6X-03

開放環境WSNにおける協調的パケット改ざん検知とトラストを用いた不正ノード孤立化手法の提案

木村　圭希 † 新居　英志‡　滝沢　泰久‡
環境都市工学部都市システム工学科 †

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,悪意のあるもの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.従って,悪意のある者は物理的な接触により不正に入手した鍵を用いて改ざん行為を行う不正ノードを用いて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.

WSN 上での改ざん検知は,簡易な署名である MAC(Message Authentication Code)[1]が利用されている.しかし,MAC は鍵の秘密性が担保されていることが前提であるため,秘密鍵をもつ不正ノードの検知には機能しない.WSN において鍵に依存せずに不正を検知する手法として,Watch Dog という手法が提案されている.Watch Dog[2]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,図1に示すように不正ノード A,B が経路上連続し, B が改ざんを行い, A ほその改ざんを通知しない場合,改ざんを検知することができない[3].

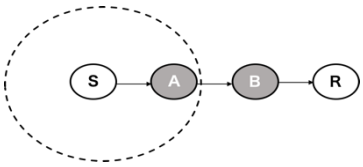

図1 連続する不正ノードの検知

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,近傍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[4]は,不正ノードが孤立化を悪用することを考慮していない.本稿では,信頼性を示すトラスト値に基いて監視対象ノードである新規ノード,再入ノードに協調的検知と孤立化のの権限を付与し,かつ不正ノードの孤立化の悪用を排除する方式を提案する.

2　提案手法

2.1 トラストによる準正規ノード

トラストの値はすべてのノードが自身の隣接ノードごとにその信頼性を示す値として保有する値であり,正規ノードに協調して不正ノードを孤立化することで上昇する.ネットワークを構成した時点のノードを正規ノード,ネットワークへの途中参加ノード,再参加ノードを監視対象ノードとし,監視対象ノードはトラストが閾値を満たすと準正規ノードに昇格する.各ノードが持つ権限は表1に示す. 孤立化反論おパケットを送信する権限は,正規ノードにのみ与えられているものであり,監視対象ノード,不正ノードは使用できない.

	正規ノード	準正規ノード	監視対象ノード
転送	○	○	○
孤立化パケット	○	○	×
孤立化反論パケット	○	×	×

表 1　各ノードがもつ権限

新規ノード,再入ノードが監視対象ノードから準正規ノードへ昇格すれば,協調的検知および孤立化レポートの権限をもつノードが在荷し,ネットワーク全体として不正ノードの検知と孤立化を向上させることができる.

2.2 協調的検知と孤立化パケット

2.1節のトラスト値により不正ノードが準正規ノードに昇格する可能性があり, この場合, 準正規ノードとなった不正ノードが孤立化パケットを悪用することが想定される.この解決策として正規ノードによる孤立化反論パケットを提案する.孤立化反論パケット作成の権限は正規ノードにのみ与えられている.孤立化反論パケットは図1のような場合に作成される. 準正規ノード A が準正規ノードまたは正規ノード B の孤立化パケットを配信し,不正ノード以外のノード D（ここでは正規ノードとしている）が受け取った場合,ノード D はノード C からの孤立化反論パケットを一定時間待つ.ノード C はノード B の近傍ノードでかつ正規ノードである.ノード C はノード B のトラストが閾値を超えていれば悪意のないノードと判断するのでノード A に対する孤立化反論パケットを送信する.ノード B のトラストが閾値を満たさない場合は B を孤立化させる.ノード D は,ノード C からの孤立化反論パケットを受け取るとノード A を孤立化させる.

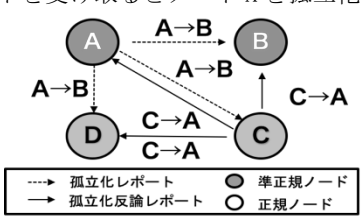

図 2　孤立化反論パケット

提案手法での孤立化のフローは図３のようになっている．図３は図２の孤立化反論パケットにおける例である．

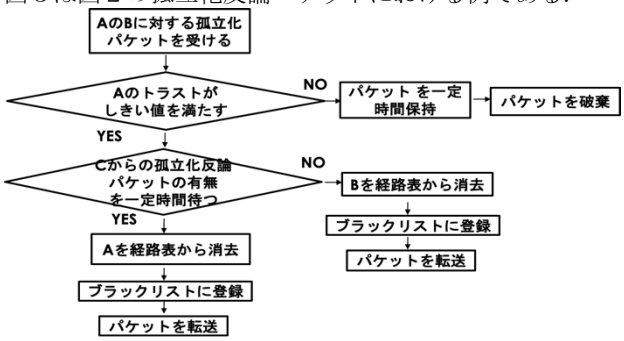

図　３ノードD孤立化パケット受信後のフロー

孤立化パケットを受け取った全てのノードは，送信元のトラストが閾値を満たしているかを確認する．次に，一定時間待機し一定時間内に孤立化反論パケットがなければ送信元を信頼し，孤立化反論パケットがあれば送信元を不正ノードと判断する．

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．

ノード配置	ランダム
ノード数	130
正規ノード数	100
不正ノード数	20
トラスト閾値	100
トラスト上げ幅	30
不正ノードによる 孤立化パケット	10 秒に１回

表２　シミュレーション諸元

- 提案手法：協調的検知，及び孤立化，及びトラストあり
- 先行研究：協調的検知，及び孤立化，及びトラストなし
- Watchdog：協調的検知，及び孤立化無し，及びトラストなし

３．１　改ざん数

図３に改ざん率についての評価結果を示す．横軸は時間を示し，縦軸は改ざん数を表す．

改ざん数については図３のように先行研究，提案手法，共に既存手法より有用であることを示した．しかし，先行研究と提案手法の大きな違いは見られなかった．提案方式は，トラスト値により準正規ノードが増加して，不正ノードの検知と孤立化が上昇して改ざん数が減少すると想定したが，準正規ノードへの昇格効果が得られなかった．

３．２　検知率

提案手法と先行研究の違いは表３検知率で確認できた．検知率は検知数/改ざん数で求められる．ここでの検知数は，重複した改ざんの検知を含まない．表３によると提案手法の検知率は先行研究に比べて高くなった．不正ノードが 10 秒に１回孤立化レポートを配信することから，先行研究においては，シミュレーション時間が 1020 秒で正規オードも含めて 102 個のノードが孤立化させられネットワーク自体が構成できない状態となったため非常に低い検知率となった．提案手法においては，検知率が 66%と他の比較して最も高いが，完全に改ざんを検知して不正ノードを排除できていない．これは不正ノードの孤立化パケットに対する孤立化反論パケットが有効に機能しているが，準正規ノードの増加による効果が得られていないためと考えられる．．

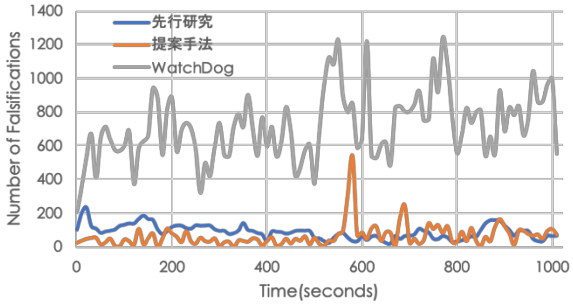

図　４　改ざん数

	改ざん数	検知数	検知率
提案手法	4115	2727	66.25(%)
先行研究	7765	238	3.1(%)
Watch Dog	73040	36920	50.5(%)

表３　検知率の比較

４　まとめ

本項では、開放環境 WSN における協調的改ざん検知と不正ノード孤立化手法の提案にノードの信頼度を示す指標トラストを設けることで安全にネットワークを拡張する提案を行なった．トラストを設けることで改ざん数を減少させ，検知数を増加させることができたが，不正ノードや改ざんを完全に排除できていない．今後は，この問題を解決することを検討する．

参考文献

[1] Mihir Bellare, Ran Canetti and Hugo Krawczyk: Message Authentication using Hash Functions, Vol2, No.1, pp1～4, 1996

[2] C.Gayathri and R.Vadivel: Survey of Watchdog Mechanism Used for Malicious Node Detection, ISSN, Vol8, No9, pp.454, 2017

[3] 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

[4] 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.

「Cooperative Detection for Falsification and Isolation of Malicious Node Based ON Trust for Wireless Sensor Networks in Open Environment」

†「Yoshiki Kimura・Kansai University」
‡「Nii Eiji・Kansai University」
‡「Yasuhisa Takizawai・Kansai University」