

機械学習に基づく NIDS 向け分散処理フレームワークの 実性能評価

梶浦真帆 *

中村純哉 *

概要

ネットワーク侵入検知システム（NIDS）は通信トラフィックを監視することで、侵入攻撃を検知する。特に、機械学習に基づく NIDS は未知の攻撃に対し高い検知率を誇ることから注目されている。これまでにスケーラブルな分散ストリーム処理システムを活用した機械学習に基づく NIDS 向け分散処理フレームワーク [2] が提案されているが、機械学習による分類を含めた包括的な評価はされていない。また、同様のフレームワークは他にもいくつか提案されているが、処理速度に着目しているものは少ない。本研究では、代表的な 5 種類の機械学習アルゴリズム（決定木、ランダムフォレスト、ナイーブベイズ、SVM, kNN）を用いて作成した分類器を [2] のフレームワーク上に実装し、スループットと処理遅延を評価する。これによって、各分類器の処理性能の違いやフレームワークにおける処理性能のボトルネックとなる箇所を明らかにする。

実験結果から、処理速度と分類精度は分類器によって大きく異なることが分かった。適切な機械学習アルゴリズムを使用することで、高い分類精度を維持しつつ NIDS の負荷を軽減することができる。また、通信トラフィックからセッションを構築する Zeek、機械学習アルゴリズムを用いて分類処理を行う Logstash、分類結果を保存する Elasticsearch はフレームワークを構成するサブシステムの中でボトルネックとなりやすい傾向があることが分かった。

本発表の詳細は、IEEE NETSAP 2024 に採択された論文のプリプリント [1] を参照されたい。

参考文献

- [1] M. Kajiura and J. Nakamura. Practical Performance of a Distributed Processing framework for Machine-Learning-based NIDS. *arXiv preprint arXiv:2405.13066*, 2024. <https://arxiv.org/abs/2405.13066>.
- [2] 多田, 中村, 大村, 小林. 機械学習ベース NIDS 構築のための分散処理フレームワーク. 情報処理学会論文誌, 60(9):1448–1465, 2019.

*1 豊橋技術科学大学, 〒441-8580 愛知県豊橋市天伯町雲雀ヶ丘 1-1