Exploring Temporal GNN Embeddings for Darknet Traffic Analysis

Original
Exploring Temporal GNN Embeddings for Darknet Traffic Analysis / Gioacchini, Luca; Cavallo, Andrea; Mellia, Marco; Vassio, Luca. - ELETTRONICO. - (2023), pp. 31-36. (Intervento presentato al convegno 2nd GNNet Workshop - Graph Neural Networking Workshop tenutosi a Paris, France nel 8 December, 2023) [10.1145/3630049.3630175].

Availability:
This version is available at: 11583/2984355 since: 2023-12-05T15:14:28Z

Publisher:
Association for Computing Machinery

Published
DOI:10.1145/3630049.3630175

Terms of use:
This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)
Exploring Temporal GNN Embeddings for Darknet Traffic Analysis

Luca Gioacchini  
Politecnico di Torino  
Turin, Italy  
luca.gioacchini@polito.it

Andrea Cavallo  
Politecnico di Torino  
Turin, Italy  
andrea.cavallo@polito.it

Marco Mellia  
Politecnico di Torino  
Turin, Italy  
marco.mellia@polito.it

Luca Vassio  
Politecnico di Torino  
Turin, Italy  
luca.vassio@polito.it

ABSTRACT

Network Traffic Analysis (NTA) serves as a foundational tool for characterizing network entities and uncovering suspicious traffic patterns, thereby enhancing our understanding of network operations and security. As successfully done in other domains, due to the scarcity of labelled data, Deep Learning (DL)-based solutions for NTA have started adopting a 2-stage approach: (i) a self-supervised upstream task generates compact and information-rich representations (embeddings) of network data without the need for a ground truth; (ii) the embeddings serve as input to specialized models for downstream tasks (supervised or unsupervised) – e.g. traffic classification or anomaly detection. Since graphs are intuitive representations of network traffic, in this work, we explore the potential of temporal Graph Neural Networks (tGNNs) in generating intermediate embeddings in a self-supervised fashion. We assess the quality of such embeddings by solving a host classification problem in a darknet traffic scenario. We evaluate static and temporal GNNs over a month-long period of traffic traces. We find that the inclusion of node features and temporal aspects in the model, together with an incremental training approach, allows for an accurate description of host activity dynamics and enables the creation of 2-stage NTA pipelines.

CCS CONCEPTS

• Networks → Network monitoring; • Security and privacy → Network security.

KEYWORDS

Darknets; Artificial Intelligence; Graph Neural Networks; Cybersecurity; Network Monitoring; Embeddings

1 INTRODUCTION

In the context of Network Traffic Analysis (NTA), Deep Learning (DL) techniques have emerged as powerful tools to address traffic classification problems [2, 18], anomaly detection [22] and exploratory traffic analysis [7, 13, 20], among others. Thanks to the availability of large data collections and user-friendly frameworks, such techniques are becoming fundamental for characterizing and comprehending the actions of network entities and unveiling significant patterns. However, differently from other domains, NTA applications typically present limited availability of labelled datasets and fast and complex dynamic data with evolving structures which complicate the training of DL models.

For this reason, recent DL-based solutions employ a 2-stage pipeline [8, 9, 15]. In the first stage, a self-supervised upstream task generates compact representations of input data in a latent space (i.e. embeddings) without the need for ground truth. Then, in the second stage, specialized machine learning or DL models operate on these embeddings to solve specific problems, referred to as downstream tasks (e.g. classification, clustering, anomaly detection). This approach is motivated by the expectation that embeddings that reflect the available relations and interactions between data points contain valuable and representative information that can be
leveraged to address several downstream problems, even though the embeddings are not specifically tailored for the final task.

Several techniques have been adopted to generate informative embeddings, i.e. the first stage of the pipeline. Many works adopt traditional feature engineering approaches and process the resulting datasets through (sparse) Autoencoders [12, 13, 16] or traditional Convolutional Neural Networks [1, 19]. Other works identify analogies between sequences of packets (or flows) and words in text documents. Hence, they generate embeddings borrowing techniques from the Natural Language Processing (NLP) field [6, 8, 20]. In the latter case, the adoption of techniques belonging to domains different from network traffic, like NLP, often requires an additional level of abstraction leading to hard-to-interpret solutions for networking experts. In fact, modelling network traffic as a graph is more intuitive and straightforward and some works started relying on Graph Neural Networks (GNNs) to capture the complex relation patterns of the network traffic. Indeed, GNNs are neural network architectures that directly operate on graphs and capture not only entity-specific information, but also connectivity patterns. Therefore, they represent a powerful tool for modelling network behaviour. Specifically, end-to-end GNN-based architectures are used to classify network packets [3, 23], and GNN-based autoencoders are applied to traffic flows classification [10, 11].

In this paper, we aim to generate robust embeddings (stage 1) that represent the activity of hosts sending traffic to darknet addresses. We propose the usage of temporal GNNs (tGNNs) as embedding generators to capture the complex spatial and temporal patterns found in network traffic. We design a downstream host classification task (stage 2) to evaluate the goodness of the embeddings, as sketched in Figure 1.

Darknets are sensors that observe traffic received by networks that are announced on the Internet but host neither production services nor client hosts. Specifically, they are commonly used to monitor incoming and potentially malicious attacks, since any packet reaching a darknet address is unsolicited. We model darknet traffic as a bipartite graph in which sender nodes (identified by their IP addresses) are connected to nodes representing the destination TCP ports. We process the graph to generate host embeddings using three different GNNs: a static Graph Convolutional Network (GCN) [14] adapted to dynamic scenarios through incremental training (i-GCN), a temporal GNN (GCN-GRU [24]) and the same temporal GNN trained incrementally (i-GCN-GRU). Additionally, to exploit the full potential of GNNs, we enrich the graph with node feature information related to the amount and type of traffic generated (received) by each host (port).

We evaluate the generated embeddings through a downstream node classification task where we label senders according to the available ground truth. We find that (i) node features are essential to map hosts belonging to the same class in the same region of the latent space (< 0.50 of average F1-Score without node features); (ii) the temporal GNN (GCN-GRU) better extracts the dynamics of host activities (0.75 of average F1-Score); (iii) the incrementally-trained temporal GNN (i-GCN-GRU) better follows the fast-changing behaviours of hosts improving the classification performance up to 0.80 of average F1-Score.

We show that the modelling of network traffic as a graph and the adoption of tGNNs extract meaningful host activity patterns and generate robust host representations, for which we envision several applications to supervised and unsupervised tasks (e.g. clustering), which can significantly advance the understanding and analysis of network behaviour.

2 HOST EMBEDDINGS WITH GNNS

We define \( \mathcal{V}_A, \mathcal{V}_B \) as two disjoint sets of nodes active in snapshot \( t \) and \( \mathcal{E}_{A,B} \) as the set of edges that in snapshot \( t \) link nodes in \( \mathcal{V}_A \) with nodes in \( \mathcal{V}_B \). We define a dynamic bipartite graph \( G = (\mathcal{V}, \mathcal{E}) \) as a sequence of \( T \) static bipartite graphs \( G^t = (\mathcal{V}^t, \mathcal{E}^t) \). More specifically, an edge \( e = (v_A, v_B, w) \in \mathcal{E}^t \) indicates that there exists a connection between nodes \( v_A \in \mathcal{V}_A \) and \( v_B \in \mathcal{V}_B \) with weight \( w \). Each node \( v \in \mathcal{V}_A \cup \mathcal{V}_B \) can be associated with a feature vector \( x^t_v \in \mathbb{R}^F \), where \( F \) is the number of features. In our case, \( \mathcal{V}_A \) contains the external hosts sending packets to the darknet. An edge \( e = (v_A, v_B, w) \) indicates that, in snapshot \( t \), \( v_A \) sent \( w \) packets toward the destination port \( v_B \).

GNNs [21] are deep learning models that exploit the structural information of a graph to generate meaningful representations for its nodes. We train the GNNs with a self-supervised task, i.e. link prediction. Specifically, at each snapshot \( t \), the GNNs generate node embeddings and estimate the likelihood of the connections \( \mathcal{E}_{A,B} \).

To exploit the full potential of GNNs, we enrich the graph with node feature information related to the amount and type of traffic generated (received) by each host (port).

\( i\text{-GCN: Adapting static GCN to dynamic scenarios.} \) Since the GCN is a static model, we adapt it to the time-evolving scenario of darknet traffic through incremental training, as illustrated in Figure 2a. Specifically, we train a GNN on the first graph snapshot \( G^1 \) (obtaining \( GCN_1 \)) and produce the embeddings for the active nodes. Then, for each subsequent snapshot \( t \in [2, T] \), we fine-tune the pre-trained model \( GCN_{t-1} \) on the graph snapshot \( G^t \) and we obtain \( GCN_t \). The resulting embeddings, thus, include past and latest information.

\( GCN\text{-GRU: Temporal GNN.} \) To model the graph structure and the dynamics of a temporal network, GCN-GRU [24] (a common tGNN) couples GNNs with recurrent neural networks, a
we train the model with
They collect large-scale Internet scans and represent a valuable
source of information for cybersecurity. In this work, we collect
3 DARKNET TRAFFIC
embeddings by feeding the model with the current graph snapshot
both the GCN and GRU layers. Differently from i-GCN, we produce
new GCN-GRU training approach. At each new time snapshot
more robust embeddings. In Figure 2c we overview the incremental
training approach to the tGNN to better follow
beddings for nodes active in each snapshot
𝐻
shots to train the GCN-GRU (GCN-GRU
tom) phases to produce node embeddings. We use the first
𝑀
𝑡
R puts through a GRU to model temporal behaviours. Formally,
quent graph snapshots independently and forwards their out-
𝐻
data. More in detail, the GCN-GRU applies a GCN to
ory to keep past information and merge it with new incoming
ploys Gated Recurrent Units (GRUs) [5], which rely on a mem-
popular tool to deal with time-evolving data. Specifically, it em-
employs Gated Recurrent Units (GRUs) [5], which rely on a mem-
ory to keep past information and merge it with new incoming data. More in detail, the GCN-GRU applies a GCN to
subsequent graph snapshots independently and forwards their out-
puts through a GRU to model temporal behaviours. Formally, $Z^t = \text{GRU}\left( \text{GCN}(G^{t-H}), \ldots, \text{GCN}(G^{t-1}), \text{GCN}(G^t) \right)$, where $Z^t \in \mathbb{R}^{|V^t| \times E}$ is the matrix containing the embeddings for all the nodes active in snapshot $t$.

In Figure 2b we overview the training (top) and inference (bottom) phases to produce node embeddings. We use the first $M$ snapshots to train the GCN-GRU ($\text{GCN-GRU}_M$). Notice that in this way we train the model with $M - H$ sequences of temporal graphs of length $H$. Then, we freeze it and use GCN-GRU$_M$ to compute embeddings for nodes active in each snapshot $t \in [M + 1, T]$.

i-GCN-GRU: Incremental extension of tGNN. Finally, we extend the incremental training approach to the tGNN to better follow the fast-changing dynamics of host activity patterns and produce more robust embeddings. In Figure 2c we overview the incremental training approach. At each new time snapshot $t$, we generate the new GCN-GRU$_t$ by updating GCN-GRU$_{t-1}$. Notice that we update both the GCN and GRU layers. Differently from i-GCN, we produce embeddings by feeding the model with the current graph snapshot and $H$ past graphs to exploit the GRU memory.

3 DARKNET TRAFFIC

Darknets are sets of IP addresses announced on the Internet but without hosting any services. Thus, all received traffic is unsolicited. They collect large-scale Internet scans and represent a valuable source of information for cybersecurity. In this work, we collect data from a /24 darknet in our university campus network for 31 days (2021-12-01 to 2021-12-31). We focus on TCP traffic, which accounts for 93.7% of traffic, and remove hosts that send less than 5 packets per day [8]. We observe 60 106 remaining hosts sending more than 62 million packets in a month.

3.1 Darknet traffic as a bipartite graph

We consider each day of our collection as a snapshot. According to definitions in Section 2, let $\mathcal{V}^t_A$ be the set of hosts targeting darknets at snapshot $t$ and let $\mathcal{V}^t_B$ be the set of the 2 500 most contacted darknet ports at snapshot $t$ plus one additional node representing all the remaining ports [8].

We obtain the dynamic bipartite graph $\{G^t\}_{t=1}^{T=31}$, which has 6 392 average nodes per snapshot and 49 198 average edges per snapshot. We compute a set of features for both host nodes and ports. Thus, each node is associated with a feature vector $x^t$ of size 37, which summarizes the traffic intensity and type as detailed in Table 1. The function $\text{Stats}(\cdot)$ extracts the sum, minimum, maximum, average and standard deviation of the provided entity.

3.2 Ground Truth

To perform classification as downstream task, we generate a ground truth for hosts considering four data sources: (i) ground truth available from [8] (ii) presence of fingerprints of Mirai-like malwares observed in received packets [4]; (iii) information from a public

Table 1: Considered node features.

<table>
<thead>
<tr>
<th>Host Node Features</th>
<th>Port Node Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Contacted darknet ports</td>
<td>#Hosts contacting a port</td>
</tr>
<tr>
<td>Stats(#Packets per darknet port)</td>
<td>Stats(#Packets per source host contacting a port)</td>
</tr>
<tr>
<td>#Contacted darknet hosts</td>
<td>0-valued dummy feature</td>
</tr>
<tr>
<td>Stats(#Packets per darknet host)</td>
<td>Stats(#Packets per darknet port)</td>
</tr>
</tbody>
</table>

Table 2: Dataset and Ground Truth overview.

<table>
<thead>
<tr>
<th>Total</th>
<th>Daily (Avg.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td>Ports</td>
</tr>
<tr>
<td>Mirai-like</td>
<td>16 147</td>
</tr>
<tr>
<td>Brute-forcers</td>
<td>976</td>
</tr>
<tr>
<td>Spammers</td>
<td>1 014</td>
</tr>
<tr>
<td>Shadowserver</td>
<td>289</td>
</tr>
<tr>
<td>Driftnet</td>
<td>252</td>
</tr>
<tr>
<td>Internetcensus</td>
<td>271</td>
</tr>
<tr>
<td>Censys</td>
<td>329</td>
</tr>
<tr>
<td>Rapid7</td>
<td>344</td>
</tr>
<tr>
<td>Onyphe</td>
<td>115</td>
</tr>
<tr>
<td>Netysystems</td>
<td>45</td>
</tr>
<tr>
<td>Shodan</td>
<td>36</td>
</tr>
<tr>
<td>Exploiters</td>
<td>430</td>
</tr>
<tr>
<td>Securitytrails</td>
<td>18</td>
</tr>
<tr>
<td>Intrinsc</td>
<td>12</td>
</tr>
<tr>
<td>Unknown</td>
<td>39 828</td>
</tr>
<tr>
<td>Total</td>
<td>60 106</td>
</tr>
</tbody>
</table>
After a parameter tuning stage, for which we omit the details for the sake of brevity, we design the model architecture as follows: in all models, the graph convolution modules have three layers (L=3) of 37 input features, 1024 and 512 neurons respectively; for GCN and i-GCN, we add a fully connected layer at the end with size $E = 128$; for GCN-GRU variants (overviewed in Figure 3), the GRU outputs embeddings sized $E = 128$. The prediction head of all models consists of a hidden layer with 64 neurons and an output layer for the pretext task with 2 neurons (existing or non-existing edge) on which we apply the Negative Log Likelihood loss function. Note that for inference we do not use the link prediction head. We train the GCN and GCN-GRU for 50 epochs with an early stopping condition of 3 iterations as patience. For incremental trainings, we train and update the weights for 1 epoch on each snapshot if node features are present, and for 5 epochs otherwise.

Unless otherwise specified, we set the GRU history $H = 5$ and $k = 3$ for the kNN classifier.

We develop all the models using the Python library PyTorch and run the experiments on a Tesla V100-PCIE-16GB. We hope our results and methodological insights can inspire the application of temporal GNN to the analysis of other network traffic traces too. For that, we release our source code and the dataset used in the paper.3

### 4.2 NLP embeddings as baseline

As baseline, we compare GNN-based embeddings with our previous approach i-DarkVec [8], which relies on Word2Vec [17] to create the intermediate embeddings for hosts. We assume that the reader is familiar with Word2Vec and provide a brief overview of i-DarkVec. In a nutshell, at each snapshot, we group packets addressed to the same darknet TCP port and extract the sequence of senders (i.e. the source hosts generating them) as they reach each port. Analogously to NLP, hosts represent "words", whereas ports represent "sentences". We feed the generated corpus as input to Word2Vec. i-DarkVec produces contextual host embeddings such that hosts co-occurring in time when targeting similar ports appear close in the latent space. The kNN classifier on these embeddings achieves $0.77 \pm 0.02$ of average F1-Score over the 11 testing days.

### 5 EXPERIMENTAL RESULTS

In Table 3 we report the per-class average F1-Score and standard deviation over the 11 test snapshots. Classes are ordered by decreasing support size. The support size counts host appearances for each class over the 11 test snapshots (possibly with repetitions).

Firstly, we focus on the macro average F1-Score. We observe that (i) tGNN without node features fails to capture meaningful dynamics from darknet traffic (average F1-Score $< 0.50$ for all the models); (ii) associating graph nodes with features empowers the tGNN to generate more informative embeddings. The average F1-Score improves by up to $\approx 0.39$.

Focusing on single classes, we observe that (i) since darknet implies a low level of interaction with senders, the classes deduced from honeypot (i.e. Brute-forcer, Spammer, and Exploiter) exhibit different patterns resulting in weak classification performance (F1-Score $< 0.65$); (ii) for the other classes, all GNNs achieve an average per-class F1-Score $> 0.80$.

Comparing standard versus incremental models, we observe that (i) a static model (GCN) with standard training over more epochs

---

1https://github.com/mcollins_at_isi/acknowledged_scanners

2https://github.com/SmartData-Polito/gnn-for-darknet.git
The main advantage of the tGNNs approach relies on enhanced intuitiveness and flexibility: (i) Whereas i-DarkVec requires extracting sequences of hosts by destination ports to highlight coordinated behaviours, tGNNs leverage the explicit connections between hosts and ports; (ii) Enriching NLP embeddings with host features, although not explored in this work, requires additional manipulation of the embeddings (e.g., concatenation of features and embeddings), whereas the tGNNs inherently include node features by design.

5.1 Impact of parameters

Finally, we evaluate the impact of the history parameter $H$ and the training epochs for i-GCN-GRU.

Impact of history $H$. In Figure 4a we evaluate the impact of the length of the temporal component of the tGNNs by reporting the average F1-Score for different values of $H$. Note that $H = 0$ corresponds to the i-GCN of Table 3. Generally, enhancing the memory length yields better results until a saturation point. This underscores the significance of incorporating historical data using time-aware GNNs, which effectively capture the evolution of the traffic over time.

Impact of training epochs. In Figure 4b we report the average F1-Score when training (fine-tuning) the i-GCN-GRU for an increasing number of epochs. Here the considerations of Table 3 are confirmed: when the model is trained for a large number of epochs on the current snapshot, it tends to overfit the model on the last time snapshot of data, leading to a loss of past learned information. This is reflected by a decrease in classification performance.

6 CONCLUSIONS

In this paper, we presented an initial exploration of tGNNs for darknet traffic analysis. We represented darknet traffic at packet level as a bipartite graph and generated host embeddings in a self-supervised way relying on both static and temporal GNNs. We defined node features and we experimented incremental training strategies to better follow the dynamics of the network.

Experimental results show that (i) GNNs without node features fail to extract similar behaviours among senders; (ii) When using node features, GNN embeddings are comparable with those produced by i-DarkVec, which relies on an NLP technique; (iii) coarse
fine-tuning of a tGNN model pre-trained on the previous snapshot can preserve useful past information, following the frequent changes in daily traffic.

All in all, despite the growing trend of NLP and cross-domain adaptation like i-DarkVec, this preliminary work highlights that more intuitive solutions based on GNNs can yield comparable results. Temporal GNNs are a more natural tool than NLP-style approaches for enhancing our comprehension of highly dynamic network traffic, facilitating the enhancement of embedded knowledge with richer information through node or edge features.

Future developments include the evaluation of the proposed method on additional datasets encompassing other darknet traces as well as different computer network scenarios. Furthermore, the comparison with other approaches relying on feature engineering or ML can provide further insights on the advantages and disadvantages of GNNs. A promising extension of the proposed architecture comprises a deeper investigation of both node and edge features and the application of different and more sophisticated GNN architectures. Moreover, the generated embeddings can serve as information-rich representations for several supervised or unsupervised downstream tasks, such as clustering or anomaly detection.

ACKNOWLEDGMENTS

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU and the PRIN Project xInternet (eXplainable Internet - 20225 CETN9 - PRIN 2022).

REFERENCES