4X-05

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不正ノード孤立化手法*

高橋 和也† 新居 英志‡ 滝沢 泰久§
関西大学 摂南大学 関西大学

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閉鎖環境と，道路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．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 [3]．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．

この問題を解決するために，鍵に依存しない方法として協調的改ざん検知と不正ノード孤立化が提案されている [1]．当該方式は改ざん検知と不正ノード孤立化から構成される．改ざん検知は図 1 に示すように，正規ノード E および F の近傍ノード送信データの傍受により傍受データの比較から改竄を検知する．不正ノード孤立化は改竄を行なった不正ノードをネットワークから遮断し，近傍ノードへ不正ノード孤立化を伝搬させる．以上により改竄を行う不正ノードを孤立化させる．

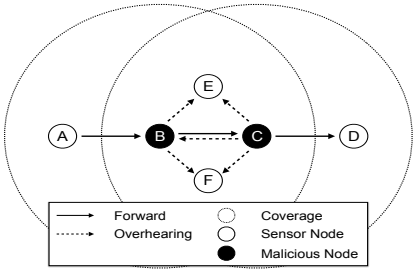

図 1: 正規ノードの近傍ノード送信傍受による改竄検知

しかし，先行研究では不正ノードが残存する問題がある．この問題の原因として，次のことが挙げられる．

- 正規ノード間で伝搬不正ノード孤立化が破棄
  不正ノード孤立化の伝搬を近傍ノードから受信した際にこれを正規な不正ノード孤立化として受け入れるかを，送信ノードの振る舞いから自己組織化マップ (SOM) を用いて正規ノードと不正ノードにクラスタリングして判断する．しかし，正規ノードにおいて不正ノードが近傍にある場合と遠隔にある場合では振る舞いが異なるため，SOM において正規ノードが 2 つのグループに分離し，2 グループ間で互いに伝搬不正ノード孤立化を破棄する．

この問題を解決するため，個々の正規ノードが隣接ノードをクラスタリングする分散型 SOM による不正ノード孤立化手法を提案する．

2 関連研究

畳み込みニューラルネットワークに基づく検出は，ネットワークフローパケット内のデータと統計情報を収集することで，悪意のあるペイロードを検出するという方式である [2]．畳み込みニューラルネットワークに基づく方式は，既知の特徴またはパターンによって侵入を識別し，トラフィックの特徴を知識内の特徴と照合することで検出できる．

しかし，これらの方式では事前に十分なトラフィックデータが必要であり，また新たな不正トラフィックには対応できない．さらに不正ノードを排除しないため，不正トラフィックは発生し続けて通信帯域を消費する．

3 提案方式

提案方式は，先行研究における不正ノード残存を解決するため，個々のノードによる隣接ノードクラスタリングする分散型 SOM クラスタリングを行う．

3.1 分散型 SOM によるクラスタリング

先行研究では，クラスタリングした際に正規ノードのグループが 2 つに分かれてしまう問題があった．この問題をそれぞれのノードで分散的に SOM を実施することによって解決する．

分散型 SOM は，各ノードにおいて自身の振る舞いを基準に（勝者ベクトルとして) 隣接ノードをクラスタリングする．従って．個々のノードが隣接ノードの範囲で，すなわち，不正ノードに隣接するノードはその範囲で，同様に不正ノードに隣接しないノードもその範囲で，自身と同質であるか否かを判断するため，個々ノードにおいては同質 (正規ノード) と異質 (不正ノード) にクラスタリングすることが可能である．また，自身の振る舞いが基準であるため，関連研究で必要とされる事前に十分なトラフィックデータによるトレーニングは不要である．

3.2 孤立化パケット送信によるクラスタリング

個々のノードにおいてクラスタリングするため，隣接ノードの振る舞いとして以下の 2 点の情報を孤立化パケッ

*Isolation of Malicious Nodes using Self-Organizing Map for Wireless Sensor Networks in Open Environments
†Kazuya Takahashi Kansai University
‡Eiji Nii Setunan University
§Yasuhisa Takizawa Kansai University

トから取得する．

- 孤立化パケットの送信回数
- 孤立化対象ノード重複回数

1つ目の要素（孤立化パケット送信回数）における正規ノードと不正ノードの振る舞いは，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：改ざんの有無に関わらず孤立化パケットを周期的またはランダムに送信する．

2つ目の要素 (孤立化対象ノード重複回数) における正規ノードと不正ノードの振る舞いは，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：ランダムなノードを対象とした孤立化パケットを送信する．

提案方式では，上記に示した個々のノードで取得した隣接ノードの振る舞いデータを成分とするベクトルによりSOMを用いてクラスタリングする．SOMのクラスタリングにおいては，勝者ベクトルを常に自身のベクトルとする．

4　評価

提案方式の有効性を示すために，NS3を用いシミュレーションを行う．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
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)	90
改ざんノード数 (個)	5
不正孤立化ノード数 (個)	5
シミュレーション時間 (秒)	1000
パケット送信インターバル (秒)	30
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
試行回数	10

上記を踏まえた上で，先行研究，提案方式を残存不正ノード数と誤孤立化正規ノード数において比較評価する．

4.1　残存不正ノード数

図2に残存不正ノード数についての評価結果を示す．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．提案方式では，先行研究と比較して残存不正ノード数を抑えることができた．要因は個々のノードにおいてSOMを実施することにより，不正ノードに近い正規ノードと遠い正規ノードの振る舞いの違いを吸収できたことである．しかし，残存不正ノード数は0に至っていない．

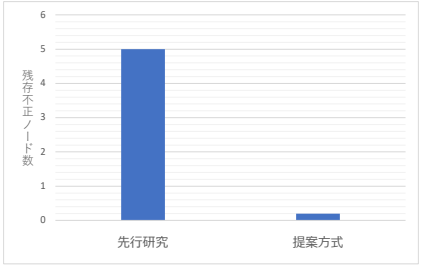

図 2: 残存不正ノード数

4.2　誤孤立化正規ノード数

図3に誤孤立化正規ノード数の結果を示す．提案方式では，先行研究と比較して，誤孤立化正規ノード数が増える．この要因は，孤立化パケット送信における振る舞いデータとして設定した，孤立化対象ノード重複回数にあると考えられる．不正孤立化ノードが不正ノードを対象に孤立化パケットを送信した場合，不正孤立化ノードとその不正ノードを孤立化の対象とした正規ノードの振る舞いが似てしまうからである．よって，正規ノードと不正孤立化ノードが同じグループにクラスタリングされてしまい，正規ノードが誤って孤立化されてしまっている．この対策として，SOMへの入力値の変更や追加が必要である．

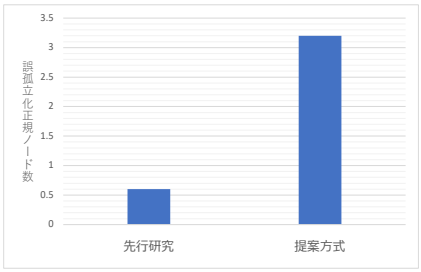

図 3: 誤孤立化正規ノード数

5　まとめ

本研究では，SOMによるクラスタリングを分散的に実施することによって，不正ノードをネットワーク上に残存する問題を解決する方式を提案した．個々のノードで実施し分散化することによって，残存不正ノード数を抑えることができた．しかし，残存不正ノード数は0に至らず，また誤孤立化正規ノード数が増加する．今後はこの問題を解決することを検討する．

参考文献

[1] 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).

[2] B. Jia, Y. Guo, H. Li and C. Du, ”A Method of Malicious Data Flow Detection Based on Convolutional Neural Network,” 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 2021, pp. 409-412, doi: 10.1109/DSC53577.2021.00064.

[3] S.Prasanna, and S.Rao: *An Overview of Wireless Sensor Networks*, IJSCE, Vol.2, Issue.2, pp.538-540(2012).