講演番号：26

多地点ゲートウェイ間連携に基づく侵入検知のための分散決定木

Distributed Decision Trees for Intrusion Detection Based on Multipoint Gateway Cooperation

渡邉 直人 † Naoto WATANABE
山崎 託 † Taku YAMAZAKI
三好 匠 † Takumi MIYOSHI
中原 正隆 †† Masataka NAKAHARA
奥井 宣広 †† Norihiro OKUI
窪田 歩 †† Ayumu KUBOTA

† 芝浦工業大学大学院理工学研究科
Graduate School of Engineering and Science, Shibaura Institute of Technology
†† 株式会社 KDDI 総合研究所
KDDI Research, Inc.

1. まえがき

IoT（Internet of things）デバイスを狙う攻撃は増加傾向にあり，様々な未知の攻撃も増加すると予想される．これらの攻撃は，インターネット上のランダムなホストに対して行われるため，ある地点で収集した攻撃情報を他の地点で利用することで，同様の攻撃が再び行われた際に検知が可能になると考えられる．

2. 多地点ゲートウェイ間連携に基づく侵入検知システム

ゲートウェイ間で連携し検知した攻撃を多地点で相互に反映する手法として，連合学習 [1] を用いた侵入検知システムが提案されている [2]．このシステムを実環境で運用する場合，計算資源が限られているゲートウェイがシステムに参加する場合が考えられる．そのため，学習コストが小さい機械学習アルゴリズムを適用することができれば，計算資源の削減や高頻度なモデルの更新が可能になると考えられる．

3. 提案手法

上述した課題に対し，学習コストが小さく，予め特徴量が抽出されたデータに高い予測性能を実現できる，決定木の利用が考えられる [3]．本稿では，決定木をそれぞれのゲートウェイ上で作成し，他のゲートウェイと共有しながら侵入検知を行う手法を提案する．

本手法の概要を図 1 に示す．まず，各ゲートウェイは，定常的に収集しているトラヒックから得られる特徴量を基に決定木を作成し，中央サーバに送信する．次に，中央サーバは，自身が保持している決定木と受信した決定木の中から一定の本数の木を最新のものから順に選択し，各ゲートウェイに送信する．各ゲートウェイは，サーバから受信した決定木を用いて，自身を通過するトラヒックに対して侵入検知を行う．なお，侵入検知を行う際，各ゲートウェイは，受信した決定木の中で，自身が作成した決定木に他のゲートウェイが作成した木より大きい重みを与え，多数決を行い最終的な予測結果を得る．これを繰り返すことで，多地点で収集したトラヒックを基に作成した決定木による侵入検知を行う．

4. 性能評価

Azure の 4 地域に設置したハニーポットを用いて収集した攻撃トラヒックと，4 研究室に設置して収集した IoT デバイスの正常通信トラヒックを用いて提案手法の評価を行った．上述した 2 種類のトラヒックは日本時間で 2022 年 1 月 1 日から同年 1 月 7 日まで収集したものであり，これらを組み合わせ 4 つのデータセットを作成した．本実験では，各データセットを 4 台のゲートウェイに割り当て，ニューラルネットワークを用いた連合学習（FL-NN）と提案手法の検知精度と学習時間を比較した．ここで，提案手法では，中央サーバは最新の 4 本の決定木を各ゲートウェイに送信しており，各ゲートウェイは自身が作成した木に他のゲートウェイが作成した木の 3 倍の重みを与えた．

1 時間間隔でモデルを更新しながら侵入検知を行った場合のある 1 台のゲートウェイにおける F 値の推移を図 2 に，学習時間を表 1 に示す．結果より，提案手法では，決定木を用いることで，短い学習時間で FL-NN と同程度の精度を実現できていることが分かる．

5. むすび

本稿では，多地点に分布しているゲートウェイ上で作成した決定木を共有しながら侵入検知を行う手法を提案した．今後は，提案手法において，検知に使用する木の本数や自身が作成した木の重みを自律的に決定するアルゴリズムを検討する予定である．

謝辞 本研究成果は，国立研究開発法人情報通信研究機構（NICT）の委託研究（JPJ012368C05201）により得られたものである．

文献

[1] T. Li, A.K. Sahu, A. Talwalkar, and V. Smith, “Federated learning: challenges, methods, and future directions,” IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50–60, May 2020.

[2] 渡邉直人, 山崎 託, 三好 匠, 中原正隆, 奥井宣広, 窪田 歩, “多地点ゲートウェイ間連携に基づくトラヒック異常の検知,” 信学ソ大, B–6–53, Sept. 2023.

[3] L. Grinsztajn, E. Oyallon, and G. Varoquaux, “Why do tree-based models still outperform deep learning on tabular data?,” arXiv preprint, arXiv:2207.08815, July 2022.

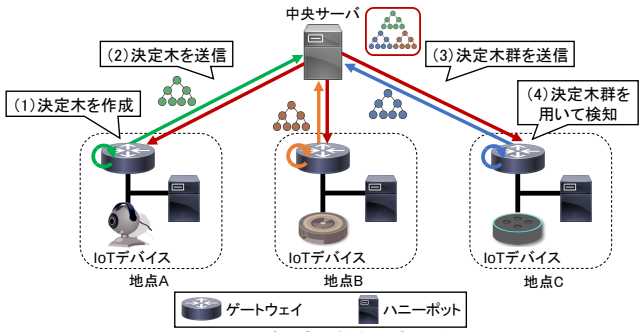

図 1　提案手法の概要

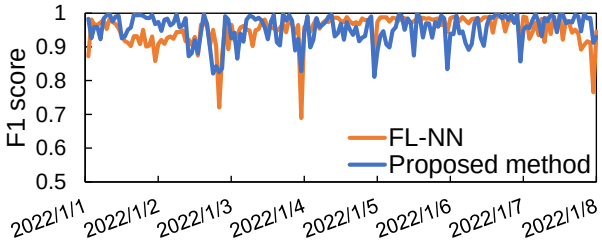

図 2　F 値の推移

表 1　学習時間 [秒]

	FL-NN	提案手法
最小	2.1805	0.0019
最大	5.5564	0.0064
平均	4.1930	0.0039
分散	0.1677	0.0001