

開放環境無線センサネットワークにおける協調的改ざん検知と自己組織化マップを用いた不正ノード孤立化手法の提案

木村 圭希¹ 滝沢 泰久²

概要：無線センサネットワークにおいて、ノードが配備される環境は管理環境と開放環境の2つに大別される。開放環境に設置される無線センサネットワークは、第三者によるセンサノードへの物理的な接触により、センサノード内に保存されている鍵などの秘密情報が不正に取得される可能性がある。従来、ネットワーク上での改ざん検知はデジタル署名や、MAC(Message Authentication Code) が用いられる。しかし、これらの手法は、鍵の秘密性を保証することが必要であり、鍵の秘密性が破綻する状況では、これらの手法は全く機能せず、データの信頼性が失われることになる。本論文は、鍵に依存せずにデータ改ざん不正に対する信頼性を確保するため、複数の正規ノードの協調により改ざんを行う不正ノードを検知する。さらに、ノード間の相互データ通信における振る舞いから、自己組織化マップに基づき正規ノードと不正ノードへクラスタリングを行い、クラスタリングの結果を基に、不正ノードを論理的に無線センサネットワークから孤立化する。協調的検知と自己組織化マップを用いた孤立化を行うことで、既存手法では検知困難な改ざんを検知し、不正ノードのみをネットワークから除外する手法を提案する。

キーワード：無線センサネットワーク、セキュリティ、自己組織化マップ、協調的検知

1. はじめに

近年、複数のセンサからの情報を包括的に解析し各種制御を行うため、無線センサネットワークの利用が急速に拡大しており、その需要から多様な環境に無線センサネットワークが配備されることが考えられる。無線センサネットワークが配備される環境は、オフィスなどの出入りする者が限られる管理環境と、道路や橋などの不特定多数の第三者が混在する開放環境の二つに大別される。開放環境では、その環境の特性から第三者によるセンサノードへの物理的な接触を完全に遮断することは難しく、悪意のある者がセンサノードへ接触することによって様々な不正を行うことができる [1] [2] [3] [4]。例えば、悪意のある者はセンサノードのストレージに直接アクセスすることで、センサノードに格納されている鍵などの秘密情報を不正に取得することができる [5] [6] [7] [8]。このように不正に取得した鍵を用いて認証をすり抜けることで、悪意のある者は改ざんなどの不正行為を行う不正ノードをネットワークに混入させることが可能となる [9] [10]。従来、ネットワーク上での改ざん検知は、デジタル署名や簡易な署名である MAC(Message Authentication Code) が広く利用されている [11]。しか

し、デジタル署名や MAC は鍵の秘密性の担保を前提とする手法である。上記のような悪意のある者が鍵を盗取した状況ではこれらの手法は機能しない [12]。無線センサネットワークにおいて、鍵に依存せずに不正行為を検知する手法として Watchdog mechanism [13] [14] [15] [16] が提案されている。しかし、Watchdog mechanism では、通信範囲外となるノードの振る舞いを監視することができない。そのため、悪意のある第三者が経路上に不正ノードを連続して配置した場合、一方の不正ノードが他方の不正ノードの改ざんを隠蔽する不正行為 [17] は、Watchdog mechanism では、その改ざんを検知できない。上記のような鍵を盗取した複数の不正ノードによる改ざんは既存方式では検知できず、無線センサネットワークにおけるデータの信頼性が失われてしまう。我々は、上記問題を解決するため、複数の正規ノードの協調により改ざんを行う不正ノードを検知し、ネットワーク内のノード間で多数決を実施することで、不正ノードを論理的に WSN から孤立化する手法（以降、先行研究）[18] を提案した。孤立化とは、改ざんを検知したノードが、不正ノードを経路表から消去し、隣接ノードに不正ノードの存在を知らせる孤立化パケットを送信することで、不正ノードをネットワークのデータ転送経路上から排除することである。先行研究は、改ざんと不正孤立化を行う不正ノードが混在する無線センサネットワークに

¹ 関西大学大学院 理工学研究科

² 関西大学 環境都市工学部

において、不正ノード数が正規ノード数より少ない条件で、鍵に依存することなくデータの信頼性を確保できることを示した。しかし、先行研究は、ネットワークの局所域において不正ノード数が正規ノード数を上回る場合、正規ノードがネットワークから除外される問題がある。

本論文は上記問題を解決するために自己組織化マップ(SOM : Self-Organizing Maps) [19] を用いてセンサノードにおける相互データ通信の振る舞いから正規ノードと不正ノードへクラスタリングし、その結果により不正ノードのみを孤立化対象としてネットワークから除外する手法を提案する。

2. 関連研究

2.1 Message Authentication Code

MAC(Message Authentication Code) [21] とは、秘密である共有鍵とハッシュ関数を用いてメッセージの完全性を担保する技術である。計算機資源での制約が大きい無線センサネットワークでの利用が想定されている [20]。送信ノードは、送信したいメッセージと事前に共有した鍵を足し合わせ、ハッシュ関数に通して MAC 値を生成する。送信ノードは元のメッセージに生成した MAC 値を添えて送信する。受信ノードは、受信したメッセージと共有した鍵からハッシュ関数を用いて MAC 値を生成する。受信ノード側が生成した MAC 値と、メッセージに添えられていた MAC 値が一致すればメッセージの改ざんが行われなかったことがわかる図 (1)。MAC 値の生成には、秘密である共有鍵が必要となる。共有鍵を知らない第三者は、正規のメッセージから生成された MAC 値を共有鍵なしで割り出すことは困難であるため、正規ノードによる改ざん検知が可能となる。ここで、秘密の共有鍵が漏洩した場合を考える。共有鍵を取得した第三者は、改ざんしたメッセージから MAC 値を生成することができる。受信ノードは受け取ったメッセージから MAC 値を生成し、添付されていた MAC 値との比較を行う。ここでメッセージは改ざんされているが、改ざんされたメッセージから生成した MAC 値を添付しているので、2つの MAC 値は一致することとなり改ざんはされていないとみなされる。上記のように、共有鍵が漏洩した場合はメッセージの改ざんが行われたとしても、正規ノードによる検知は不可能となる。次に、鍵を用いず改ざんを検知する手法である Watchdog mechanism について説明する。

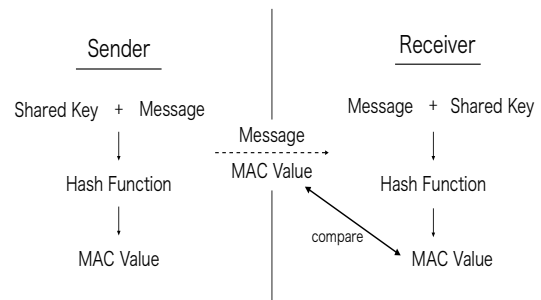


図 1 Message Authentication Code

2.2 Watchdog mechanism を用いた改ざん検知

以下に、Watchdog mechanism [13] を用いた改ざん検知手法について述べる。

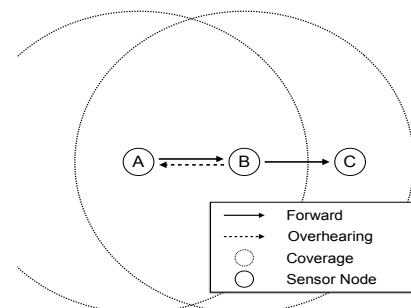


図 2 Watchdog mechanism

図 2 において、ノード A がノード C にパケットを送信する場合を考える。ノード A とノード C は直接通信できる範囲にいないので、ノード A は隣接ノードであるノード B にパケットの中継を依頼する。無線通信の特性より、ノード A はノード B が送信を傍受することができる。ノード B がノード C に中継を行なった際、ノード A はノード B が送信したパケットを傍受し、ノード A 自身が送信したパケットと比較することで、ノード B が正しく中継を行なったかどうかを確認することができる。この手法は鍵に依存しない手法であるため、鍵が漏洩したネットワークにおいても有効である。しかし、この手法は送信ノード自身が中継ノードの振る舞いをモニタリングする手法であるため、通信範囲外のノードの振る舞いを監視することはできない。

2.3 改ざんの隠蔽

図 3 に不正ノードが連続して中継する場合を示す。ノード B は自身ではパケットの改ざんを行わずノード C に中継をする。パケットを受け取ったノード C は転送の際にパケットを改ざんするが、この場合 Watchdog mechanism を用いてノード C の改ざん行為を検知できるのはノード B のみとなる。しかし、ノード B も不正ノードであるため、ノード C の改ざん行為を正規ノードに対して隠蔽することができる。このような状況下では Watchdog mechanism

による改ざん検知は難しく、不正ノードによる改ざんがネットワークのデータの信頼性を大きく損なわせることになる。

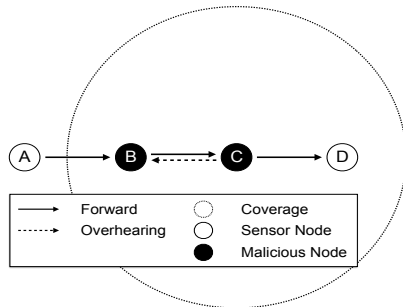


図 3 改ざんの隠蔽

3. 先行研究

先行研究では、Watchdog mechanism の問題を解決するために、協調的検知と多数決手法を用いた不正ノード孤立化手法を提案した。以下に、各種ノードの定義と手法の詳細を示す。

3.1 ノードの定義

先行研究において、無線センサネットワークの各ノードを次のように定義する：

- 正規ノード：改ざん行為や不正孤立化行為を行わないノード。
- 協調ノード：送信ノードと受信ノードに共通して隣接する正規ノードを協調ノードとする。
- 改ざんノード：中継の際に改ざんを行うノード。
- 不正孤立化ノード：孤立化を悪用し、正規ノードをネットワークから除外することを目的とするノード。
- 不正ノード：改ざんノードと不正孤立化ノードの総称。また、他の改ざんノードによる改ざん行為を隠蔽するノードも不正ノードとする。

3.2 協調的改ざん検知

協調的改ざん検知は、送信ノードと複数の協調ノードが行う。以下に、Watchdog mechanism では検知できない場合における協調的改ざん検知について述べる。図 4 において、ノード A, D, E は正規ノードで、ノード B, C は不正ノードである。ノード A, B, C, D は経路上に連続して配置され、ノード E はノード B, C に共通する隣接ノードで協調ノードである。ノード B は不正ノードであるが改ざんを行わず転送を行い、ノード C はパケットを改ざんし転送を行う。ノード C が行う改ざんを検知するには、ノード B と C の両方が転送したパケットを傍受する必要がある。先行研究において、協調ノード E はノード B と C の両方のパケットを傍受することが可能であり、その二つのパケッ

トの中身を比較することで改ざん検知が可能となる。

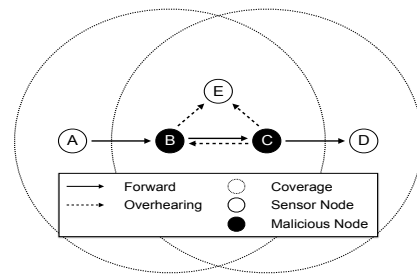


図 4 改ざんの隠蔽に対する検知

3.3 多数決手法を用いた不正ノードの孤立化

先行研究では、全てのノードに協調的検知と孤立化の権限を付与している。理由は、協調的検知と孤立化の権限を限定したノードに付与すると、権限を持つノードがネットワークから離脱した際に検知率が著しく低下することが想定されるからである。しかし、全てのノードに協調的検知と孤立化の権限を付与すると、不正ノードが孤立化パケットを悪用し正規ノードを孤立化させることが想定される。従って、先行研究では不正な孤立化を行うノードを排除するために、ノード毎の孤立化に関与した回数を用いて、不正ノードを孤立化する手法を提案した。

3.3.1 不正ノード孤立化

改ざん行為を検知したノードは、隣接ノードへ不正ノードの存在を知らせるために孤立化パケットを送信する。孤立化パケットには、孤立化パケット送信ノードと孤立化対象ノードの IP アドレスが格納されている。孤立化パケットを受け取ったノードは、経路表に孤立化対象ノードが存在する場合、孤立化対象ノードの IP アドレスを経路表から削除し、ブラックリストに登録する。孤立化対象ノードを経路表から削除することで、転送先として不正ノードを選択する可能性を排除する。経路表に孤立化対象ノードが存在しない場合は、ブラックリストへの登録のみを行う。このブラックリストは経路作成要求を受信した際に参照される。経路作成要求を受信した際、その要求の送信元がブラックリストに登録されている場合はその要求を破棄する。ブラックリストを参照することにより、不正を行ったノードが経路に再参加することを防ぐことで、データの信頼性を確保する。

3.3.2 孤立化関与回数

各ノードは孤立化パケットを受信した場合、次の条件の隣接ノードの孤立化関与回数を加算する：

- 孤立化の対象となった場合
- 孤立化パケットを送信した場合

上記に従い孤立化関与回数は更新される。この孤立化関与回数が閾値を超えたノードに対して孤立化を行う。すなわち、多くのノードが送信する孤立化パケットが正しい（多数決）とし、これを採用して対象ノードをネットワークか

ら孤立化する。一方で、孤立化パケット送信に関わる機会が多いノードは孤立化関与回数が大きくなる。そのため、関与した孤立化パケットが多数決で採用された場合、他のノードは採用された孤立化パケットに関与したノードを信頼できるノードとして、その孤立化関与回数を初期値 0 へ戻す。

4. 提案手法

先行研究では、既存手法に対する比較評価において、データの信頼性を確保できることを示した。しかし、先行研究では全域的、局所的に不正ノード数が正規ノード数を上回る場合、孤立化パケット送信の多数決において正規ノードの孤立化関与回数が増大して、正規ノードをネットワークから排除する問題がある。従って、提案方式では上記問題を解決するために SOM を用いて正規ノードと不正ノードのそれぞれの孤立化パケット送信における振る舞いからクラスタリングを試みる。SOM を用いてノードをクラスタリングした結果により孤立化を行うことで、不正ノードのみをネットワークから除外する手法を提案する。

4.1 自己組織化マップ(SOM : Self-Organizing Maps)

自己組織化マップ (SOM: Self-Organizing Map) [19] は、コホネン (T. Kohonen) により提案されたアルゴリズムである。SOM は観測空間 (入力層) と潜在空間 (出力層) からなる 2 層構造の学習ニューラルネットワークである。高次元の入力データに対し、データ分布の位相的構造を保存しつつ低次元空間へ写像することによって、データを予備知識なし (教師なし) に分類することができる。本論文において、SOM を利用する理由は以下のとおりである。提案方式では、目的変数を設定できない。そのため、教師なし学習である必要がある。また、提案方式では正規ノードと不正ノードを明確に 2 分させる必要がある。クラスタリングの精度を上げるために、今後入力データを高次元化する可能性がある。そのために、高次元の入力データにも対応することができる SOM を利用する。

4.2 孤立化パケット送信における振る舞いデータ

SOM を用いるには、入力データが必要である。本論文では、以下の 2 点の情報を孤立化パケットから取得する。孤立化パケットから取得した孤立化パケット送信における振る舞いデータを入力データとする：

- 孤立化パケットの送信回数
- 孤立化パケット対象ノードの IP アドレス

上記の 2 点を入力データの要素として選択した理由は、上記の 2 点において正規ノードと不正ノードでふるまいに違いが出ると想定するからである。1 つ目の要素 (孤立化パケットの作成回数) における正規ノードと不正ノードの振る舞いは、以下のように想定される：

- 正規ノード：改ざんを検知すれば孤立化パケットを送信する。また、改ざんノードが孤立化されれば、孤立化パケットの送信を停止する。
- 不正孤立化ノード：改ざんの有無に関わらず孤立化パケットを周期的またはランダムに送信する。

2 つ目の要素 (孤立化パケット対象ノードの IP アドレス) における正規ノードと不正ノードの振る舞いは、以下のよう

- に想定される：
- 正規ノード：改ざんノードを対象とした孤立化パケットを送信する。
 - 不正孤立化ノード：正規ノードを対象とした孤立化パケットを送信することが想定される。
- 本論文では、上記に示した正規ノードと不正ノードのふるまいの違いに着目して SOM を利用する。

4.3 SOM の孤立化への利用

SOM を用いた孤立化のアルゴリズムは以下のとおりである：

- (1) 一定期間、正規ノードは他のノードの孤立化パケットを監視し、前述の孤立化パケット送信における振る舞いデータ (入力データ) を取得する。
- (2) 各ノードの孤立化パケット送信回数、孤立化対象 IP アドレスによる振る舞いデータをそれぞれの 2 次元データとして、各正規ノードが SOM に基づきクラスタリングを行う。
- (3) クラスタリングされた結果から、各正規ノードが他ノードとのノード間距離を計算する。
- (4) ノード間距離が閾値より小さいノード、すなわち、孤立化パケット送信において自身と同じ振る舞いをするノードを信頼できるノードと判断し、ノード間距離が閾値より大きいノード、すなわち、孤立化パケット送信において自身と異なる振る舞いをするノードを信頼できないノードと判断する。

各ノードにおいて自身と同じ振る舞いをする信頼できるノードグループと、異なる振る舞いをする信頼できないノードグループに明確に 2 分させるため、提案方式では、step2 においてクラスタリングを行う際に SOM を 2 段階とする。1 度目の計算では、広い範囲に学習を与え、2 度目の計算では、狭い範囲に学習を与える。2 段階で SOM を回すことで、SOM の出力層においてノード群を 2 つのグループにクラスタし、さらにグループ間の距離が大きくなることを図る。

SOM 実施後の孤立化の流れについて示す。SOM 実施後は、信頼できるノードが送信した孤立化パケットに従って以下の孤立化処理を実施する。孤立化対象ノードが経路表に存在する場合、孤立化対象ノードの IP アドレスを経路表から削除し、経路再構成を行う。次に、孤立化対象ノードをブラックリストに登録する。孤立化対象ノードが経路

表に存在しない場合、孤立化対象ノードをブラックリストに登録する。最後に孤立化パケットを転送する（重複受信した孤立化パケットは破棄）。孤立化処理は、次の条件で実施する。

- 信頼できるノード（SOM 出力層において自身とノード間距離が近いノード）から孤立化パケットを受信した場合、孤立化パケットの対象ノードに対して実施。
- 信頼できるノードを対象とする孤立化パケットを受信した場合、孤立化パケット送信ノードを不正ノードとして、孤立化パケット送信ノードを対象に実施。

それ以外は、信頼できないノード（SOM 出力層において自身とのノード間距離が遠いノード）からの孤立化パケットとして破棄し、孤立化処理は行わない。

5. シミュレーション評価

シミュレーション諸元を表 1 に示す。提案方式の有効性を示すために、NS3 を用いシミュレーションを行う。

項目	値
シミュレータ	NS3
フィールド空間 (m ²)	1,000 × 1,000
トポロジ	ランダム
正規ノード数 (個)	90, 80, 70, 60, 50
改ざんノード数 (個)	5, 10, 15, 20, 25
不正孤立化ノード数 (個)	5, 10, 15, 20, 25
シミュレーション時間 (秒)	1000
データサイズ (バイト)	12
無線通信	IEEE802.11b
通信カバレッジ (m)	250
ルーティングプロトコル	AODV
バッファ容量 (個)	50

表 1 シミュレーション諸元

合計のノード数を 100 個で固定する。全ノードのうち、不正ノードの割合を 10 % から 50 % へ 10 % ずつ増加させた計 5 通りで評価する。不正ノードは、改ざん行為のみを行う改ざんノードと、正規ノードを対象とした不正な孤立化パケットの送信のみを行う不正孤立化ノードを用意する。改ざんを行いかつ、不正な孤立化を行うノードは改ざんを行なった時点で孤立化されてしまうので今回は考えないこととする。また、不正ノードによる改ざん隠蔽の状況を作り出すために、不正ノードがパケットを転送する際に、転送先が不正ノードである場合は改ざんは行わず転送する。転送先が正規ノードがある場合は、その不正ノード自身で改ざんを行う。上記を踏まえた上で、Watchdog mechanism, 先行研究, 提案方式を次の 4 つの項目において比較評価する：

- 改ざん検知率
- 正規ノード孤立化数
- 残存不正ノード数

- 改ざん率

5.1 評価結果と考察

5.2 改ざん検知率

図 5 に改ざん検知率の評価結果を示す。改ざん検知率は、全改ざんパケットに対して、検知した改ざんパケットの割合として算出している。Watchdog mechanism は改ざんノード数が増加すると改ざん検知率が低下する。一方、先行研究と提案方式では、協調的検知を行なっているため、Watchdog mechanism では検知不可能な連続する不正ノードによる改ざんも検知できる。その結果、全ノードに対する不正ノードの割合が 50% の場合でも、先行研究では 95% 以上、提案方式では 97% 以上の改ざん検知率を維持している。また、先行研究と提案方式において、全ノードに対する不正ノードの割合が 30% 以上の場合、検知率が 100% にならない理由は、不正ノードの隣接に十分な数の正規ノードが存在しないためである。今回の検証では、全ノードに対する不正ノードの割合が増加するにつれて、正規ノード数が減少する。その結果、協調的検知が機能する条件である「経路上で連続する不正ノードの両方の隣接ノードとなる正規ノードが存在する」を満たせない箇所がネットワーク上に存在することになる。

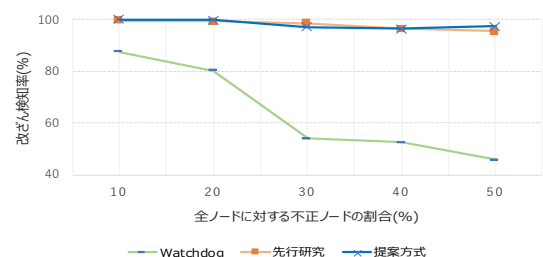


図 5 改ざん検知率

5.3 正規ノード孤立化数

図 6 に正規ノード孤立化数の評価結果を示す。正規ノード孤立化数は、不正孤立化ノードによって孤立化された正規ノード数を示す。全ての近傍ノードから通信経路を遮断された状態を、孤立化が成立した状態とする。Watchdog mechanism では、孤立化を行わないので正規ノード孤立化数は 0 になる。先行研究では、多数決を行う為、局所的に不正ノード数が正規ノード数を上回る場合、不正な孤立化が成立してしまう。一方、提案方式では、SOM を用いて正規ノードと不正ノードをクラスタリングすることで不正な孤立化が成立していない。これは、正規ノードと不正ノードをクラスタリングできていることを示す。つまり、正規ノード孤立化の排除という観点からは有効なクラスタリングができているといえる。

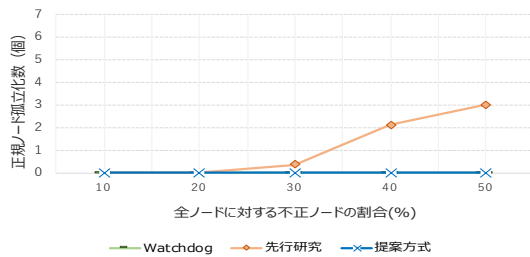


図 6 正規ノード孤立化数

5.4 残存不正ノード数

残存不正ノード数の評価結果を図 7 に示す。残存不正ノード数は、シミュレーション終了時点で孤立化されていない不正ノード数を示す。Watchdog mechanism では、孤立化が行われない為、全ての不正ノードが残る。なお、Watchdog mechanism では孤立化を行わない為、不正孤立化ノードは不正ノードとして扱わず、改ざんノードのみを不正ノードとして扱っている。先行研究では、不正ノードの割合が 30% 以上の場合、不正ノードが残ってしまう。これは、図 6 に示すように、不正ノードの割合が 30% 以上の場合、ネットワークの一部の領域で不正ノード数が正規ノード数を上回り、不正孤立化が成立し正規ノードが排除され、その結果、不正ノードが残存する。一方、提案方式では多数の不正ノードが残った。これは、多くの場合、SOM の出力層において、正規ノードが 2 グループに分かれていることが原因であると考えられる。提案方式で残存している不正ノードの多くは不正孤立化ノードである。そこで、以下に提案方式において、多数の不正孤立化ノードが残存する理由を示す。

正規ノード A とのノード間距離が近い正規ノード群をグループ g1、正規ノード A とのノード間距離が遠い正規ノード群をグループ g2 と仮定した上で、以下の 2 つの場合を考える：

- 不正孤立化ノード X がグループ g1 のノード（ノード間距離が近いノード）に対して孤立化パケットを送信する場合
- 不正孤立化ノード X がグループ g2 のノードに対して孤立化パケットを送信した場合

不正孤立化ノード X がグループ g1 のノード（ノード間距離が近いノード）に対して孤立化パケットを送信する場合：グループ g1 に所属するノード A は、ノード X が信頼できないノード（ノード間距離が遠いノード）であるため、受信した不正孤立化パケットを破棄する。さらにノード A は、明らかな不正孤立化パケットを送信したとして、ノード X に対して以下の孤立化処理を実施する。

ノード X を対象とした孤立化パケットを送信する。ノード X が経路表に存在する場合、ノード X の IP アドレスを経路表から削除し、経路再構成

を行う。次に、ノード X をブラックリストに登録する。また、ノード X が経路表に存在しない場合、ノード X をブラックリストに登録する。

グループ g2 に所属するノードは、ノード X が信頼できないノードである、かつグループ g1 に所属するノードも信頼できないため、孤立化パケットを破棄し、孤立化処理は行わない。

不正孤立化ノード X がグループ g2 のノードに対して孤立化パケットを送信した場合：グループ g1 に所属するノード A は、ノード X が信頼できないノードである、かつグループ g2 に所属するノードも信頼できないため、孤立化パケットを破棄し、孤立化処理は行わない。グループ g2 に所属するノードは、ノード X は不正ノードであると判断して受信した孤立化パケットを破棄し、ノード X を対象として孤立化処理を行う。つまり、不正孤立化ノード X の近傍にグループ g1 の正規ノードとグループ g2 の正規ノードが混在する場合、その不正孤立化ノードを孤立化することができないことがある。

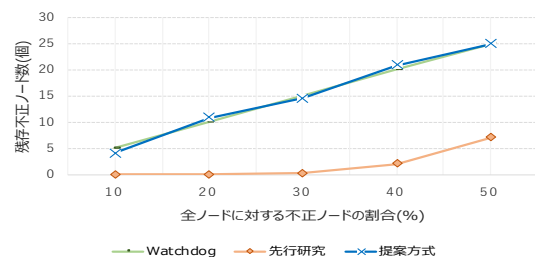


図 7 残存不正ノード数

5.5 改ざん率

改ざん率の評価結果を図 9 に示す。改ざん率は、「シンクサーバに到達した改ざんパケット数/シンクサーバに到達した全パケット数」で表される。Watchdog mechanism では、孤立化が行われない為、不正ノード数に比例して改ざん率が増加する。先行研究と提案方式では、Watchdog mechanism と比較して改ざん率を抑えることができた。先行研究では、図 7 に示すように改ざんノードを孤立化することによって改ざん率を抑えることができた。一方、提案方式では、残存不正ノード数が多数存在するのにもかかわらず先行研究より改ざん率を抑えることができた。以下に提案方式において、残存不正ノード数が多数存在するのにもかかわらず改ざん率を抑えることができた理由を示す。

正規ノード A1 とのノード間距離が閾値より近い正規ノード群をグループ g1、正規ノード A1 とのノード間距離が閾値より遠い正規ノード群をグループ g2 と仮定する。図 8 において、ノード A1, A2, B1, B2 は正規ノード、ノード Z は改ざんノード、ノード A1, A2 がグループ g1、ノード B1, B2 がグループ g2 であると仮定する。（ノード

B1 - ノード Z) と (ノード B2 - ノード Z) を結ぶ波線はリンクを示す。

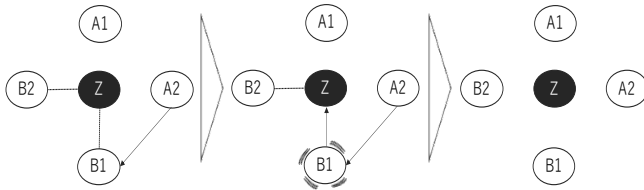


図 8 改ざんノードの孤立化フロー

グループ g1 のノード A1 /A2 がノード Z の改ざんを検知した場合、ノード Z へのリンクを遮断し、孤立化パケットを送信する。ノード間距離が近いグループ g1 に相当するノードはこれを採用するが、ノード A1 /A2 とノード間距離が遠いノードは自身とは異なる振る舞いのノードからの孤立化パケットであるので、これを無視する。従って、ノード B1 /B2 はノード Z へのリンクを保持している。以上の状況でノード A2 がノード Z を迂回してノード B1 にパケットを転送する場合、ノード B1 はノード Z へのリンクを切っていないのでノード Z へパケットを転送する可能性がある。その場合は、ノード B1 はノード Z の改ざんを検知することができるのでノード Z とのリンクを遮断し、孤立化パケットを送信する。ノード B1 とノード間距離が近いグループ g2 に相当するノードはこれを採用する。つまり、ノード Z は完全に孤立化される。仮にノード B1 がノード Z 以外のノードへ転送する場合、ノード B1 とノード Z、ノード B2 とノード Z のリンクが残存していてもこのリンクは経路上不要なリンクであり、ノード Z へデータが転送されることはない。従って、改ざんノードが残存している、すなわち、改ざんノードと正規ノード間にリンクが残存している場合、その残存リンクは経路上不要なリンクであり、改ざんノードへデータが転送されることはない。以上の理由より、提案方式では、残存不正ノード数が多数存在するのにも関わらず改ざん率を抑えることができた。

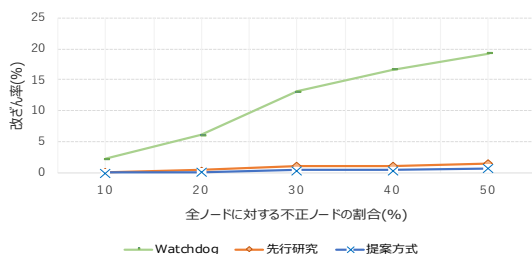


図 9 改ざん率

6. まとめ

本論文では、鍵の秘密性が失われた WSN において、複数の正規ノードの協調により改ざんを行う不正ノードを検

知し、SOM を用いて相互データ通信における振る舞いから正規ノードと不正ノードの分類を行うことで、検知した不正ノードを論理的にネットワークから孤立化する手法を提案した。提案方式は、先行研究と同様に協調的検知により既存手法では検知困難な改ざんを検知するとともに、先行研究の正規ノードが孤立化されるという問題を解決し、さらに改ざん数を抑えられることを示した。しかし、提案方式では、以下の 2 つの課題が残る：

- 不正ノードが残存する課題
- リソースの課題

提案方式では、多数の不正ノード数が残存した。これは、SOM 出力層において正規ノードが 2 つのグループに分かれることが原因である。そのため、孤立化パケット送信における振る舞いデータ以外の情報を SOM への入力データとして加え、入力データを高次元化することで、正規ノードを一つのグループにまとめる方式の検討を進める。また、提案方式では、リソースが脆弱であると想定される IoT デバイスにとって大きな負荷がかかることが想定される。そのため、通信トラフィックや計算量が少なくなるように、個々のノードが自身で計測した振る舞いデータから SOM を実施して、局所的な孤立化処理を行う手法の検討も進める。

参考文献

- [1] VP.Illiano, and EC.Lupu: *Detecting Malicious Data Injections in Wireless Sensor Networks:A Survey*, ACM Computing Surveys, Vol.48, No.2, Article 24 (2004).
- [2] 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 論文集, Vol.2012, No.3, pp.254-261 (2012).
- [3] S.Bartariya, and A.Rastogi: *Security in Wireless Sensor Networks:Attacks and Solutions*, IJARCCCE, Vol.5, Issue.3, pp.214-220 (2016).
- [4] A.Perrig, J.Stankovic, and D.Wagner: *Security in wireless sensor networks*, Commun.ACM, vol.47, no.6, pp.53-57 (2004).
- [5] S.Prasanna, and S.Rao: *An Overview of Wireless Sensor Networks*, IJSCE, Vol.2, Issue.2, pp.538-540 (2012).
- [6] 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, 電子情報通信学会論文誌, Vol.J92-B, No.4, pp.678-688 (2009).
- [7] C.Karlof, N.Sastry and D.Wagner: *TinySec: A Link Layer Security Architecture for Wireless Sensor Networks*, SenSys '04 Proceedings of the 2nd international conference on Embedded networked sensor systems, pp.162-175 (2004).
- [8] G.Pamavathi and D.Shanmugapriya: *A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks*, IJCSIS, Vol.4, No.1, pp.1-9 (2009).
- [9] H.Chan, and A.Perrig: *Security and Privacy in Sensor Networks*, IEEE Computer Society, Vol.36, Issue.10, pp.103-105 (2003).
- [10] T.Park, KG.Shin: *Soft Tamper-Proofing via Program Integrity Verification in Wireless Sensor Networks*, IEEE

- Transaction on Mobile Computing, Vol.4, Issue.3, pp.297-309 (2005).
- [11] X.Du and H.Chen: *SECURITY IN WIRELESS SENSOR NETWORKS*, IEEE Wireless Communications, pp.60-66 (2008).
 - [12] J.Granjal, E.Monteiro and JS.Silva: *Security in the integration of low-power Wireless Sensor Networks with the Internet:A survey*, Ad Hoc Networks, Vol.24, Part A, pp.264-287 (2015)
 - [13] Y.Cho, G.Qu, Y.Wu: *Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks*, IEEE Symposium on Security and Privacy Workshops (SPW 2012), pp.134-141(2012).
 - [14] G.Wang, et al.: *On Supporting distributed collaboration in sensor networks*, Military Communications Conference, 2003. MILCOM '03. 2003 IEEE, Vol.2, pp.752-757 (2003).
 - [15] H.Chen, H.Wu, X.Zhou and C.Gao *Reputation-based Trust in Wireless Sensor Networks*, International Conference on Multimedia and Ubiquitous Engineering (MUE'07), pp.603-607 (2007).
 - [16] S.Ganeriwala, Laura K.Balzano and Mani B.Srivastava *Reputation-based framework for high integrity sensor networks*, ACM Transactions on Sensor Network (TOSN), Vol.4, Issue 3, pp.1-37 (2008).
 - [17] A.Aikebaier, M.Jibiki, Y.Teranishi and N.Nishinaga: *Proposal and Evaluation of a Cooperative Malicious Node Isolation*, IEICE Technical Report IA2013-73, pp.31-36 (2014).
 - [18] 木村圭希, 新居英志, 滝沢泰久: 開放環境無線センサネットワークにおける協調的パケット改竄検知と多数決手法を用いた不正ノード孤立化手法の提案, 情報処理学会研究報告マルチメディア通信と分散処理 (DPS), Vol. 2019-DPS-180, No.17, pp.1-8, (2019).
 - [19] Kohonen, T: *自己組織化マップ (Self-Organizing Maps)*, シュプリンガーフェアラーク東京 (2005)
 - [20] Jaydip Sen: *A Survey on Wireless Sensor Network Security*, IJCNIS, Vol.1, No2, pp.55-78 (2009).
 - [21] A.Perrig, R.Szewczyk, JD.Tygar, V.Wen and DE.Culler: *SPINS:Security protocols for sensor networks*, Wirel. Netw., Vol.8, Issue.5, pp.521-534 (2002).