追加される。以下の①～③でその要素を詳述する。

①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、$\{E,\ i_1,\ M_{i1},\ i_2,\ M_{i2},\ \cdots,\ i_T,\ M_{iT}\}$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。

②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。さらに提案手法では、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：

$$R_{ij}(t+1) = \begin{cases} R_{ij}(t) + \Delta s & \text{ノード}k\text{から返答あり} \\ R_{ij}(t) - \Delta f & \text{ノード}k\text{から返答なし} \\ R_{ij}(t) - \Delta d & \text{ノード}j\text{が破棄} \end{cases}$$

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。なお、上式のパラメータΔs、Δf、Δd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。

③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。

(3) ノード修復

既存手法を参考にして、故障ノードや改ざんノードに対して少量の移動ロボットが交換・修復を行う手法を考える。三つのアルゴリズム（集中管理、静的分散管理、動的分散管理）に対して、移動ロボットの移動消費電力や送受信コストを比較する。

集中管理では、1 台のロボットが領域の中心に固定されて、manager としてすべての故障を報告される。残りのロボットは maintainer としてランダムに一様に領域に配置される。故障報告された manager は、故障ノードの位置と最も近い maintainer を選び、故障ノードを交換させる。

静的分散管理では、領域が均等に分けられ、各領域に 1 台のロボットが割り当てられる。各領域のロボットは、manager と maintainer 二つの役割を担当する、つまり担当領域の故障を独力で修復する。

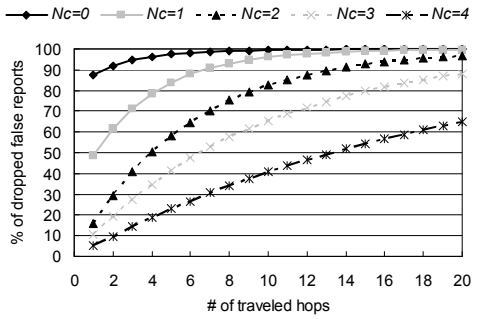
動的分散管理では、各ロボットの間に固定的な境界がなく、ロボットの間の境界は Voronoi 図のように動的に構成される。ロボットが故障修復して移動するとき境界が変わるため、静的分散管理と異なる点は Voronoi 図をどのように動的に維持するかである。

４．研究成果

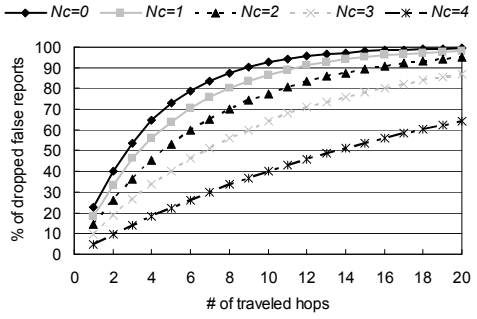
(1) 比較シミュレーション

提案する免疫型統計的経路フィルタリングの効果を確認するためにシミュレーションを行った。シミュレーション環境は Ye らと同じとする（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異なる環境でもシミュレーションを行ったが、ここでは割愛する）。200×20 m^2 のフィールドサイズに 340 個のノードが一様に配備される。BS とイベント発生地点はフィールドの両端にあり、それらの間には約 100 個の転送ノードがあることになる。BS は N= 1000 個の秘密鍵のプールを保持し、その鍵プールは n = 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 m = 100 個の鍵があるとする。各ノードには k = 50 個の鍵を格納し、イベントレポートには T= 5 個の MAC を添付する。そして、攻撃のシナリオとしては、攻撃者はイベント付近の複数個のノードを乗っ取り、N_c($0 \le N_c \le T$-1)個の異なるパーティションから秘密鍵を不正に入手し（攻撃者は入手できない T-N_c 個の MAC を偽造する必要がある）、1000 個の偽造レポートを送信することとする。なお、提案手法のパラメータΔs、Δf、Δd はここではすべて 0.01 で固定する。結果は 100 個のネットワークトポロジーの平均とする。

不正入手されたパーティション数 N_c を変えながら提案手法と Ye らの既存手法の性能を比較した結果を図 1 に示す。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ことが分かる。例えば N_c = 1 のとき、つまり 1 個の鍵だけが不正入手され、残り 4 個の MAC は偽造されなければならない場合、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既存手法では約 64%の偽造レポートが検知されるのに対して、免疫型統計的経路フィルタリングでは約 84%が破棄される。つまり、提案手法が既存手法よりも早い段階で偽造データを破棄できることが確認された。ただし、N_c が大きくなるにつれてレポート内の正当な MAC が減るため、偽造レポートの検出は困難になり、例えば N_c = 4 のとき両手法ともに 20 ホップ以内に約 65%の偽造レポートしか破棄できていない。この点については、統計的経路フィルタリングそのものの課題であり、別のアプローチが必要である。



(a) 提案手法



(b) 既存手法

図 1　不正入手されたパーティション数 N_c を変えながら、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
((a)が提案手法、(b)が既存手法)

(2) パラメータ検証

鍵プールやノード配備密度に関するパラメータ N、k、Tについては既存研究で検証済みであるため、本提案手法に固有なパラメータであるΔs、Δf、Δd について解析を行った。三つのパラメータのうち一つを 0 から 0.1 まで変化させ、残り二つを 0.01 で固定した場合の性能を調べた。図 2 に変化させたパラメータを横軸、1 ホップで破棄された偽造レポートの割合を縦軸とする検証結果を示す。結果からΔs が減少し、Δf やΔd が増加するにつれて偽造レポートの破棄率が増えることが分かる。特にパラメータと性能の関係において相転移的現象が観測されたことが興味深い。$\Delta s > 0.01$ に対して性能が悪化する理由として、偽造レポートを破棄できた転送ノードがもつ信用度が$\Delta d = 0.01$ だけ減少したとしても、異なる偽造 MAC をもつ偽造レポートがその転送ノードをすり抜けてしまい、その信用度がΔsによって1に回復してしまいうるからである。$\Delta f < 0.01$ や$\Delta d < 0.01$ に対する性能悪化も同様の理由が当てはまるといえる。

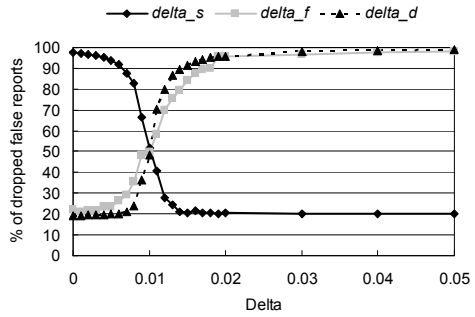


図 2　提案手法に固有なパラメータであるΔs、Δf、Δd を変化させたときの 1 ホップで破棄された偽造レポートの割合

(3) 数学的解析

数学的解析により既存手法と提案手法の偽造レポートの破棄率を求めた。まず、攻撃者は入手できない T-N_c 個の MAC を偽造する必要があるため、ある転送ノードが T-N_c 個のうち 1 個の鍵を持つ確率、つまりその 1 個の不正 MAC を検出してレポートを破棄できる確率 p_1 は、以下で与えられる。

$$p_1 = \frac{T - N_c}{n} \cdot \frac{k}{m} = \frac{k(T - N_c)}{N}.$$

そして既存手法において h ホップ以内に破棄される偽造レポートの期待割合 p_h は以下となる。

$$p_h = 1 - (1 - p_1)^h.$$

一方、提案手法に対して h ホップ以内に破棄される偽造レポートの割合 p'_h は p'_{h-1} を用いて以下のように再帰式として計算される。

$$p'_h = p'_{h-1} + (1 - p'_{h-1})(1 - R_{h,h-1}) + (1 - p'_{h-1})R_{h,h-1}p_1,$$

ここで、$R_{h,h-1}$ はノード h における転送元ノード h-1 の信用度である。この式の右辺第 1 項は、h-1 個の転送ノードで偽造レポートが破棄された割合を示す。第 2 項は、h-1 個の転送ノードをすり抜けた偽造レポートが確率 1-$R_{h,h-1}$ でノード h に届かなかったことを示す。第 3 項は、偽造レポートがノード h に届いたものの確率 p_1 でノード h により破棄されたことを意味する。上式を展開し整理すると

$$p'_h = 1 - (1 - p_1)^h \prod_{i=1}^{h} R_{i,i-1}.$$

を得る。すべての信用度を更新しない場合、$\prod_{i=1}^{h} R_{i,i-1} = 1$ であるから、p'_h は既存手法の p_h と等しくなる。もしいくつかの信用度が減少したら、$\prod_{i=1}^{h} R_{i,i-1} < 1$ となり $p'_h > p_h$ となる。

$N_c = 1$ に対して全ノードの信用度を同じとして 0.5 から 1 まで変化させたときの h ホップ以内に破棄される偽造レポートの割合 p'_h を図 3 に示す。同図から $p'_h > p_h$ を再確認できる。図 1(a)の $N_c = 1$ に対するシミュレーション結果と比較すると、数学的解析はシミュレーション結果よりも鋭い曲線である。その理由は、シミュレーションでは各ノードの信用度は異なり、攻撃者に乗っ取られたノードに近いノードが他のノードよりも恐らく低い信用度を持つためである。

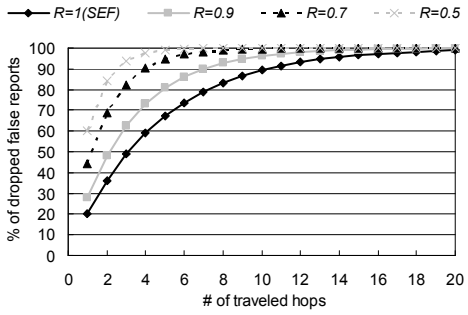


図 3　$N_c = 1$ に対して信用度を変化させたときの数学的解析による破棄された偽造レポートの割合

(4) ノード修復

ノード修復については、自作の簡易ネットワークシミュレータおよび市販の高速かつ高精度なシミュレータ QualNet 上でのプログラム作成を行った。そして、既存手法では場合によっては修復作業が集中すること、ロボットの保持できるノード数が無限であるなどの問題点を洗い出した。プログラム作成に予想以上に時間を要したため、この結果を現在まとめているところであり近々発表予定である。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計４件）

① Yuji Watanabe, Performance Evaluation of Immunity-based Statistical En-route Filtering in Wireless Sensor Networks, Artificial Life and Robotics, Vol.16, No.3, pp.422-425, 2011, 査読有
DOI:10.1007/s10015-011-0969-x

② Yuji Watanabe, An Analysis of Immunity-based Statistical En-route Filtering in Wireless Sensor Networks, Proceeding of the International Conference on Management of Emergent Digital EcoSystems, Vol.3, pp.250-256, 2011, 査読有
DOI:10.1145/2077489.2077536

③ Yuji Watanabe, An Immunity-based Scheme for Statistical En-route Filtering in Wireless Sensor Networks, Lecture Notes in Computer Science (Knowledge-Based Intelligent Information and Engineering Systems), Vol.6278, pp.660-665, 2010, 査読有
DOI:10.1007/978-3-642-15393-8_74

④ Yuji Watanabe and Tong Tran Nhat Linh, A Secure Routing Scheme for Mobile Wireless Sensor Networks, Artificial Life and Robotics, Vol.15, No.3, pp.302-305, 2010, 査読有
DOI:10.1007/s10015-010-0812-9

〔学会発表〕（計３件）

① 渡邊裕司、田村知嗣、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、コンピュータセキュリティシンポジウム 2012、2012 年 10 月 31 日、松江

② Yuji Watanabe and Tomotsugu Tamura, A Multipath Immunity-based Statistical En-route Filtering in Wireless Sensor Networks, The Seventeenth International Symposium on Artificial Life and Robotics, 2012 年 1 月 21 日、別府

③ 渡邊裕司、田村知嗣、無線センサネットワークにおける統計的経路フィルタリングへの免疫的アプローチ、第 23 回自律分散システム・シンポジウム、2011 年 1 月 30 日、北海道

〔図書〕（計１件）

① 渡邊裕司　他、12.5 免疫アルゴリズム、電気学会・進化技術応用調査専門委員会編者、進化技術ハンドブック　第Ⅰ巻基礎編、近代科学社、pp.158-160、2010

６．研究組織

(1)研究代表者

渡邊　裕司（WATANABE　YUJI）
名古屋市立大学・システム自然科学研究科・准教授
研究者番号：60314100

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：