Vol.2015-DPS-165 No.10
2015/12/10

開放環境WSNにおける協調的パケット改竄検知と不正ノード孤立化手法の提案

新居　英志[1]　安達　直世[2]　滝沢　泰久[2]

概要：無線センサネットワークでは，多様な環境に配備されてることが想定され，第三者による端末への物理的な接触を考慮に入れる必要がある．悪意のある第三者が端末を物理的に取得しストレージに直接アクセスすることで，端末内の鍵などの秘密情報の盗取や端末に改竄行為をさせるようなコードの書き換えを行うことができる．従来では改竄検知にデジタル署名などを用いてきた．しかし，鍵の秘密性が破綻した状況ではデジタル署名等の手法は有効ではない．そこで，本稿では複数の正規ノードが中継ノードの振る舞いを協調的に監視することにより，不正ノードの改竄を検知する手法を提案する．本手法は，改竄を検知した後，再度改竄をさせないように不正ノードを論理的に孤立化する．

1. はじめに

近年，無線センサネットワークの利用が急速に拡大している．無線センサネットワークは多様な環境に配備されることが予想される．そのため無線センサネットワークにおいては，第三者による端末の不正な取得などの物理的な接触を考慮に入れる必要がある．特に開放環境で使用する場合，物理的な接触を完全に遮断することは難しく，第三者は端末に接触することで様々な不正を行うことができる．例えば，悪意のある者が物理的に端末を入手した時，端末のストレージに直接アクセスすることで端末内の鍵などの秘密情報を不正に取得することができる．また，端末に対し悪意のあるコードを書き込み，再度正規ネットワークに戻すことによってその端末に不正行為をさせることができる [1][2]．ここで意味する不正行為とは，メッセージの改竄行為や，虚偽の内容を記したメッセージの送信などを指す．

従来より改竄の検知においては，公開鍵暗号方式を用いたデジタル署名が広く利用されている [3]．デジタル署名は, 送信者がメッセージと共に署名を添えて送信し，受信者が添えられた署名を検証することで改竄の検知を行う．無線センサノードは，電源確保の問題により電池駆動であることが求められるので，運用期間を延長するために計算資源に大きな制約がかかる．限られた計算資源でデジタル署名を実現することは難しく，無線センサノードにおいて改竄を検知するには計算量的に安価な手法を用いる必要がある．

[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

無線センサネットワークでは事前に共有した鍵を用いてMAC(massage authentication code) を作成し，メッセージと共に送信することで受け手側で改竄の検知を行う手法を取っている [4][5]．事前に共有した鍵を用いることにより，デジタル署名よりも少ない計算量で改竄の検知を行うことができる．このような鍵を用いた手法においては，共有した鍵が第三者に知られていないという鍵の秘密性が担保されていることが，安全な通信を行う上で必要となる．しかし，無線センサノードへの物理的な接触によって，共有した鍵を入手した不正ノードは，メッセージと MAC の両方を書き換えることにより正規ノードによる改竄の検知を逃れることができる．つまり，鍵が不正取得されるような状況において改竄を検知を可能にするには，鍵の秘密性に依存しない手法が必要となる．

このような状況で不正を検知する手法として，Watchdog Mechanism という手法が提案されている [6]．これは送信者が，自身が送信したパケットを自ら監視することにより不正を検知する仕組みである．送信者は，一次近傍ノードの振る舞いは監視できる．しかし，通信範囲外となる 2 ホップ以上の近傍ノードの振る舞いを監視することができないため，複数の不正ノードによる改竄が検知できない．

本論文では鍵の秘密性を前提とせず，複数の近傍ノードが協調することによって改竄を検知する手法を提案する．この手法は，送信者，受信者以外の正規の第三者が協調的に中継ノードを監視することによって，送信者自身が監視するだけでは見抜けなかった改竄を検知する．新たにネットワークに参加するノード，及び一時的に離脱し再参加をするノードは，悪意のあるノード，もしくは悪意のある

コードが書き込まれた正規ノードである可能性がある．そのため，上記のノードを監視対象とし監視を行う．さらに，不正を検知した後，繰り返し不正行為をさせないように不正ノードをネットワークから論理的に隔離する．

本論文の構成を以下に示す．二章で既存研究を挙げ，三章で提案手法を述べる．四章ではシミュレーション結果を示し，五章で本論文の結論を述べる．

2. 既存方式とその問題点

2.1 Massage Authentication Code

MAC(MassageAuthenticationCode) 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．送信者は，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．送信者は元のメッセージに生成した MAC 値を添えて送信する．受信者は，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．受信者側が生成した 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竄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，正規のノードによる改竄検知が可能となる．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，改竄したメッセージから MAC 値を生成することができる．受信者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竄されているが，改竄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，二つの MAC 値は一致することとなり改竄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竄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．

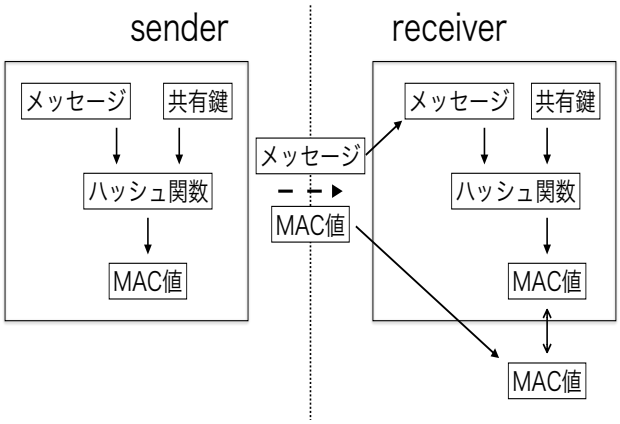

図 1 massage authentication code

2.2 Watchdog Mechanism

Watchdog Mechanism とは，無線通信の特性により周囲の振る舞いをモニタリングする手法である．図 2 において，ノード S がノード R にパケットを送信する場合を考える．S と R は直接通信できる範囲にいないので，S の近傍ノードであるノード A に中継を依頼する．無線の特性上，A が R に対し中継を行った際，送信者である S は A が中継したパケットを受け取り，A が正しく中継したかどうかを確認することができる．このようにして送信者は近傍ノードの振る舞いをモニタリングすることができる．また，鍵の秘密性に頼ら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，この手法は送信者が中継者の振る舞いを監視する手法であるため，二次以上の近傍ノードの振る舞いを監視することはできない．

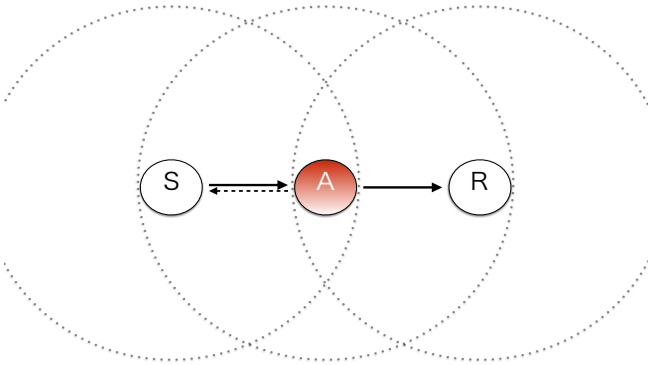

図 2 Watchdog Mechanism

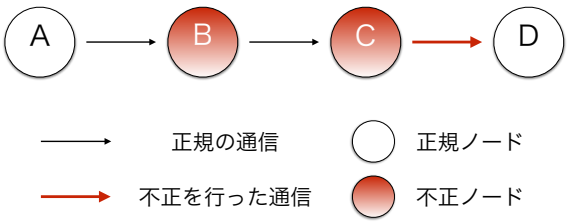

図 3 複数の不正ノードによる不正の隠蔽

図 4 傍受の失敗

図 3 のように不正ノードが連続してパケットを中継する場合，片方の不正ノード (ノード B) がもう片方の不正ノード (ノード C) の改竄を隠蔽することによって正規ノードに気付かれないように改竄を行うことが可能となる．このような場合では，Watchdog Mechanism だけでは改竄の検知は難しく，不正ノードによる改竄がネットワークの完全性を大きく損なわせることとなる．さらに，図 4 のようにノード S が中継ノード A の中継したパケットの傍受に失敗すると，振る舞いを監視することができなくなる．混雑したネットワークの中では，改竄を検知することが難しくなる．

3. 提案手法

本手法は鍵の秘密性に頼らず，かつ不正ノードが連続して経路に存在する場合でも，改竄を検知し不正ノードをネットワークから孤立化する手法を提案する．

3.1 前提条件

提案方式において，WSN 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する．
- 監視対象ノード：ネットワークへの新規参入ノード，及び再参加ノードとする．

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．再参加ノードとは，正規ノードが一時的にネットワークを離脱し，そのあとネットワークに再参加したノードと定義する．再参加ノードは，不正行為を行うように端末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，再参加ノードの二つの対象を監視対象とする．

本手法では，複数の正規ノードが協調して監視対象ノードの振る舞いを監視し，改竄を検知する．改竄を検知した後，不正ノードをネットワークから論理的に孤立化する．以下に詳細を示す．

3.2 改竄検知

図 5 において，正規のノード S は正規のノード R にパケットを送るために不正ノード A に中継を依頼する．この時，協調ノードであるノード M は中継ノードであるノード A の振る舞いを監視する．協調ノードとは，パケットの送信ノード，中継ノード以外の近傍ノードと定義する．ノード S から送信されたパケットは通信範囲内である協調ノード M は傍受 (OverHearing，オーバーヒアリング) できる．また，ノード A がパケットを中継し，ノード R へ向けて送信する．この時に，ノード M はノード A の通信範囲にも入っているので，中継パケットもオーバーヒアリングできる．ノード M は受け取った送信パケットと中継パケットの二つをハッシュ関数にかけて比較をする．二つのパケットのハッシュ値が一致していれば改竄はされていないとみなし，一致していなければ改竄が行われたとみなす．

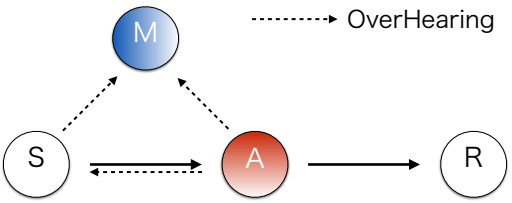

図 5 協調ノードによる改竄検知

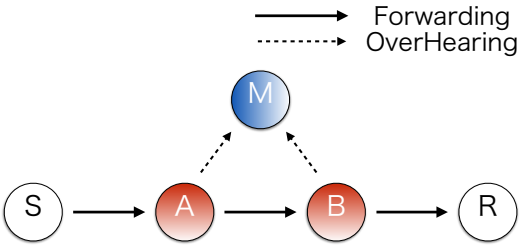

図 6 不正行為の隠蔽に対する検知

図 6 のように不正ノードが連続して経路に存在する場合を考える．ノード A は不正ノードであるが，ノード A 自身は改竄をせずに中継を行うノードであり，ノード B は改竄を行う不正ノードであるとする．図 6 においてノード B が改竄を行った場合，WatchdogMechanism によりノード B の改竄を検知できるのはノード A のみである．この時，ノード B による改竄行為をノード A は隠蔽することができる．不正行為を隠蔽することにより繰り返し改竄を行うことができ，悪意のある者がネットワークの完全性に対し大きなダメージを与えることができる．

提案手法では不正ノードが連続して経路に存在する場合においても，不正行為を検知することができる．協調ノード M はノード A が中継したパケットと，ノード B が中継したパケットをオーバヒアリングしハッシュ関数に通し比較を行う．協調ノード M における比較処理により不正ノード A が隠蔽した不正ノード B の改竄を検知できる．このように，WatchdogMechanism では検知不可である改竄も正規ノードが協調して対象ノードを監視することにより検知可能とする．また，不正ノードが改竄を隠蔽した場合でも，協調的に中継ノードの監視を行うことで改竄を検知することができる．

さらに，図 7 のようにノード S が中継パケットの傍受に失敗した場合を考える．WatchdogMechanism においては送信ノードが中継パケット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なくなり改竄を検知することが不可能となる．ここで，提案手法は複数の正規近傍ノー

ドが中継ノードの監視を行う．そのため，中継ノードを出入りするパケットをより多くのノードで監視することができるため，検知率を向上させることができる．

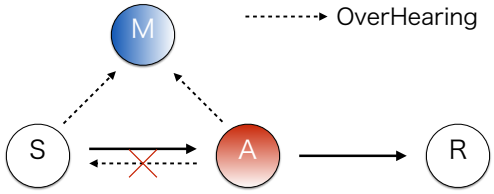

図 7 送信ノードの傍受失敗の際の協調ノードによる改竄検知

改竄を検知したノードは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．

3.3 孤立化

不正ノードによる検知したノードは，一次近傍ノードへ不正ノードの存在を知らせるために孤立化レポートを送信する．孤立化レポートを受け取ったノードは，レポートに記載されている不正ノードが近傍ノードに存在するかを確認する．不正ノードが近傍ノードにいない場合は，孤立化レポートを破棄する．近傍ノードリストに不正ノードが存在する場合のみ孤立化処理に入ることで，不正ノードの近傍ノードにのみ孤立化レポートを通達することができる．よって，孤立化のための通信量を削減することが可能となる．

孤立化処理は，現在の経路表に不正ノードが存在する場合は経路表から削除し，ブラックリストへの登録を行う．近傍ノードに不正ノードが存在するが，現在の経路表に不正ノードがいない場合はブラックリストへの登録のみを行う．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．経路作成要求を送信したノードが，ブラックリストに登録されている場合は経路作成要求を破棄する．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．

以上の処理により，通信量を削減しつつ不正ノードの論理的な孤立化を行う．

4. シミュレーション評価

本手法の有効性を評価するためにシミュレーションを行う．

4.1 シミュレーション条件と評価方法

正規ノード数は 100 ノード，格子状に配置し，不正ノードはランダムに配置する (図 10)．本稿では，協調ノードが確実に一定数存在する条件で提案手法の有効性を検証するため，正規ノードを格子状に配置する．

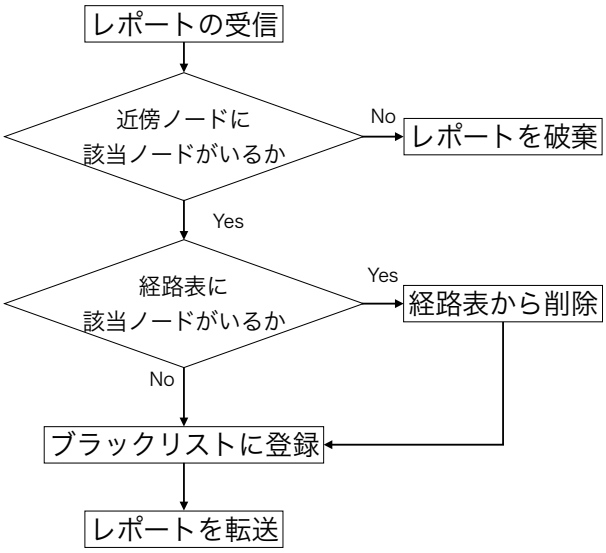

図 8 孤立化処理のフロー

左上のノードをシンクノードとし，その他の正規ノードはシンクノードを宛先としてパケットを送信する．正規ノードによるパケット送信レートは 450Kbps とし，無線通信は IEEE802.11b を用いる．ルーティングプロトコルは AODV を用いる．不正ノードはパケットの中継のみを行い，中継する際に 100%の確率で改竄を行う．

改竄検知は MAC 層で行われ，孤立化の際に送信する孤立化レポートは MAC 層でのブロードキャストが行われる．孤立化レポートのフォーマットを図 9 に示す．

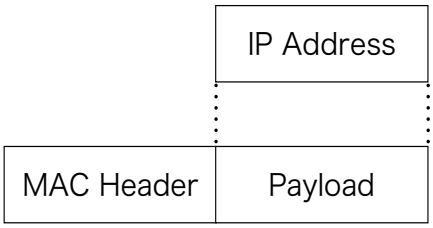

図 9 孤立化レポートのフォーマット

孤立化レポートには不正ノードの IP アドレスが格納されており，その IP アドレスを経路から削除し，ブラックリストに登録する．

評価は以下の三つの手法に対して行う．協調的検知の有効性を示すために検知率を，孤立化の有効性を示すために改竄数を比較する．改竄数とは，不正ノードが中継の際に改竄してネットワークに流入したパケット数である．ただし，一度改竄されたパケットは他の不正ノードによって再び改竄されることはないものとする．

- 提案手法：
  協調的検知を行った後，孤立化のステップに移行して不正ノードの孤立化を行う．

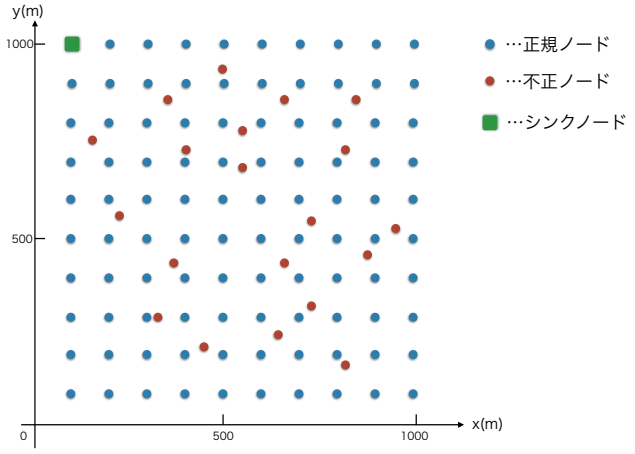

図 10 ノード配置

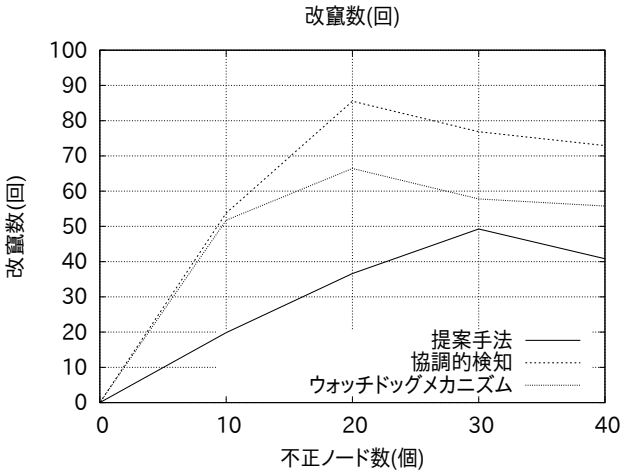

図 12 改竄数

- 協調的検知手法：
  協調的検知のみであり，孤立化は行わない．
- WatchdogMechanism：
  送信者自身の検知のみであり，協調的検知及び孤立化は行わない．

4.2 シミュレーション結果

4.2.1 検知率の比較

図 11 は検知率を表す．横軸が不正ノードの数を表し，縦軸が検知率を表す．値が高いほど改竄されたパケットを検知できているということになる．WatchdogMechanism では，検知率は 50%程度にとどまっているが，協調的検知を用いた他の二つの手法では 95%の検知率を保っている．このことより，複数の正規ノードが協調的に監視することで，WatchdogMechanism では検知できない改竄を検知することができる．

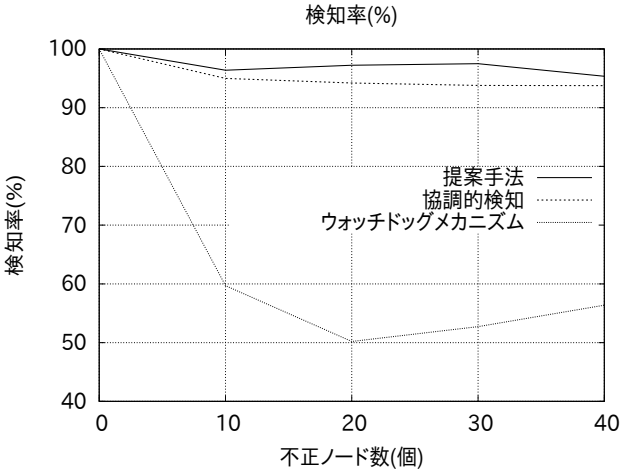

図 11 検知率

4.2.2 改竄数の比較

図 12 は各手法においての改竄数を示す．横軸が不正ノードの数であり，縦軸が改竄数を表す．値が低いほどネットワークに流入した改竄パケット数が少ないということになる．どの手法においても不正ノード数が増加するにしたがって改竄数も増加している．しかし，孤立化を行わない手法は不正ノード数が 20 ノードの時，改竄数は 80 回程度であるが，提案手法は 40 回程度であり他の手法と比べ 50%程度である．このことから，提案手法における不正ノードの孤立化により改竄を抑制できたと言える．しかし，今回のシミュレーションでは構成経路の相違が発生したことやサンプリング回数が少なかったことから，協調的検知と WatchdogMechanism の間に経路上の不正ノード数の大きな相違が発生し，そのために改竄数の大きな違いとなった．

提案方式では不正ノードの孤立化を実施し，改竄パケットの流入を大きく減少させるが，0 には至らない．これは，孤立化レポートの伝搬に時間を要し，その間に不正ノードから改竄パケットがネットワークへ流入するためである．しかし，孤立化レポートの伝搬が完了した以降は，不正ノードは完全にネットワークから分離させられるため，改竄パケットの流入は 0 となる．この問題を解決するためには，以下のような機構が必要となる．

- 改竄を検知したノードは改竄されたパケットを特定し，特定したパケットをシンクノードに通達する．
- 通達を受けたシンクノードは，改竄されているパケットをデータベースから削除する

図 13 に改竄検知から孤立化の流れを示す．不正ノードである 10.1.1.3 が経路に存在し，パケットを中継する際に改竄を行った．この時，協調ノードである 10.1.1.4 はオーバーヒアリングを行い，10.1.1.3 が改竄を行ったことを検知した．その後，不正ノードの IP アドレス 10.1.1.3 を含んだ孤立化レポートを近傍ノード 10.1.1.1，10.1.1.5 にブ

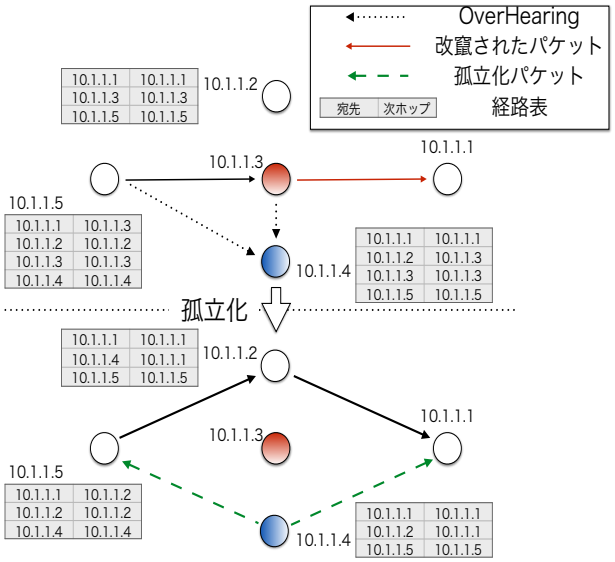

図 13 孤立化の流れ

ロードキャスト送信する．孤立化レポートを受け取った 10.1.1.1，10.1.1.5 は，まず孤立化レポートに記載されている IP アドレス 10.1.1.3 のノードが近傍ノードに存在するかを確認する．近傍ノードに存在する場合は 10.1.1.3 の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．その後，受信した孤立化レポートを転送する．レポートの転送を行うことで 10.1.1.4 と直接通信できない 10.1.1.2 にも 10.1.1.3 が不正ノードであることを知らせることができる．

5. 結論と今後の課題

本稿では，鍵の秘密性が破綻し改竄を行うノードが侵入した WSN において，複数の正規近傍ノードが協調的に監視を行うことで改竄を検知する手法を提案した．協調的に監視をすることで WatchdogMechanism よりも高い検知率を保つことができ，孤立化によって協調的検知手法よりも不正ノードによる改竄を抑制することを可能とした．

今後の課題としては以下の点が挙げられる．

- データ集約型 WSN
- 不正ノードによる虚偽のパケットの送信

データ集約型 WSN とは，ノードがデータを中継する際に，受け取ったデータと自身がセンシングしたデータを集約して中継する方式である．データを集約する場合，ある任意のノードが受け取ったパケットとそのノードが中継したパケットで内容が変わるので，協調ノードが傍受した二つのパケットのハッシュ値は異なるものとなってしまう．このような状況では，改竄の検知が難しくネットワークの完全性が損なわれてしまう．

不正ノードによる虚偽のパケットの送信が行われた場合を考える必要がある．虚偽のパケットとは以下のようなものである．

- 虚偽のセンシングデータ
- 虚偽の孤立化レポート

一つ目は，不正ノードが虚偽の内容のセンシングデータを送信することである．WSN は工場の温度管理やビル，橋梁のメンテナンスなどでの利用が想定されるが，センシングしたデータはその構造物の状況を表す重要なメトリックである．虚偽の内容のセンシングデータを送ることで，構造物のメンテンス工程に大きな支障をきたすこととなる．二つ目は，本手法で用いている孤立化レポートの送信である．不正ノードが正規ノードを悪意のあるものであると虚偽の報告することで，ネットワークから正規ノードを排除する不正行為である．正規ノードをネットワークから排除することで，有用なデータの収集を妨げることができ，ネットワークを破綻させることができる．以上より，データ集約方 WSN への適応と，不正ノードによる虚偽のパケットの送信を今後の課題とする．

今後の予定としては，トラストマネジメントシステムを導入しシミュレーションを行う．トラストマネジメントシステムとは，ノード毎にトラスト値と呼ばれる信頼の度合いを表すメトリックを追加し，そのトラスト値によって振る舞いを変えるシステムである．トラスト値を参照することにより，孤立化レポートやセンシングデータの受理の判断をすることで，不正ノードから送信された虚偽の内容が記載されたパケットを遮断することができると考えている．比較する手法以外の部分を同様にし手法の比較をするとともに，サンプリング回数を増やしシミュレーションを行っていく．

参考文献

[1] A.Perrig , J.Stankovic, and D.Wagner: *Security in wireless sensor networks*, Commun.ACM, vol.47, no.6,pp.53-57, 2004
[2] 清 雄一：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複製ノードの分散検知, 電子情報通信学会論文誌, Vol.J92-B, No.4, p.689-p.699, 2009
[3] 齋藤 孝道：マスタリング TCP/IP 情報セキュリティ編オーム社 (2013)
[4] X.Du and H.Chen: *SECURITY IN WIRELESS SENSOR NETWORKS*, IEEE Wireless Communications, p.60-p.66, 2008
[5] Jaydip Sen: *A Survey on Wireless Sensor Network Security*, IJCNIS, vol1, No2, p.55-p.78, 2009
[6] Youngho Cho, Gang Qu, Yuanming 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
[7] 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