情報処理学会論文誌 Vol.63 No.2 578–587 (Feb. 2022)

開放環境無線センサネットワークにおける自己組織化マップを用いた改ざんノード協調的排除方式

木村 圭希[1] 新居 英志[2] 滝沢 泰久[3,a)]

受付日 2021年5月10日, 採録日 2021年11月2日

概要：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り，鍵などの秘密情報が不正に取得され改ざんノードがネットワークに混入された場合，従来のデジタル署名やMAC（MessageAuthentication Code）などの鍵の秘密性を前提とする暗号に基づく方式は改ざんを排除できず，データの信頼性が失われることになる．本論文は，開放環境の無線センサネットワークにおいて，鍵に依存せずにデータ改ざん不正に対してデータの信頼性を確保するために，自己組織化マップを用いた改ざんノードの協調的排除方式を提案する．提案方式は，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，さらに，ノード間の相互データ通信における振舞いから，自己組織化マップに基づき正規ノードと改ざん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づいて，改ざんノードを無線センサネットワークから排除する．

キーワード：無線センサネットワーク，改ざん，自己組織化マップ，協調的排除

Cooperative Elimination for Falsification Nodes in Open Environment Wireless Sensor Networks using Self-organizing Maps

Yoshiki Kimura[1] Eiji Nii[2] Yasuhisa Takizawa[3,a)]

Received: May 10, 2021, Accepted: November 2, 2021

Abstract: In open environment wireless sensor networks, it is difficult to eliminate that outsiders physically access a deployed sensor node, and then an outsider may unauthorizedly takes a secure information stored in a sensor node such as encryption key by physical access to a sensor node. Therefore, if a malicious person takes an encryption key and put falsification nodes in networks, conventional encryption scheme, such as a digital signature and MAC (Message Authentication Code), cannot eliminate falsifying data, and then data loses its reliability. In this paper, to defend data against falsification without secure encryption key, we propose cooperative elimination for falsification node using self-organizing maps. The proposing scheme detects falsification nodes by cooperating among proper nodes, furthermore classifies nodes into proper nodes and falsification nodes based on their behavior of the detection using self-organizing maps, and finally eliminates falsification nodes from wireless sensor networks.

Keywords: wireless sensor networks, falsification, self-organizing maps, cooperative elimination

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

1 関西大学大学院理工学研究科
Graduate School of Science and Engineering, Kansai University, Suita, Osaka 564–8680, Japan
2 関西大学先端科学技術推進機構
Organization for Research and Development of Innovative Science and Technology Kansai University, Suita, Osaka 564–8680, Japan
3 関西大学環境都市工学部
Faculty of Environmental and Urban Engineering, Kansai University, Suita, Osaka 564–8680, Japan
a) takizawa@kansai-u.ac.jp

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 2 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]．たとえば，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，悪意のある者は不正な改ざん行為を行うノード（改ざんノード）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方式であるため，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方式は機能しない [12]．

無線センサネットワークにおいて，鍵に依存せずに改ざん行為を検知する方式として Watchdog 方式 [13], [14], [15], [16] が提案されている．しかし，Watchdog 方式では，通信範囲外となるノードの振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改ざんノードを連続して配置し，正規ノードから 1 ホップの改ざんノードは改ざんを行わずに正規ノードから 2 ホップの改ざんノードが改ざん行為を行う [17] 場合，Watchdog 方式では改ざんを実施するノードが通信範囲外となるために，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改ざんノードによる改ざん行為は既存方式では検知できず，無線センサネットワークのデータの信頼性が失われてしまう．

我々は，上記の問題を解決するため，経路上連続する改ざんノードにおいて共通の隣接ノードとなる複数の正規ノードより改ざんを検知（協調的改ざん検知）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，改ざんノードを無線センサネットワークから論理的に孤立化させて，排除する方式（以降，先行方式）[18] を提案した．改ざんノードの孤立化は，改ざんを検知したノードが自身の経路表から改ざんノードを消去し，さらに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，改ざんノードをネットワークのデータ転送経路上から完全に排除することである．先行方式は，改ざん転送と不正孤立化を発信するノードが混在する無線センサネットワークにおいて，改ざん転送および不正孤立化を行うノード数が正規ノード数より少ないという条件で，これらをネットワークから排除して，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，先行方式は，ネットワークの局所域において改ざん転送および不正孤立化を行う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排除されるという問題がある．

本論文は上記の問題を解決するために，協調的改ざん検知に基づき，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孤立化パケット通信の振舞いから正規ノードと不正孤立化を行うノードへクラスタリングし，その結果により改ざんおよび不正孤立化を行うノードを孤立化対象としてネットワークから排除する改ざんノード協調的排除方式を提案する．

2. 関連研究

2.1 Message Authentication Code

MAC（Massage 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分かる（**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見なされる．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

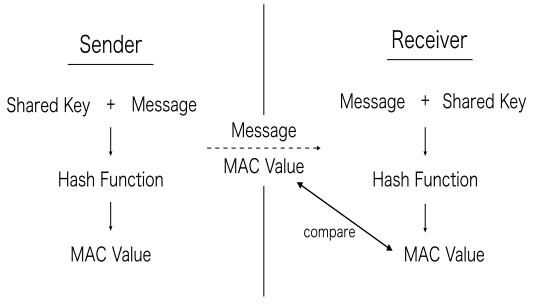

図 1 MAC: Message Authentication Code
Fig. 1 MAC: Message Authentication Code.

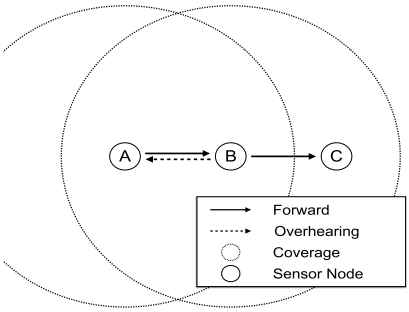

図 2 Watchdog 方式
Fig. 2 Watchdog mechanism scheme.

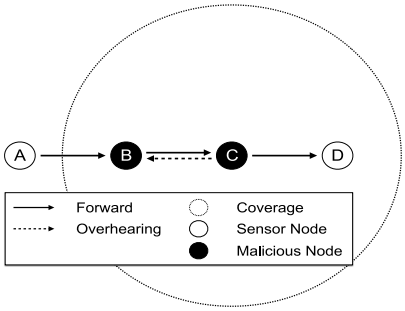

図 3 経路上連続するノードによる改ざん行為
Fig. 3 Falsification with two successive nodes on a route.

ても，正規ノードによる検知は不可能となる．

2.2 Watchdog mechanism を用いた改ざん検知

鍵を用いず改ざんを検知する方式である Watchdog 方式について説明する．**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 が正しく中継を行ったかどうかを確認することができる．この方式は鍵に依存しない方式であるため，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，この方式は送信ノード自身が中継ノードの振舞いをモニタリングする方式であるため，通信範囲外のノードの振舞いを監視することはできない．

2.3 経路上連続するノードによる改ざん

図 3 に経路上連続するノードによる改ざんを示す．ノード A からノード D への経路上においてノード B とノード C が連続する場合，すなわちノード B はノード A から 1 ホップノード，ノード C はノード A から 2 ホップノードである場合，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 に転送し，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．この場合，Watchdog 方式を用いてノード 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 も改ざんノードであるため，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 方式は改ざん検知が困難となり，改ざんデータの混在により無線センサネットワークデータの信頼性を失うことになる．

3. 先行方式

先行方式では，Watchdog 方式の問題を解決するために，経路構成ノードではない複数正規ノードを用いた協調的改ざん検知と不正孤立化を判定するノード間多数決を用いた不正孤立化ノード排除方式を提案した．以下に，先行方式の詳細を説明し，その後に先行方式の既存方式との相違を示す．

3.1 ノードの定義

先行方式において，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：改ざん転送および不正孤立化発信を行わないノード．
- 協調ノード：任意の経路上のデータ転送ノードと転送データ受信ノードに共通して隣接する正規ノード．
- 改ざんノード：パケット転送の際にパケット改ざんを行うノード．または，隣接改ざんノードによる改ざん行為を隠蔽するノード．
- 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排除する孤立化パケットを発信するノード．
- 不正ノード：改ざんノードと不正孤立化ノードの総称．

3.2 協調的改ざん検知と改ざんノードの排除

協調的改ざん検知は，パケット転送正規ノードと複数の協調ノードが行う．以下に，Watchdog 方式では検知できない経路上連続するノードによる改ざん行為における協調的改ざん検知の処理について述べる．**図 4** において，ノード A，D，E は正規ノードで，ノード B，C は改ざんノードである．ノード A，B，C，D は連続して経路を構成し，ノード E は当該経路を構成するノードでなく，またノード 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 は改ざんノードであるがパケット改ざんを行わずに転送を行い，ノード C は受信パケットを改ざんし転送を行う．ノード C が行うパケット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．先行方式において，協調ノード E はノード B と C の両方の隣接ノードあるため両方の転送パケットを傍受することが可能であり，その 2 つのパケットを比較することで改ざん検知が可能となる．

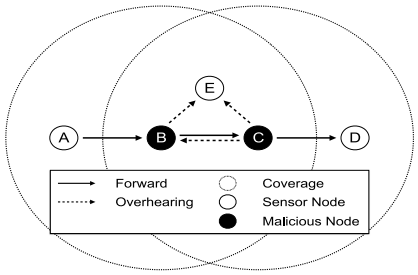

図 4 協調的検知
Fig. 4 Cooperative detection for falsification.

改ざんを検知したノードは，経路表に改ざんノードが存在する場合，改ざんノードを経路表から削除し，ブラックリストに登録する．さらに，隣接ノードへ改ざん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．孤立化パケット受信ノードは，経路表に孤立化対象ノードが存在する場合，孤立化対象ノードを経路表から削除し，ブラックリストに登録する．また，孤立化対象ノードが隣接ノードである場合は孤立化パケットを隣接ノードへ転送する．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．また，経路再構成の際に転送先として改ざんノードを選択することを排除する．以上を孤立化処理と呼ぶ．

3.3 ノード間多数決を用いた不正孤立化ノードの排除

先行方式では，すべてのノードに協調的検知と孤立化パケット送信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，すべてのノードに協調的検知と孤立化パケット送信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．したがって，先行方式では，協調的改ざん検知により改ざんノードを排除するとともに，不正孤立化ノードを排除するために，ノード間での多数決を用いて，不正孤立化ノードを孤立化する方式を提案した．

ノード間多数決は孤立化関与回数を用いて実施する．孤立化関与回数は孤立化に関わった回数を示し，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元の場合

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，多くのノードが孤立化の対象とするノードが改ざんノードである（多数）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処理する．一方で，隣接に改ざんノードが多数存在する場合，当該ノードの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，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．採用されない孤立化パケットを送信し続けるノードはその孤立化関与回数が増加し，いずれは孤立化対象ノードとなる．すなわち，採用されない孤立化パケットを送信し続けるノードは少数の不正孤立化ノードとして判別されて孤立化処理される．

以上により，先行方式は改ざんノードと不正孤立化ノードをネットワークから排除する．

3.4 無線センサネットワークにおける不正ノード検知

無線センサネットワークでは，ノードの振舞いを監視することにより不正ノードなどを検知する方式が提案されている．文献 [22], [23], [24], [25], [26], [27], [28] は，個々のノードが隣接ノードの振舞いから不正ノードあるいは，自身の電力温存のために転送すべきパケットの廃棄などを行うセルフィッシュなノードを検知する方式であり，文献 [28] は先行方式と同様に周囲のノードと協調する方式である．しかし，これらの方式は経路制御方式において，不正ノードあるいはセルフィッシュなノードの検知による安全な経路の構築を目的としており，データパケットの改ざんは扱っていない．

文献 [29] はシンクサーバに到着したデータの改ざんをバックトレース法により検知する方式である．この方式は MAC を多層化した方式で，各ノードは自身の ID と固有のハッシュキーにより MAC 値を生成し，これをデータに付与し転送する．シンクサーバはすべてのノードのハッシュキーを保持しており，受信したデータに付与された MAC 値と個々のノードのハッシュキーを用いて受信メッセージの MAC 値を生成して，これらを比較することで改ざん検知を行う．この方式は全ノードで生成した MAC 値とシンクサーバまでの経路情報を転送する必要があるためトラフィックが増大する．また，ノード ID が改ざんされた場合，データ改ざんの有無は検知可能であるが，改ざんを行ったノードの特定はできない．以上から，先行方式は文献 [22], [23], [24], [25], [26], [27], [28] と異なるパケット改ざん問題を対象として，文献 [29] とも異なり鍵に依存せずに改ざんノードを検知する．

4. SOM を用いた改ざんノード協調的排除方式

先行方式では，Watchdog 方式と比較して，高い改ざんノード検知率を示し，またそれらをネットワークから排除可能であるためその有用性は高い．しかし，先行方式では局所的に不正ノード（改ざんノードまたは不正孤立化ノー

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，正規ノードを孤立化処理するという問題がある．したがって，提案方式である改ざんノード協調的排除方式では上記の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舞いからクラスタリングを行い，その結果により孤立化処理を行うことで，不正ノードのみをネットワークから排除する方式を提案する．

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

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．

以下に，提案方式においてSOMを利用する理由を述べる．クラスタリング手法には，K-Means法 [30]，c-Means法 [31]，学習ベクトル量子化（Learning Vector Quantization: LVQ）[32] などがあるが，K-Means法やc-Means法は事前にクラスタ数を設定する必要があり，LVQは教師データが必要となる．しかし，不正ノードの振舞いは不明であるため，クラスタ数の設定や教師データの用意は困難である．SOMはクラスタ数の設定や教師データが不要であり，多様な不正ノードの振舞いに応じてクラスタリング可能である．また，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ため，今後入力データを高次元化することが可能性である．以上のことから，SOMを利用する．

4.2 孤立化パケット送信における振舞いデータ

提案方式では，先行方式と同様に，協調的改ざん検知を実施し，自身で検知した改ざんノードに対して孤立化処理を行う．孤立化処理で送信される孤立化パケットを受信したノードは，その受信孤立化パケットから次の2項目を隣接ノードの孤立化パケット送信における振舞いデータとする．

- 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

1項目目（孤立化パケットの作成回数）における正規ノードと不正孤立化ノードの振舞いは，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：改ざんの有無にかかわらず孤立化パケットを送信する．

2項目目（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孤立化ノードの振舞いは，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．

提案方式では，上記に示した正規ノードと不正孤立化ノードの振舞いの違いからSOMを用いて，正規ノードと不正孤立化ノードをクラスタリングする．

4.3 SOMを用いた孤立化パケット送信によるクラスタリング

SOMを用いた孤立化パケット送信の振舞いからノードをクラスタリングするアルゴリズムは以下のとおりである．

(1) 一定期間，正規ノードは隣接ノードの孤立化パケットをモニタリングし，前述の孤立化パケット送信における振舞いデータを取得する．

(2) 各ノードの孤立化パケット送信回数，孤立化対象IPアドレスによる振舞いデータをそれぞれのSOMの位置ベクトルとし，各ノードにおいてSOMに基づき次のようにクラスタリングを行う．

step1 自身と隣接ノードからランダムに勝者ノードを1つ選択する．

step2 勝者ノードの位置ベクトルに基づき他のすべてのノードの位置ベクトルを次のように更新する．

$$m_i(t+1) = m_i(t) + h_{c,i}(t) \cdot (c(t) - m_i(t)) \quad (1)$$

$$h_{c,i}(t) = \alpha(t) \cdot \exp\left(-\frac{||c(t) - m_i(t)||^2}{2\sigma^2(t)}\right) \quad (2)$$

$c(t)$ は t 回目更新時の勝者ノードの位置ベクトル，$m_i(t)$ は t 回目更新時の勝者ノードの以下のノード i の位置ベクトル，$\alpha(t)$ は t 回目更新時の学習係数，$\sigma^2(t)$ は t 回目更新時の学習範囲調整パラメータである．

step3 更新回数が設定数（n）に至ってない場合step1に戻り，それ以外は終了する．

さらに，より強く明確なクラスタリングするため，上記の処理を2回実施する2フェーズ処理とする．第1フェーズの位置ベクトル更新では，広い範囲（式 (2) の σ^2 を小さな値）のノードを対して学習を与え，第2フェーズでは，狭い範囲（式 (2) の σ^2 を大きな値）のノードに対して学習を与える．

(3) クラスタリングされた結果から，自身と他ノードとのSOMの位置ベクトルからノード間距離を計算する．ノード間距離が閾値（d_t）よりも小さいノード，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（d_t）よりも大きいノード，すなわち，孤立化パケット送信において自身と異なる振舞いをするノードを信頼できないノードと判断する．

SOM クラスタリング結果による信頼できるノードグループと信頼できないノードグループのクラスタ化とこれら隣接ノードの孤立化パケット内容に基づいて，次のように孤立化処理を実施する．孤立化処理は先行方式と同様とする．

- 信頼できるノード（SOM 位置ベクトル空間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孤立化処理を実施する．これにより自身で検知できない改ざんノードを排除する．
- 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孤立化ノードとして，孤立化パケット送信元ノードを対象に孤立化処理を実施する．これにより不正孤立化ノードを排除する．
- 上記以外は，信頼できないノード（SOM 位置ベクトル空間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

5.1 評価方法

提案方式の有効性を示すために，NS3 を用いてシミュレーション評価を行う．シミュレーションは各ノード数の組合せごとに 10 回試行し，その平均値を評価結果とした．

ノード数を 100 として，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．不正ノードとは，先行方式と同様に，改ざん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を行う不正孤立化ノードとする．不正孤立化ノードは，作為的なビザンチン故障 [33] と同等であると想定し，規則的または不規則的な周期で不正孤立化パケットを送信する．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．**表 1** にそのシミュレーション諸元を示す．

センサネットワークではセンシングしたデータをシンクサーバへ集約し，そのデータをもとに解析・制御を行うため，データ取得を行う正規ノードの数やシンクサーバに到達するデータの完全性が担保されているかが重要となる．そこで本シミュレーション評価では，上記のノード構成において，Watchdog 方式，先行方式，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
- シンクサーバ到着データにおける改ざん率

表 1 シミュレーション諸元
Table 1 Parameters for simulation.

試行回数	10
フィールド空間	1,000 m × 1,000 m
ノード配置	ランダム
正規ノード数	90，80，70，60，50
改ざんノード数	5，10，15，20，25
不正孤立化ノード数	5，10，15，20，25
n	200
d_t	0.06
シミュレーション時間	1000 sec
データサイズ	12 bytes
無線通信	IEEE802.11b
通信カバレッジ	250 m
ルーティングプロトコル	AODV

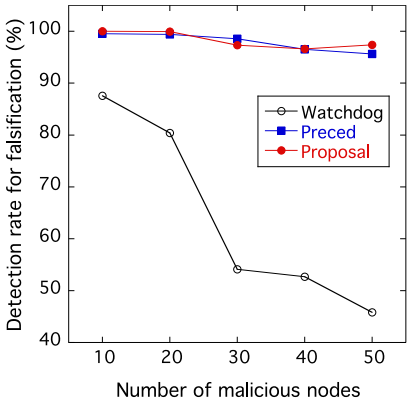

図 5 改ざん検知率
Fig. 5 Detection rate for falsification.

5.2 評価結果と考察

5.2.1 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 方式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，先行方式と提案方式では，協調的改ざん検知を行っているため，Watchdog 方式では検知不可能な連続する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，先行方式では 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．

先行方式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

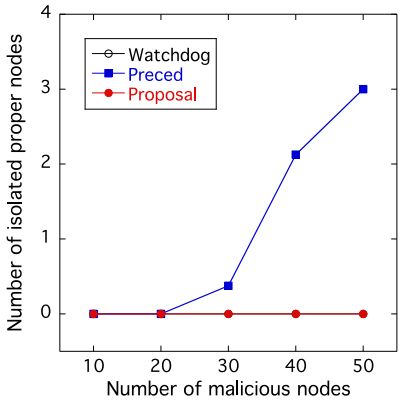

図 6 正規ノード孤立化数
Fig. 6 Number of isolated proper nodes.

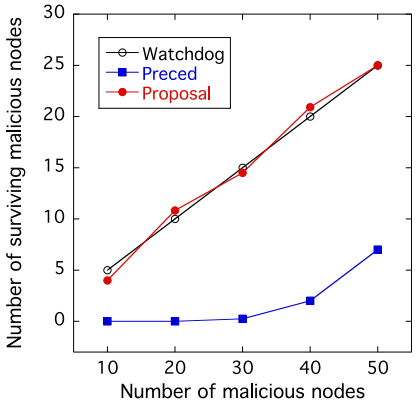

図 7 残存不正ノード数
Fig. 7 Number of surviving malicious nodes.

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．

先行方式と提案方式はどちらも協調的改ざん検知を行っているが，改ざん検知率に若干の差異がみられる．これは，**図 6** で後述するような不正な孤立化による正規ノード数の減少に起因して，協調的検知が機能する条件を満たさない箇所が存在するためであると考えられる．

5.2.2 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．すべ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 方式では，孤立化を行わないので正規ノード孤立化数は 0 になる．先行方式では，多数決を行ため，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．

5.2.3 残存不正ノード数

残存不正ノード数の評価結果を**図 7** に示し，**図 8** に残存不正ノードの内訳を示す．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 方式では，孤立化が行われないため，すべての不正ノードが残存する．なお，Watchdog 方式では孤立化を行わないため，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．

先行方式では，不正ノードの割合が 30%以上の場合，不正ノードが残存する．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．

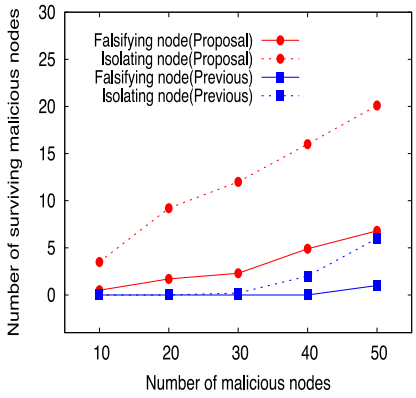

図 8 残存不正ノード数の内訳
Fig. 8 Details of number of surviving malicious nodes.

一方，提案方式では多数の不正ノードが残存する．この原因は，SOM の位置ベクトル空間において，不正孤立化ノードグループと正規ノードグループにクラスタ化されるが，さらに，正規ノードグループが隣接に改ざんノードが存在するノードグループと隣接に改ざんノードが存在しないノードグループにクラスタ化され，この 2 つの正規ノードグループ間において信頼関係がないためと考えられる．また，図 8 から分かるように，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．

この正規ノードの 2 グループへのクラスタ化が多数の不正孤立化ノードを残存させる理由を次に示す．

正規ノード A とのノード間距離が近い正規ノードグループをグループ g1，正規ノード A とのノード間距離が遠い正規ノードグループをグループ g2 と仮定したうえで，以下の 2 つの場合を考える：

- 不正孤立化ノード X が正規ノード A へグループ g1 のノードを孤立化対象ノードとする孤立化パケットを送信した場合
- 不正孤立化ノード X が正規ノード A へグループ g2 の

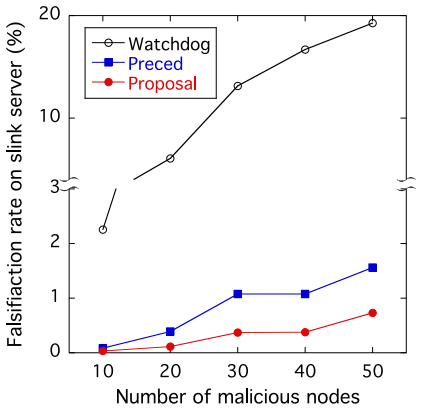

図 9 シンクサーバにおけるデータ改ざん率
Fig. 9 Falsification rate on arrival data to sink server.

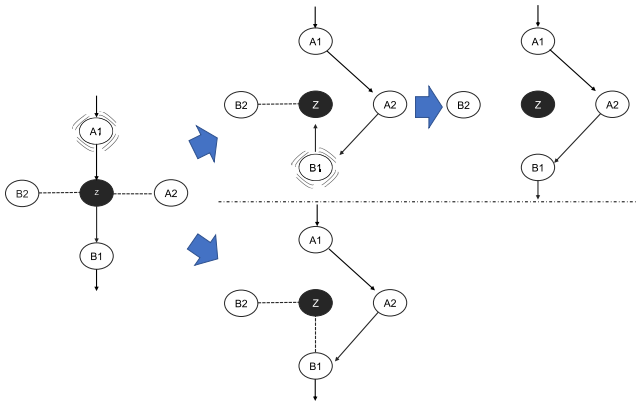

図 10 改ざんノードの迂回
Fig. 10 Detoure route for falsification nodes.

ノードを孤立化対象ノードとする孤立化パケットを送信した場合

不正孤立化ノード X が正規ノード A へグループ g1 のノード（ノード間距離が近いノード）を孤立化対象ノードとする孤立化パケットを送信する場合において，グループ g1 に属するノード 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 に対して孤立化処理を実施し，ノード X を孤立化対象とする孤立化パケットを送信する．この孤立化パケットを受信したグループ g2 に属するノードは，ノード X が信頼できないノードであり，かつグループ g1 に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 が正規ノード A へグループ g2 のノードに対して孤立化パケットを送信した場合において，グループ g1 に属するノード A は，ノード X が信頼できないノードであるため，孤立化パケットを破棄し，孤立化処理は行わない．

以上のことから，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させることができないことがある．

5.2.4 シンクサーバにおける改ざん率

シンクサーバにおける改ざん率の評価結果を**図 9** に示す．シンクサーバにおける改ざん率（以降，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 方式では，孤立化が行われないため，不正ノード数に比例して改ざん率が増加する．先行方式と提案方式では，Watchdog 方式と比較して改ざん率を抑えることができている．

先行方式では，図 7 に示すように改ざんノードを孤立化させることによって改ざん率を抑えることができていると考えられる．

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方式より改ざん率を抑えることができている．

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にもかかわらず改ざん率を抑えることができた理由を述べる．

正規ノード A1 とのノード間距離が小さい正規ノードグループをグループ g1，正規ノード A1 とのノード間距離が大きい正規ノードグループをグループ g2 と仮定する．**図 10** 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．波線はリンク，実線矢印は経路を構成するリンクを示す．

グループ g1 のノード A1 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．グループ g1 のノード A2 はこれを採用するが，グループ g2 のノード B1/B2 はこれを破棄してノード Z へのリンクを保持する．以上の状況でノード A1 がノード Z を迂回してノード A2 へ，ノード A2 は B1 へ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経路を構成する可能性がある．ノード B1 がノード Z へ転送する経路構成の場合は，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 と同じグループ g2 のノード B2 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（図 10 上段）．仮にノード B1 がノード Z 以外のノードへ転送する経路を構成する場合，ノード B1 とノード Z，ノード B2 とノード Z のリンクが残存するが，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（図 10 下段）．したがって，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残存するにもかかわらず改ざん率を抑えることができている．

5.2.1 項〜5.2.4 項の結果より，提案手法は多くの改ざんを検知できている．また，不正ノード孤立化において多数の不正ノードが残存しているが，そのほとんどが不正孤立化ノードである．正規ノードは，SOM を用いたクラスタリングにより，残存孤立化ノードからの孤立化パケットを自身とは異なるクラスタのノード（信頼できないノード）からの要求として破棄し，正規ノードの不正な孤立化を排除する．さらに，前段落で述べたように，残存している改ざんノードと正規ノードのリンクはシンクサーバまでの転送経路に用いられない不要リンクとなる．すなわち，改ざんノードの一部の正規ノードへのリンクは遮断されていないが，改ざんノードはシンクサーバまでの経路において迂回され，その経路において孤立化されていることに相当する．以上の点から，残存改ざんノードがシンクサーバまでの経路を持たず，最終的にシンクサーバーに到達する改ざんデータ率は比較方式の中で最も低くなる．

6. まとめ

本論文では，鍵の秘密性が失われた無線センサネットワークにおいて，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 を用いて孤立化パケット通信における振舞いから正規ノードと不正孤立化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し排除する方式を提案した．提案方式は，先行方式と同様に協調的検知により既存方式では検知困難な改ざんを検知するとともに，先行方式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．

一方で，提案方式では，SOM 位置ベクトル空間において正規ノードが 2 つのグループに分かれるために不正ノードが残存する．残存不正ノードは経路再構成において経路構成ノードになり，その不正検知までの一時的な期間において改ざんデータがシンクサーバへ到達する可能性がある．

今後の課題として，上記の問題を解決するために，孤立化パケット送信における振舞いデータを高次元化して，正規ノードを 1 グループにまとめて不正ノードを完全に排除する方式を検討する．また，提案方式を無線センサネットワークにおけるポイズニングへの適用を検討する予定である．

参考文献

[1] Illiano, V.P. and Lupu, E.C.: 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] Bartariya, S. and Rastogi, A.: Security in Wireless Sensor Networks: Attacks and Solutions, *IJARCCE*, Vol.5, No.3, pp.214–220 (2016).

[4] Perrig, A., Stankovic, J. and Wagner, D.: Security in wireless sensor networks, *Comm. ACM*, Vol.47, No.6, pp.53–57 (2004).

[5] Prasanna, S. and Rao, S.: An Overview of Wireless Sensor Networks, *IJSCE*, Vol.2, No.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の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] Karlof, C., Sastry, N. and Wagner, D.: TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, *SenSys '04 Proc. 2nd International Conference on Embedded Networked Sensor Systems*, pp.162–175 (2004).

[8] Pamavathi, G. and Shanmugapriya, D.: A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, *IJCSIS*, Vol.4, No.1, pp.1–9 (2009).

[9] Chan, H. and Perrig, A.: Security and Privacy in Sensor Networks, *Computer*, Vol.36, No.10, pp.103–105, IEEE Computer Society (2003).

[10] Park, T. and Shin, K.G.: Soft Tamper-Proofing via Program Integrity Verification in Wireless Sensor Networks, *IEEE Trans. Mobile Computing*, Vol.4, No.3, pp.297–309 (2005).

[11] Du, X. and Chen, H.: SECURITY IN WIRELESS SENSOR NETWORKS, *IEEE Wireless Communications*, pp.60–66 (2008).

[12] Granjal, J., Monteiro, E. and Silva, J.S.: 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] Cho, Y., Qu, G. and Wu, Y.: 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] Wang, G. et al.: On Supporting distributed collaboration in sensor networks, *Military Communications Conference, 2003. MILCOM '03*, Vol.2, pp.752–757, IEEE (2003).

[15] Chen, H., Wu, H., Zhou, X. and Gao, C.: Reputation-based Trust in Wireless Sensor Networks, *International Conference on Multimedia and Ubiquitous Engineering* (*MUE'07*), pp.603–607 (2007).

[16] Ganeriwal, S., Balzano, L.K. and Srivastava, M.B.: Reputation-based framework for high integrity sensor networks, *ACM Trans. Sensor Network* (*TOSN*), Vol.4, No.3, pp.1–37 (2008).

[17] Aikebaier, A., Jibiki, M., Teranishi, Y. and Nishinaga, N.: 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] Sen, J.: A Survey on Wireless Sensor Network Security,

IJCNIS, Vol.1, No.2, pp.55–78 (2009).
[21] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V. and Culler, D.E.: SPINS: Security protocols for sensor networks, *Wirel. Netw.*, Vol.8, No.5, pp.521–534 (2002).
[22] Buchegger, S. and Boudec, J.Y.L.: Performance analysis of the CONFIDANT protocol, *MobiHoc'02*, pp.226–236 (2002).
[23] Buttyan, L. and Hubaux, J.P.: Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks, *Mobile Networks and Applications*, pp.579–592 (2003).
[24] Zhong, S. and Chen, J.: Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks, *IEEE INFOCOM 2003, 22nd Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol.3, pp.1987–1997 (2003).
[25] 横山 信，中根由和，高橋 修，宮本衛市：アドホックネットワークにおける高精度な不正動作ノードの検知と防御方式の提案および実装評価，情報処理学会論文誌，Vol.49, No.2, pp.639–649 (2008).
[26] Yu, W., Sun, Y. and Liu, K.J.R.: HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks, *IEEE INFOCOM*, Vol.2, pp.1252–1261 (2005).
[27] Wang, G., Zhang, W., Cao, G. and Prota, T.: On supporting distributed collaboration in sensor network, *IEEE MILCOM* (2003).
[28] Yang, H., Shu, J., Meng, X. and Lu, S.: SCAN: Self-organized network layer security in mobile ad hoc networks, *IEEE Journal on Selected Areas in Communication*, Vol.24, No.2, pp.261–272 (2006).
[29] Ye, F., Yang, H. and Liu, Z.: Catching "moles" in sensor networks, *IEEE ICDCS* (2007).
[30] Arthur, D.: k-means++: The advantages of careful seeding, *Proc. 8th Annual ACM-SIAM Symposium on Discrete Algorithm*, pp.1027–1035 (2007).
[31] Havens, T.C., Bezdek, J.C., Leckie, C., Hall, L.O. and Palaniswami, M.: Fuzzy c-Means Algorithms for Very Large Data, *IEEE Trans. Fuzzy Systems*, Vol.20, No.6, pp.1130–1146 (2012).
[32] Hollmen, J., Tresp, V. and Simula, O.: A learning vector quantization algorithm for probabilistic models, *2000 10th Eur. Signal Process. Conf.*, pp.1–4 (2000).
[33] Sota, N. and Higaki, H.: Byzantine failure detection in wireless ad-hoc networks, *2015 36th IEEE Sarnoff Symposium*, pp.173–178 (2015).

木村 圭希 （学生会員）

2019 年関西大学環境都市工学部都市システム工学科卒業．関西大学大学院博士課程前期課程において無線センサネットワークにおける協調的改竄検知と不正ノード孤立化手法の研究に従事．

新居 英志 （正会員）

2020 年関西大学大学院博士課程後期課程修了．2020 年国際電気通信基礎技術研究所波動工学研究所研究員．2021 年関西大学先端科学技術推進機構ポスト・ドクトラル・フェロー．現在，無線ネットワークにおける群知能等の研究に従事．博士（工学）．

滝沢 泰久 （正会員）

1983 年京都工芸繊維大学工芸学部機械工学科卒業．同年日本ユニシス（株）入社．1990 年住友金属工業（株）入社．1998 年 ATR 環境適応研究所出向．2002 年 ATR 適応コミュニケーション研究所主任研究員．2008 年同研究所上級主任研究員．2009 年関西大学環境都市工学部准教授，ATR 適応コミュニケーション研究所客員研究員．2014 年関西大学環境都市工学部教授．現在，無線ネットワークにおける自己組織化等の研究に従事．博士（工学）．電子情報通信学会，IEEE，IEEE-CS 各会員．