Anomaly Detection in Network Traffic Using Tensor Decomposition and IP-Based Multi-Aggregation

Jospin Price Yonel Mitsouma[1*], Pouya Ataei[2], Marcellin Atemkeng[3,4], Emmanuel Fouotsa[1]

[1*], Center For Cybersecurity and Mathematical Cryptology, , Bamenda, , , Cameroon.
[2], Scholarspark.ai, 68A Hendon Avenue Mount Albert, Auckland, , , New Zealand.
[3]Department of Mathematics, Rhodes University, PO Box 94, Grahamstown, 6140, , South Africa.
[4], National Institute for Theoretical and Computational Sciences, , Stellenbosch, 7600, , South Africa.

*Corresponding author(s). E-mail(s): jospinprice@gmail.com;
Contributing authors: pouya.ataei.7@gmail.com; m.atemkeng@ru.ac.za; emmanuelfouotsa@gmail.com;

Abstract

The proliferation of connected devices in today's interconnected world has created the need for sophisticated anomaly detection systems capable of rapidly identifying abnormal behaviours within massive and heterogeneous data streams. However, traditional anomaly detection systems generally process data in a two-dimensional format, which limits their ability to capture the inherently multidimensional structure of communication data. Tensors provide a principled framework for representing multidimensional data. Nevertheless, tensor-based anomaly detection methods remain predominantly experimental and are subject to inherent limitations that constrain their practical applicability. In this work, we propose a framework that integrates CP decomposition, distinguished by its essential uniqueness (up to permutation and scaling of rank-one components) with IP based multi-aggregation and deep learning, incorporating an automatic

rank selection mechanism to optimize the detection of anomalies in network traffic. The method was evaluated using the CIC-IoT 2024 dataset, achieving an accuracy of 99.96% and a recall of 99.6%.

Keywords: Tensor decomposition, Multi-aggregation, Deep Learning, Anomaly detection, Network security

Acknowledgements

Thanks the National Research Foundation of South Africa for support through project number CSRP23040990793.

Declarations

Funding

This research was supported by the National Research Foundation of South Africa through project number CSRP23040990793.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data availability

The data used in our study are publicly available and can be accessed at http://cicresearch.ca/IOTDataset/CIC%20IoT-IDAD%20Dataset%202024/. This dataset, known as the CIC IoT-IDAD 2024 Dataset, provides a comprehensive collection of IoT network traffic, including both normal and malicious patterns, making it suitable for anomaly detection and cybersecurity research.

Author contributions

Jospin Price Yonel Mitsouma: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Software, Visualisation, Writing – original draft, Writing – review & editing.

Pouya Ataei: Conceptualization, Methodology, Formal analysis, Visualisation, Writing–review & editing, Supervision, Coding, Creating the Actual Pipeline, Mathematics, Validation.

Marcellin Atemkeng: Conceptualization, Methodology, Visualisation, Formal analysis, Writing – review & editing, Supervision, Validation.

Emmanuel Fouotsa: Resources, Writing – review & editing, Validation, Funding acquisition, Supervision.

Ethics approval

Not applicable.

Consent to participate

Not applicable.

Consent for publication

Not applicable.