Back

SECURITY AND PRIVACY / Volume 7, Issue 1 / e337

SURVEY PAPER

Unleashing the power of SDN and GNN for network anomaly detection: State-of-the-art, challenges, and future directions

Archan Dhadhania, Jitendra Bhatia, Rachana Mehta, Sudeep Tanwar, Ravi Sharma, Amit Verma

First published: 30 July 2023
https://doi.org/10.1002/spy2.337

Abstract

Modern computer networks' increasing complexity and scale need serious attention towards network anomaly detection. Software-defined networking (SDN) and graph neural networks (GNN) have emerged as promising approaches for anomaly detection due to their ability to capture dynamic network behavior and learn complex patterns from large-scale network data. The amalgamation of SDN and GNN for network anomaly detection presents promising opportunities for improving the accuracy and efficiency of network anomaly detection. This paper focuses on various trends, issues, and challenges by integrating GNN on the top of SDN for network anomaly detection. The article highlights the advantages of using SDN for providing fine-grained control and programmability in network monitoring. At the same time, GNN can model network behavior as a graph and learn representations from graph-structured data. The authors also discuss the limitations of traditional anomaly detection methods in SDN, such as rule-based approaches, and the potential of GNN to overcome these limitations by leveraging their ability to capture non-linear and dynamic patterns in network data. This paper also presents a case study of DoS attack detection using SDN. The result shows that SDN based approach helps to detect attacks with an accuracy of 97% with future research directions.

Open Research

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

REFERENCES

1 Radford BJ, Apolonio LM, Trias AJ, Simpson JA. Network traffic anomaly detection using recurrent neural networks. arXiv preprint arXiv:1803.10769. 2018.

Google Scholar

2 Saeed R, Qureshi S, Farooq MU, Zeeshan M. Sdn/nfv enabled security for an enterprise network using commodity hardware. Paper presented at: 2022 International Conference on Computing, Electronics & Communications Engineering (iCCECE), IEEE. 2022:25–30.