6S-04

開放環境WSNにおける協調的パケット改ざん検知と不正ノード孤立化手法の提案とその評価

新居　英志[†]　北乃馬　貴正[†]　安達　直世[‡]　滝沢　泰久[‡]
関西大学大学院理工学研究科[†]　関西大学環境都市工学部[‡]

1　はじめに

近年，開放環境において無線センサネットワーク(WSN:Wireless Sensor Networks)の利用が急速に拡大している．開放環境 WSN は第三者による物理的な接触を完全に遮断することは難しく，悪意ある者がセンサノード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，悪意のある者は物理的にセンサノードを入手し，センサノードのストレージ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．このように不正に取得した鍵を用い認証をすり抜けることで，悪意のある者は改ざん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できる[1]． WSN 上での改ざん検知は，簡易な署名である MAC(Message Authentication Code)が利用されている[2]．しかし，MAC は鍵の秘密性が担保されている状況を前提とするため，鍵の秘密性の担保が難しい状況において MAC は機能せず，WSN はそのデータの信頼性を失う．

WSN において鍵に依存せず不正を検知する手法として，Watchdog という手法が提案されている[3]．Watchdog は，ノード自身が隣接ノードの振る舞いをモニタリングする仕組みであり，自身が送信したパケットと隣接ノードが転送したパケットを比較することにより，改ざん検知が可能となる．しかし，監視を行うノードは通信範囲外となる 2 ホップ以上先の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，経路に連続するように不正ノードを配置した場合，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[5]は，送信ノードから 2 ホップ以上先のノードで改ざんが行われ，Watchdog を用いた検出方法では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ができず，WSN におけるデータの信頼性が失われてしまう．
そこで，本稿では，鍵の盗取などにより鍵の秘密性が失われた WSN において署名に依存せずにデータの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し，検知した不正ノードを論理的に WSN から孤立化する手法を提案する．

2　提案手法

本稿では，鍵の秘密性が失われた WSN においてデータの信頼性を確保するために，WSN 構成時のノードを正規ノード，新規参加ノード及び再参加ノードを監視対象ノードとし，正規ノードによる近傍ノード協調型の改ざん検知手法を提案する．また，不正ノードをネットワークから孤立化し，改ざん行為自体を排除する．

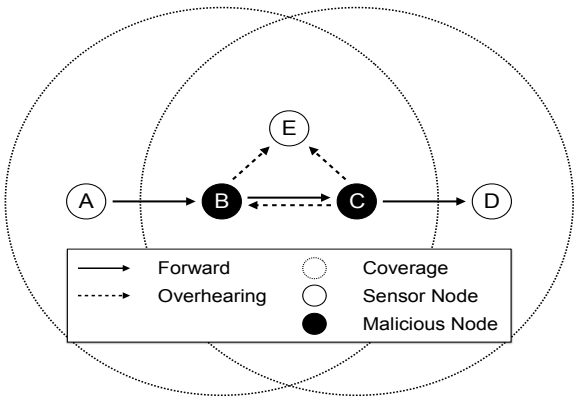

図 1 改ざんの隠蔽に対する検知

2.1 協調的改ざん検知

図 1 において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 B は不正ノードであるが自身は改ざんを行わずパケットの中継を行う．ノード C は自身で改ざんを行うノードとする．図 1 においてノード C が改ざんを行った場合，Watchdog によりノード C の改ざんを検知できるのはノード B のみである．この時，ノード B はノード C による改ざん行為を正規ノードに対し隠蔽することができる．既存手法では上記のような状況で改ざん行為は検知できないが，提案手法では改ざん行為を検知することができる．提案手法において，正規ノードであるノード E は，ノード B が中継したパケットとノード C が中継したパケットをオーバーヒアリングしハッシュ値の比較を行う．ノード E における比較処理により不正ノード B が隠蔽した不正ノード C

の改ざんを検知できる．

2.2　不正ノードの孤立化

不正ノードを検知したノードは，隣接ノードへ孤立化の対象である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正規ノードは，孤立化レポートに記載されている不正ノードの 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．その後，孤立化レポートを周囲に送信する．

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再度経路に参加することを防ぐ．

以上の処理により，不正ノードを論理的に孤立化して，改ざん行為自体をネットワークから排除する．

3　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 を用い以下の点についてシミュレーションにより提案手法と既存手法の比較評価を行う．評価する手法は以下の通りである．

- 提案手法：協調的検知，及び孤立化
- 協調的検知：協調的検知のみ，孤立化無し
- Watchdog：協調的検知，及び孤立化無し

3.1　検知率

図 2 に検知率についての評価結果を示す．横軸は不正ノード数を表し，縦軸は検知率を表す．検知率は，全改ざんパケットにおける検知できたパケットの割合として算出している．図 2 より，Watchdog では不正ノードが 40 個の時，検知率は 80%未満となるのに対し，協調的検知を行っている他の２つの手法は不正ノードが 40 個の場合でも検知率はおおよそ 100%を維持している．協調的検知は，Watchdog では検出することのできない協調的改ざんを検知することができ，不正ノードが増加しても高い検知率を保つことができる．

3.2　改ざん率

図 3 に改ざん率についての評価結果を示す．横軸は不正ノード数を表し，縦軸は改ざん率を表す．改ざん率は，シンクノードに到達したパケットの中で改ざんされたパケットの割合を表す．図 3 より，孤立化を行わない協調的検知と Watchdog の２つの手法は，改ざん率が高く，不正ノードに繰り返し改ざん行為を許していることがわかる．一方，提案手法では不正ノードが 40 個の場合でも改ざん率を 1.6%程度であり，また時間経過とともに不正ノードの孤立化が進み，最終的には改ざん率は 0 に至る．

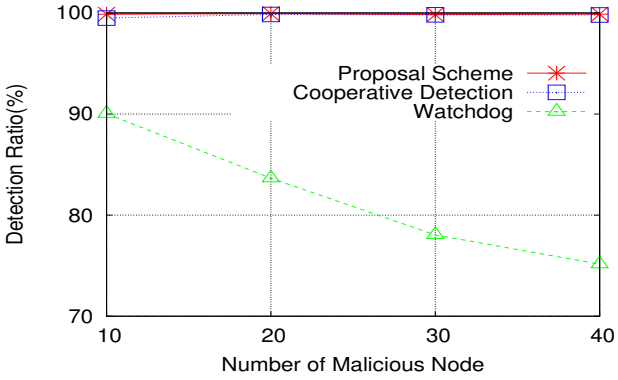

図 2 検知率

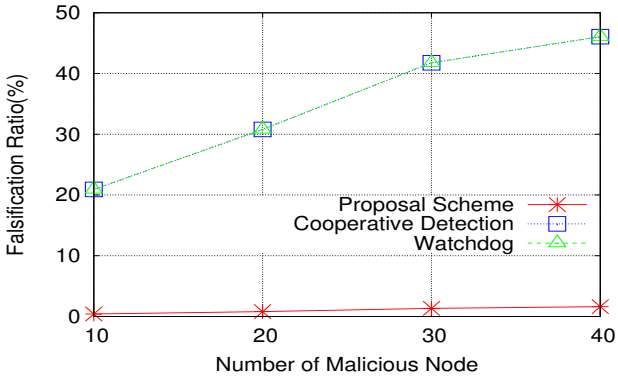

図 3 改ざん率

4　まとめ

本稿では，鍵の秘密性を担保できない WSN においてデータの信頼性を確保する協調的改ざん検知と不正ノード孤立化手法の提案を行った．提案手法と既存手法の比較評価により，提案手法は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．

参考文献

[1] H.Chan, and A.Perrig: Security and Privacy in Sen- sor Networks, IEEE Computer Society, Vol.36, Issue.10, pp.103-105(2003). [2]X.Du and H.Chen: SECURITY IN WIRELESS SEN- SOR NETWORKS, IEEE Wireless Communications, pp.60-66(2008). [3]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).