Vol.2019-DPS-180 No.17
Vol.2019-EIP-85 No.17
2019/9/20

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

木村　圭希[1]　新居 英志[1]　滝沢 泰久[2]

概要：開放環境に設置された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を不正に取得される可能性がある. この場合，不正に取得した鍵を用いることで認証をすり抜け，改ざんなどの不正を行うノードをネットワークに混入させることが可能となる. 従来ネットワーク上での改ざん検知はデジタル署名を用いてきた. また，計算機資源や消費電力に制約がある無線センサネットワークでは簡易な署名である MAC(Message Authentication Code) を用いて改ざん検知を行う. しかし，これらの手法は鍵の秘密性が担保されていることが必須である. すなわち，上記のような鍵の秘密性が破綻した状況では全く機能せず， データの信頼性を完全に失う. 本稿は，鍵に依存せずにデータの信頼性を確保するため，複数のノードの協調により改ざんを行う不正ノードを検知し，検知した不正ノードをネットワーク内に存在するノードの中で多数決をとることによって, 論理的に無線センサネットワークから孤立化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

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配備されることが考えられる．配備される環境は，オフィスなど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できる．開放環境ではその環境の特性から，第三者による端末への物理的な接触を完全に遮断することは難しく，悪意のある者が端末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 [2] [3] [4] [5]．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 [6] [7] [8] [9]．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 [10] [11]．従来ネットワーク上での改ざん検知は，共通鍵方式が広く利用されている．端末の計算機資源や消費電力に制約があるセンサネットワークでは，簡易な署名である MAC(Message Authentication Code) を用いて改ざん検知を行う [12]．しかし，共通鍵方式や MAC は鍵の秘密性の担保を前提とする手法である．つまり，鍵が第三者に漏洩していないこと状況でのみ有効に機能する手法であるため，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手法は機能しない．それゆえに，無線センサネットワークはデータの信頼性を失う [13].

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 が提案されている [14] [15]．この手法は，ノード自身が隣接ノードの振る舞いをモニタリングし，の不正な廃棄等を検知する仕組みである．Watchdog mechanism は [16] [17]，隣接ノードの振る舞いをモニタリングする際に，自身の送信したと隣接ノードが送信したを傍受し比較することで，改ざん検知へ適用できる．しかし，Watchdog mechanism はモニタリングを行うノードは隣接しているノードの振る舞いは監視できるが，通信範囲外となるノードの振る舞いはモニタリングすることができない．そのため，Watchdog mechanism において，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，一方の不正ノードが他方の不正ノードの不正行為を隠蔽することで [18]，改ざん行為が可能となる．

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で取得したデータに改ざんされたデータが混在することにな

[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

る．すなわち，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．

先行研究 [1] は，上記問題を解決するため，複数の正規ノード（ネットワーク構成時のノード）の協調により改ざんを行う不正ノードを検知し，検知した不正ノードを倫理的に無線センサネットワークから孤立化する手法を提案した. 孤立化は，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から除外することである. 先行研究は，既存手法の比較評価により，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，先行研究は改ざんの検知も孤立化も正規ノードのみが行なっている，従って，正規ノードが電池交換やノードの故障によりネットワークから離脱した場合，正規ノード数が減少することを想定すると，検知率が著しく低下することが考えられる．本稿では，この問題を解決するために協調的検知と孤立化の権限を全てのノードに付与し，ネットワーク内のノードで多数決を取ることで正規ノード数に依存せずに高い検知率を保ち，かつ悪意のないノードが不正な孤立化をされない手法を提案する．

2. 関連研究

2.1 Message Authentication Code

MAC(Massage Authentication Code) 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 [22]．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) [23]．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．

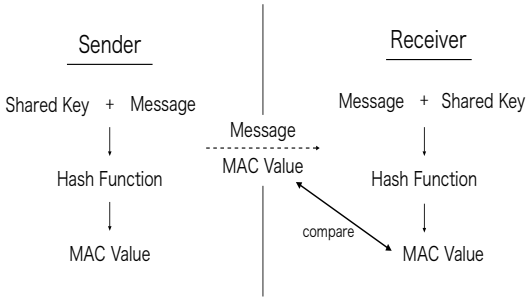

図 1 Message Authentication Code

2.2 Watchdog mechanism を用いた改ざん検知

以下に，Watchdog mechanism を用いた改ざん検知手法について述べる．

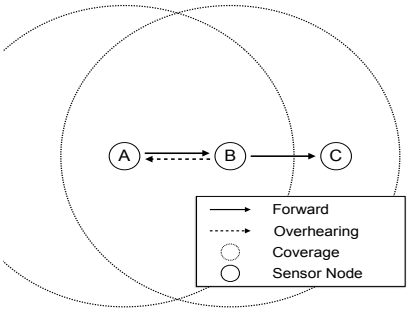

図 2 Watchdog mechanism

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 が送信したを傍受しノード A 自身が送信したと比較することで，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．

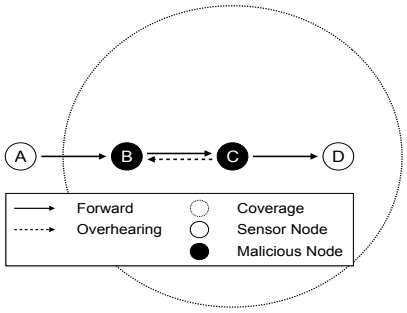

図 3 改ざんの隠蔽

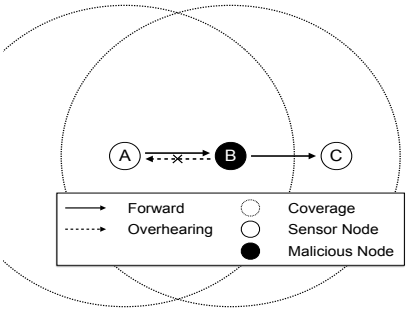

図 4 傍受の失敗

2.2.1 改ざんの隠蔽

図 3 に不正ノードが連続してを中継する場合を示す．ノード B は自身ではの改ざんを行わずノード C に中継をする．を受け取ったノード C は転送の際にを改ざんするが，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．

2.2.2 Watchdog mechanism のロスへの耐性

図 4 にように，モニタリングを行うノードが監視対象ノードの傍受に失敗すると，振る舞いをモニタリングできなくなる．すなわち，ロスが頻繁に発生するネットワークでは，改ざんの検知漏れの可能性が高くなる．次に，鍵を用いずかつ， 連続する不正ノードによる改ざんの検知を行う手法である先行研究について説明する．

2.3 先行研究

先行研究 [1] である協調的検知と不正ノード孤立化手法について述べる．以下に， 各種ノードの定義と手法の詳細を示す．

2.3.1 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：ネットワークが構築された時点でのノードを正規ノードとする．の送信と中継，孤立化パケットの送信を行う．
- 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．
- 監視対象ノード：監視対象ノードは，ネットワークへの新規参入ノード，及び再参加ノードを監視対象ノードとする．の中継のみが許可され，自身発のの送信は許可されない．
- 新規参入ノード：ネットワーク構築後，新たにネットワークに参入してきたノードを新規参入ノードとする．
- 再参加ノード：正規ノードが一時的にネットワークを離脱し，その後ネットワークに再参加したノードを再参加ノードとする．
- 不正ノード：監視対象ノードにおいて，中継の際に改ざんを行うノード，他の不正ノードの改ざん行為を隠蔽するノードを不正ノードとする．
- 孤立化対象ノード：正規ノードによって改ざん行為を検知された不正ノードを孤立化対象ノードとする．

ネットワークへの新規参入ノードは，悪意のある第三者によって設置された不正ノードである可能性が考えられる．再参加ノードも，不正行為を行うようにセンサノード内のコードを第三者によって書き換えられた正規ノードであることが考えられる．このことから，新規参入ノード，再参加ノードの 2 つを監視対象とする．

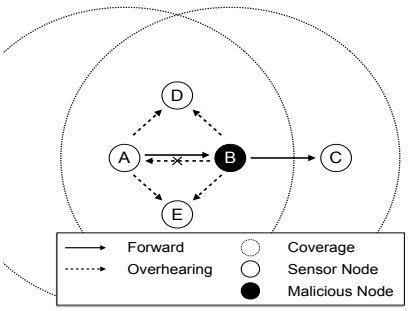

図 5 協調ノードによる改ざん検知

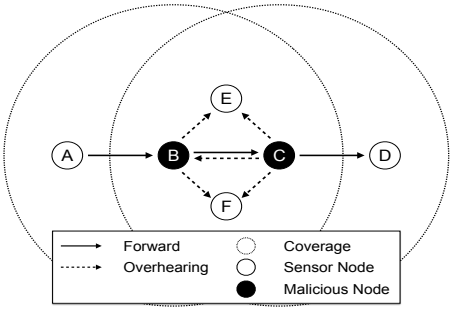

図 6 改ざんの隠蔽に対する検知

2.3.2 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．図 5 に協調的改ざん検知を示す．ノード A，C，D，E は正規ノードで，ノード B は不正ノードである．ノード A，B，C は経路上に連続して配置され，ノード D，E はノード A，B の共通の隣接ノードであり協調ノードである．ノード B がノード A からのを改ざんしノード C へ転送したとき，ノード A は自身が送信したとノード B が転送したを比較することによって，ノード B の改ざんを検知することができる．さらに，協調ノードである D，E もノード A，B の送信したを傍受できるためノード B の改ざんを検知できる．

次に，不正ノードが経路上に連続して存在する場合を考える．図 6 において，ノード A，D，E，F 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，F 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 はを改ざんし転送を行う．この時，ノード A，D はそれぞれノード C，B が送信したを傍受することができないため，改ざんの検知はできない．このような改ざんは Watchdog mechanism では検知できない．しかし，協調的改ざん検知において，ノード E，F はノード B，C のを傍受することが可能であり，その二つのの中身を比較することで改ざん検知が可能となる．

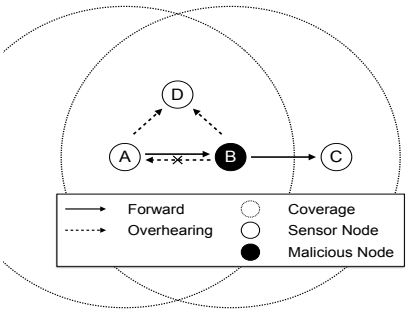

図 7 傍受失敗における協調的検知と Watchdog の比較

さらに，図 7 のようにノード A が中継の傍受に失敗した場合を考える．Watchdog においては，電波衝突によるロスなどによって送信ノードが中継の傍受に失敗をすると，中継ノードの振る舞いを監視できず改ざんを検知することが不可能となる．一方，提案手法では複数の正規隣接ノードが中継ノードの監視を行う．そのため，中継ノードが送受信するをより多くのノードで監視することができ，電波干渉によるランダムなロスに対して耐性が高く，検知漏れを防止できる．以上により，協調的改ざん検知は改ざんを検知するとともに，改ざんを行った不正ノードも検知する．改ざんを行った不正ノードを検知したノードは，その不正ノードをネットワークから孤立化するステップに移行する．

2.3.3 不正ノードの孤立化

図 8 に孤立化のフローを示す．改ざん行為を検知したノードは，孤立化対象ノードの存在を隣接ノードへ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対象ノードの IP アドレスが格納されており，孤立化パケットを受信したノードはその 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．

孤立化パケットを受け取ったノードは，パケットに記載されている孤立化対象ノードが自身の隣接ノードに存在するかを確認し，存在する場合はパケットを受理し隣接ノードへ転送する．存在しない場合は孤立化パケットを破棄する．すなわち，孤立化パケットを孤立化対象ノードの隣接ノードの周辺に限定して通知することにより，その通信量を抑制できる．

孤立化パケットを受理したノード，すなわち，不正ノードに隣接する正規ノードは，その経路表に孤立化対象ノードが存在する場合は，孤立化対象ノードを現在の経路表から削除し，転送先として不正ノードを排除する．また，その不正ノードをブラックリストへ登録する．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，一度不正を働いたノードが経路に再参加することを防ぐ．不正ノードの孤立化はデータの信頼性を確保するとともに，改ざん行為を排除するため，正規の到達率を向上させる．

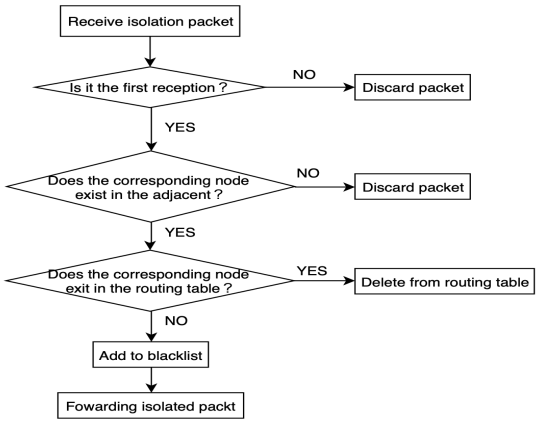

図 8 孤立化の手順

3. 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，先行研究は改ざんの検知と不正ノードの孤立化の権限を正規ノードにのみ与えている．つまり，正規ノード数が減少すると検知率が著しく低下することが想定される．

先行研究において正規ノード数への依存性をなくすために，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悪意のないノードを孤立化させることでネットワークが壊滅することが想定される．

そこで，提案手法では全てのノードに孤立化の権限を付与することで検知率を上昇させ，かつ不正な孤立化が成立しないことを目的とする。

本稿では，不正ノードによる改ざん検知，不正ノード排除，不正孤立化を対象として議論し，不正ノードによる不正データの発信は扱わないこととする．

また，今回の検証では正しいノードが多数を占め，悪意のあるノードが少数を占める状況を想定している．

3.1 改竄検知

ノードは電池駆動であることが想定されるので，電池交換やノードの故障により正規ノード数が減少する可能性がある．先行研究では正規ノードにのみ協調的検知の権限を付与していた．つまり，協調的検知可能な範囲は正規ノード数に依存する．従って，提案手法では正規ノードに加えて監視対象ノードにも協調的検知の権限を付与することで正規ノード数に依存せずに協調的検知可能な範囲を維持する．基本的な協調的改竄検知の方法は先行研究と同様である．

3.2 孤立化関与回数

提案手法では，不正な孤立化を抑制するために孤立化に関わる全てのノードの孤立化関与回数を数える．不正ノードとして想定される振る舞いは次の通り．

- 複数のノードから孤立化対象のノードとされる場合
- 頻繁に孤立化パケットを送信する場合

1 項目目は，不正ノードが改竄を行うと協調的検知によって複数のノードから改竄に対する孤立化パケットが発信される．従って，各ノードがノード毎に孤立化対象となった回数を累積することで，その累積回数が高いノードが不正ノードである可能性が高いと判断するからである．2 項目目は，頻繁に孤立化パケットを送信するノードは孤立化を乱用しているノードである可能性があるからである．上記の振る舞いを相互に監視して振る舞い回数から不正ノードを見極めるため，各ノードは隣接ノード毎に前述の振る舞い回数を累積する孤立化関与回数を保持する．

3.3 多数決に基づく孤立化

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．

- 孤立化パケットの対象ノード
- 孤立化パケットの配信ノード

上記に従い更新した孤立化関与回数が閾値を超えたノードを自身の経路表から削除し孤立化を実施する．また，孤立化を実施した対象の孤立化パケットの配信ノードは不正ノードではないと判断して孤立化関与回数を 0 に更新する．図 9 に提案手法における孤立化のフローを示す．図 9 はノード A がノード B を対象として配信した孤立化パケットを C が受け取った時の C が行う孤立化に関するフローチャートである．ノード C は孤立化に関与した A，B 両方の孤立化関与関数を 1 増加させる．次にノード A の孤立化関与回数が閾値を超えている場合はノード A を孤立化しノード B の孤立化関与関数をリセットする．次にノード B の孤立化関与回数が閾値を超えている場合はノード B を孤立化しノード A の孤立化関与関数をリセットする．

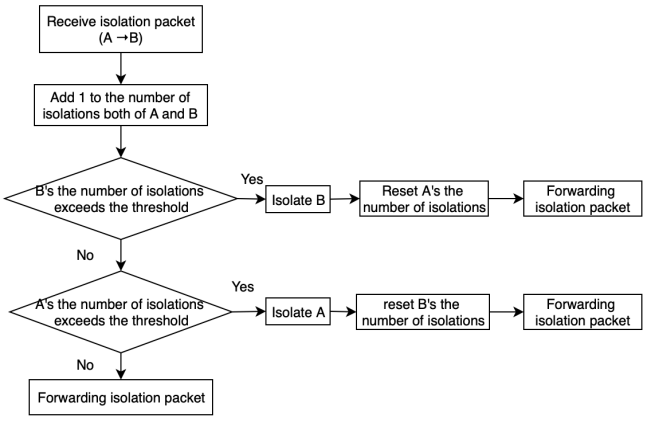

図 9 提案手法におけるフローチャート

4. シミュレーション評価

提案手法の有効性を示すために，NS3 を用い，以下についてシミュレーションにより評価を行う．

- 検知率

- 不正に孤立化されたノード数
- 未検知不正ノード数
- 不正ノード数の時間推移

以下に各項目についての評価結果を示し，考察を行う．

4.1 提案手法と既存手法に対する比較方法

評価する手法は以下の通りである．

- 提案手法：全てのノードに孤立化の権限を付与
- 先行研究：正規ノードにのみ孤立化の権限を付与

シミュレーション諸元を表 1 に示す．

表 1 シミュレーション諸元

項目	値
シミュレータ	NS3
フィールド空間 (m^2)	$1,000 \times 1,000$
トポロジ	ランダム
正規ノード数 (個)	10，20，30，40
非不正監視対象ノード数 (個)	80，70，60，50
不正ノード数 (個)	20，30, 40
孤立化関与回数閾値	10
シミュレーション時間 (秒)	2500
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

ノードを配置するフィールドは，1 辺の長さを 1000m の正方形とし，フィールド内に正規ノード及び不正ノードをランダムに配置する．

図 10 に無線センサネットワークのトポロジ例を示す．

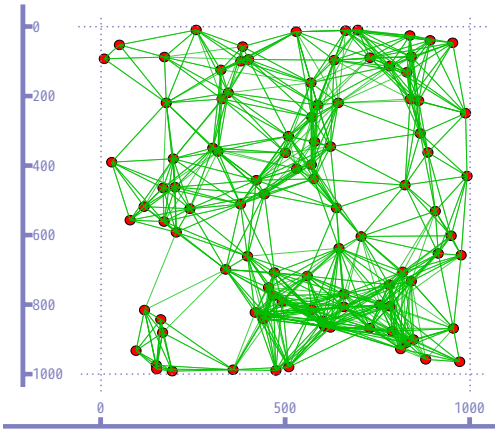

図 10 ネットワークトポロジの一例

図 11，図 12，図 13 の先行研究における正規ノード数と非不正監視対象ノード数の割合を表 2 に示す．

表 2 先行研究における正規ノード数と非不正監視対象ノード数の割合

正規ノード数	非不正監視対象ノード数	合計
10 個	80 個	90 個
20 個	70 個	90 個
30 個	60 個	90 個
40 個	50 個	90 個

提案手法は悪意のないノード数を 90 個で固定する．また，不正ノード数を 20 個から 40 個まで 10 個ずつ増加させ，計 3 通りで評価する．

送信するデータサイズは 12 バイト，無線通信は IEEE802.11b を用い，通信カバレッジは 250m とした．ルーティングプロトコルは AODV を用いる．センサノードがを保持するバッファ容量は 50 とする．

先行研究においては，正規ノードのみが協調的検知，不正ノード孤立化を行う．提案手法においては，正規ノードに加えて監視対象ノードも協調的検知，不正ノード孤立化を行う．

先行研究，かつ提案手法において，データの改ざんを行うノード に加えて， 不正な孤立化のみを行うノードを用意する．なお，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．

4.2 評価結果と考察

4.2.1 検知率

検知率を図 11 に示す．検知率は（検知数/改ざん数）× 100 で算出している．検知率において提案手法はすべての場合において先行研究よりも高い値を示した．これは，先行研究においては正規ノードにのみ協調的検知の権限が与えられているのに対して，提案手法においては全ノードに協調的検知の権限を付与しているため協調的検知可能な範囲が広がったことが要因であると考えられる．

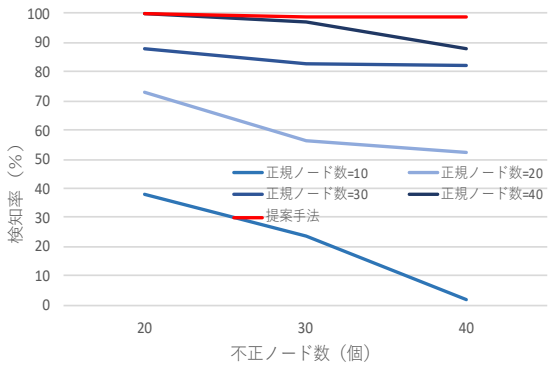

図 11 検知率

Vol.2019-DPS-180 No.17
Vol.2019-EIP-85 No.17
2019/9/20

4.2.2 未検知不正ノード数

未検知不正ノード数を図 12 に示す．未検知不正ノード数とはシミュレーション終了時（2500 秒時点）で排除されなかった不正ノード数である．先行研究において，正規ノード数 10 個の場合，改竄を行う不正ノードが残った．不正な孤立化を行う不正ノードは，先行研究では正規ノードにのみ孤立化パケット発信の権限を付与しているため，孤立化パケットの発信元が正規ノードでない場合，孤立化パケットは破棄され，また孤立化パケットの配信元ノードは不正ノードとして孤立化される．従って，先行研究における未検知の不正ノードは改ざんを行うノードとなる，これは正規ノードの協調的検知可能な範囲外に不正ノードが配置されていることが原因であると考えられる．すなわち，先行研究は正規ノード数が枯渇すると明らかに不正ノードの排除が困難となる．

提案手法において，全ての不正ノードを排除することができた．改ざんを行う不正ノードは不正ノードの周囲の複数のノードから孤立化パケットの発信が行われ不正ノードの孤立化関与回数が閾値を超えることで改竄を行うノードが排除された．また，不正な孤立化を行う不正ノードは，頻繁に孤立化パケットを配信するため孤立化関与回数が増加し閾値を超え孤立化されたと考えられる．

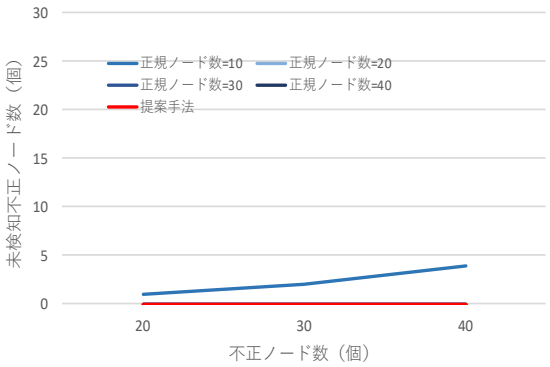

図 12 未検知不正ノード数

4.2.3 不正に孤立化されたノード数

不正に孤立化されたノード数を図 13 に示す．先行研究においては，正規ノード数に関わらず，不正に孤立化されるノードは発生しない．先行研究は正規ノードのみが孤立化パケットの送信権限を有するので，正規ノード以外からの孤立化パケットは破棄される．従って，不正に孤立化されるノードは発生し得ない．一方，提案方式において，不正に孤立化されるノードが，不正ノード 20 個および 30 個の場合に 1 個，不正ノード数 40 個の場合に 2 個が発生する．非不正ノードが孤立化される場合は，改ざんノードを排除するために孤立化パケットを配信し，また不正な孤立化パケットの対象ノードとなる場合と考えられる．すなわち，このような場合は不正ノードとする誤った判断となる．しかし，今回の評価では，非不正ノード数が 90 個に対して不正ノード数が 20-40 個であり，不正ノード数の割合が高い．実環境では，不正ノード数の割合は本評価より相当低くなると考えるのは妥当であるので，この場合は不正に孤立化されるノード数は発生しないと考えられる．

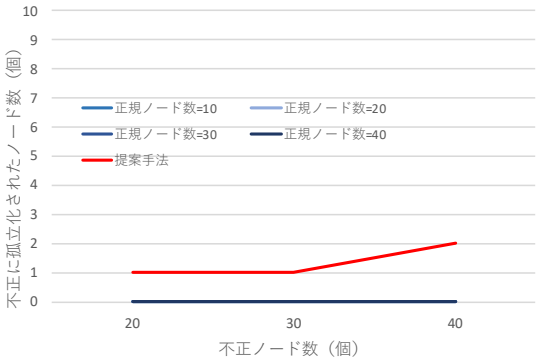

図 13 不正に孤立化されたノード数

4.2.4 不正ノード数の時間推移

不正ノードの時間推移を図 14 に示す．図 14 は先行研究において正規ノード数 30 個，監視対象ノード数 60 個．先行研究，提案手法共に，不正ノード数 40 個の不正ノードの時間推移である．先行研究においては孤立化は改ざん検知後に直ちに実施されるため不正ノードは早い段階で排除される．しかし，提案方式は，先行研究と比較して，全ての不正ノードを排除するのに明らかに大きな遅延が発生している．この遅延の原因は，孤立化関与回数の対象となる 2 つの振る舞いにおいて，不正な孤立化パケットを配信する不正ノードの排除に時間を要しているためである．改ざん検知により孤立化パケットの対象ノードとなる不正ノードの場合，改ざんを複数ノードが検知し不正ノードを対象とする複数の孤立化パケットが発生する．そのため，急速に当該ノードに対する孤立化関与回数が増えることにより迅速に改ざんを行う不正ノードが排除され，大きな遅延に至らない．一方，不正な孤立化パケットを配信する不正ノードは，不正な孤立化パケットの配信周期に依存して当該ノードに対する孤立化関与回数が増えるために，排除までに時間を要することになる．すなわち，大きな遅延の原因は不正な孤立化パケットを配信する不正ノードの排除に時間を要している点にある．しかし，改ざんを行う不正ノードは迅速に排除されることから改ざんされた不正データ数は少なく，不正な孤立化パケットは孤立化関与回数が閾値に到るまでは，孤立化が実施されるため遅延による実害はないと考える．

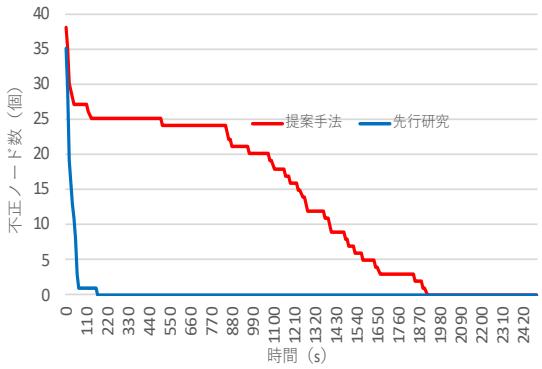

図 14 不正ノード数の時間推移

5. まとめ

先行研究において協調的検知と，孤立化の権限を正規ノードにのみ付与しているため，正規ノード数が減少した際に改竄検知率が著しく低下するという問題点があった．本稿では，先行研究の問題点を解決するため，全てのノードに協調的検知，孤立化の権限を付与し正規ノードへの依存性を無くし，多数決を用いて不正ノードによる悪意のある孤立化を阻止する手法を提案した．

シミュレーション結果から，先行研究は直ちに不正ノードを排除できるが，正規ノード数が減少すると検知率が低下し，かつ不正ノードのすべてを排除できなくなる．一方，提案方式は不正ノードを排除するまでに時間を要し，極少数であるが不正に排除されるノードが発生するものの，全ノードに改ざん検知，孤立化の権限を与え，正規ノードに依存することなく，全ての不正ノードを排除することができる．

今後の課題として以下の 2 つの場合への適応を検討する．

- 局所的に不正ノードが多数を占める場合
- 特定のノードに対しての攻撃

参考文献

[1] E.Nii, T.Kitanouma, N.Adachi, and Y.Takizawa *Cooperative detection for falsification and isolation of malicious nodes for wireless sensor networks in open environment*, Proc. of IEEE APMC 2017, pp.521-524, 2017.
[2] 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).
[3] 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).
[4] S.Bartariya, and A.Rastogi: *Security in Wireless Sensor Networks:Attacks and Solutions*, IJARCCE, Vol.5, Issue.3, pp.214-220 (2016).
[5] A.Perrig , J.Stankovic, and D.Wagner: *Security in wireless sensor networks*, Commun.ACM, vol.47, no.6, pp.53-57 (2004).
[6] S.Prasanna, and S.Rao: *An Overview of Wireless Sensor Networks*, IJSCE, Vol.2, Issue.2, pp.538-540 (2012).
[7] 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).
[8] 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).
[9] 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).
[10] H.Chan, and A.Perrig: *Security and Privacy in Sensor Networks*, IEEE Computer Society, Vol.36, Issue.10, pp.103-105 (2003).
[11] 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).
[12] X.Du and H.Chen: *SECURITY IN WIRELESS SENSOR NETWORKS*, IEEE Wireless Communications, pp.60-66 (2008).
[13] 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)
[14] 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).
[15] 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).
[16] 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).
[17] S.Ganeriwal, 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).
[18] 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).
[19] Prashant Kumar Maurya, Gaurav Sharma and Vaishali Sahu: *An Overview of AODV Routing Protocol*, International Journal of Modern Engineering Research (IJMER), Vol.2, Issue 3, pp.728-732 (2012).
[20] 間瀬, 阪田 : アドホック・メッシュネットワーク -ユビキタスネットワーク社会の実現に向けて- , pp.1-4, コロナ社 (2007).
[21] 半田 史郎, ユビキタス技術 センサネットワーク, pp.42-44, オーム社 (2006).
[22] Jaydip Sen: *A Survey on Wireless Sensor Network Security*, IJCNIS, Vol.1, No2, pp.55-78 (2009).
[23] 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).