


[Submitted on 14 Jul 2022 (v1), last revised 23 Jul 2022 (this version, v4)]

Anomal-E: A Self-Supervised Network Intrusion Detection System based on Graph Neural Networks

Evan Caville, Wai Weng Lo, Siamak Layeghy, Marius Portmann

This paper investigates Graph Neural Networks (GNNs) application for self-supervised network intrusion and anomaly detection. GNNs are a deep learning approach for graph-based data that incorporate graph structures into learning to generalise graph representations and output embeddings. As network flows are naturally graph-based, GNNs are a suitable fit for analysing and learning network behaviour. The majority of current implementations of GNN-based Network Intrusion Detection Systems (NIDSs) rely heavily on labelled network traffic which can not only restrict the amount and structure of input traffic, but also the NIDSs potential to adapt to unseen attacks. To overcome these restrictions, we present Anomal-E, a GNN approach to intrusion and anomaly detection that leverages edge features and graph topological structure in a self-supervised process. This approach is, to the best our knowledge, the first successful and practical approach to network intrusion detection that utilises network flows in a self-supervised, edge leveraging GNN. Experimental results on two modern benchmark NIDS datasets not only clearly display the improvement of using Anomal-E embeddings rather than raw features, but also the potential Anomal-E has for detection on wild network traffic.

Subjects: Machine Learning (cs.LG); Artificial Intelligence (cs.AI); Cryptography and Security (cs.CR); Networking and Internet Architecture (cs.NI)

Cite as: arXiv:2207.06819 [cs.LG]
(or arXiv:2207.06819v4 [cs.LG] for this version)
<https://doi.org/10.48550/arXiv.2207.06819> 

Submission history

- From: Wai Weng Lo [view email]
[v1] Thu, 14 Jul 2022 10:59:39 UTC (490 KB)
[v2] Wed, 20 Jul 2022 07:08:57 UTC (885 KB)
[v3] Thu, 21 Jul 2022 00:23:48 UTC (887 KB)
[v4] Sat, 23 Jul 2022 11:29:27 UTC (886 KB)

Download:

- PDF
- Other formats



Current browse context: cs.AI

< prev | next >
[new](#) | [recent](#) | [2207](#)

Change to browse by: cs

- cs.CR
- cs.LG
- cs.NI

References & Citations

- NASA ADS
- Google Scholar
- Semantic Scholar

Export Bibtex Citation

Bookmark



Bibliographic Tools

Code & Data

Demos

Related Papers

About arXivLabs

Bibliographic and Citation Tools

☐

Bibliographic Explorer [\(What is the Explorer?\)](#)

☐

Litmaps [\(What is Litmaps?\)](#)

☐

scite Smart Citations [\(What are Smart Citations?\)](#)

Which authors of this paper are endorsers? | [Disable MathJax](#) *(What is MathJax?)*