GNNs and Node Entropy for Misinformation Spreader Detection on Twitter Network

Conference Paper · November 2023

CITATIONS
0

READS
38

2 authors:

Asep Maulana
Simula Research Laboratory
19 PUBLICATIONS **81** CITATIONS
SEE PROFILE

Johannes Langguth
Simula Research Laboratory
80 PUBLICATIONS **504** CITATIONS
SEE PROFILE

GNNs and Node Entropy for Misinformation Spreader Detection on Twitter Network

Asep Maulana[1] and Johannes Langguth[1]

Simula Research Laboratory, Oslo, Norway
asep@simula.no, langguth@simula.no
WWW home page: https://www.simula.no/

1 Introduction

In the era of rapid social media expansion, the proliferation of misinformation has emerged as a pressing and intricate challenge, particularly on platforms such as Facebook and Twitter. The imperative to identify and address the dissemination of misinformation agents has never been more pronounced, given its potential for deleterious effects on both users and the broader society. In response, this paper introduces a groundbreaking approach aimed at discerning potential aberrant nodes within Twitter networks that act as conduits for spreading misinformation. This method ingeniously integrates Graph Neural Networks (GNNs) with an entropy-based mechanism to achieve its objectives.

By leveraging the capabilities of GNNs, this approach effectively condenses complex information diffusion patterns and user attributes into concise node embeddings [2]. This fusion of network structure and user characteristics offers a nuanced representation of the complex dynamics underlying information propagation. Moreover, this paper pioneers the use of node attribute entropy analysis on these embeddings, enabling the identification of nodes that exhibit attribute distributions markedly divergent from the norm. In our research, we conducted thorough experiments on real-world Twitter datasets, focusing on content related to misinformation. Our innovative approach demonstrates its effectiveness in pinpointing potential anomalous nodes that act as misinformation spreaders across different categories. By leveraging the power of Graph Neural Networks (GNNs) and seamlessly incorporating entropy-based methods through node embeddings, our methodology presents a promising pathway for gaining deeper insights into the actions of unique misinformation spreaders and their potential impact on others.

2 Methodologies

Our research approach centers on utilizing node embeddings generated by GNNs and computing Node Entropy for node attributes, subsequently classifying nodes exhibiting high entropy. Node embedding through Graph Neural Networks (GNNs) constitutes a fundamental technique in network analysis and machine learning. GNNs play a pivotal role in transforming intricate network structures into low-dimensional vector representations, effectively encapsulating both structural and semantic node information. They

excel in capturing nuanced patterns of information diffusion, relationships, and community structures within graphs. Furthermore, our approach employs node entropy to classify nodes that display significant differences compared to others within the same class, enhancing the granularity of node characterization. The Node Entropy Theory (NET) is a concept that originates from information theory [1], and is adapted to the context of networks [3]. It focuses on quantifying the uncertainty and information content of individual nodes within a network. Node Entropy Theory finds applications in various fields, such as social network analysis, biological networks, and communication networks [3] [8] [7]. In Node Entropy Theory, we are interested in the entropy associated with individual nodes within a network. Consider a network represented as a graph G = (V, E), where V is the set of nodes (vertices) and E is the set of edges connecting the nodes. For a specific node v in V, we define its Node Entropy H(v) as the Shannon Entropy of the probability distribution of the node's neighboring states.

Let's denote the set of neighboring nodes of v as N(v). For each neighbor u in N(v), there is an associated probability P(u) representing the likelihood of v being in the state represented by u.

Then, the Node Entropy H(v) is given by:

$$H(v) = -\sum_{u \in N(v)} P(u) \log_2(P(u))$$

Where the summation is performed over all neighbors u of v. In some cases, the interactions between nodes may have different strengths or weights. To consider these weights in the Node Entropy calculation, we introduce a weight function w(u, v) that gives the weight of the edge between nodes u and v. The Weighted Node Entropy $H_w(v)$ is then calculated as follows:

$$H_w(v) = -\sum_{u \in N(v)} w(u,v) \cdot P(u) \cdot \log_2(P(u))$$

Where w(u, v) represents the weight of the edge between nodes u and v, and the summation is performed over all neighbors u of v.

The key insight derived from node entropy within the network lies in its ability to delineate the character of individual nodes. Nodes with lower entropy typically exhibit similar characteristics, sharing commonalities within their class, whereas nodes with higher entropy tend to stand out as notably distinct from their counterparts (that can be categorized as anomalous nodes). This distinction is particularly pronounced for nodes with high entropy, as they tend to establish diverse connections and engage more actively within the network.

3 Results

The datasets consists of a Twitter interaction graph of 1.6 millions nodes and about 258 millions edges [4]. The nodes represent Twitter accounts, and a pair is connected by an edge if at least one account has retweeted at least one tweet of the other. Although the graph is inherently directed, our analysis focuses on a subgraph derived from the larger graph, which is undirected and comprises 1772 nodes connected by 3488 edges.

These nodes are labeled to indicate whether their associated tweets promote or discuss one of nine categories of conspiracy theories [5]. Additionally, the vertices in this subgraph are enriched with user attributes encompassing six different characteristics. In this graph with node attributes, we encounter a classification challenge encompassing nine distinct misinformation categories [5] [6]. Each category is further divided into three classes: Class 1 comprises *unrelated*, Class 2 is *related* and Class 3 is *promoting* associated with misinformation spreading. We assess entropy for each node in both Class 2 and Class 3. For nodes to be classified as having high entropy, their entropy value must exceed the mean plus one standard deviation of the entropy values within their respective class. Conversely, nodes with high centrality are those whose centrality values surpass the mean across all nodes in the entire network. In addition to measuring centrality in our analysis, we employ four distinct centrality metrics: Betweenness, Closeness, Degree, and Eigenvector centrality. This comprehensive approach allows us to thoroughly evaluate the role and significance of individual nodes in the propagation of misinformation within Class 2 and Class 3.

Table 1. Number of misinformation spreader in different categories along with the number of nodes with high entropy as well as node with high entropy and centrality

Category	Number of Misinformation Spreader		Node with high Entropy		Node with high Entropy and Centrality	
	Node class2	Node class3	Node class2	Node class3	Node class2	Node class3
Category1	9	29	2	3	2	3
Category2	88	66	17	9	16	2
Category3	109	94	23	10	21	5
Category4	100	144	22	19	19	13
Category5	71	186	14	26	11	17
Category6	37	25	6	3	5	2
Category7	31	106	8	11	7	9
Category8	18	112	3	12	2	5
Category9	35	53	5	8	3	5

Summary In our research, we focus on identifying specific nodes acting as aggressive misinformation spreaders, particularly those with the potential to disseminate extensive misinformation across various categories. Our initial detection process involves the computation of node entropy for each node within a specific class. Nodes exhibiting elevated entropy values, signifying significant distinctions compared to their peers, are singled out through an examination of their vector values within the node embeddings. This methodology allows us to identify nodes within the class that possess unique char-

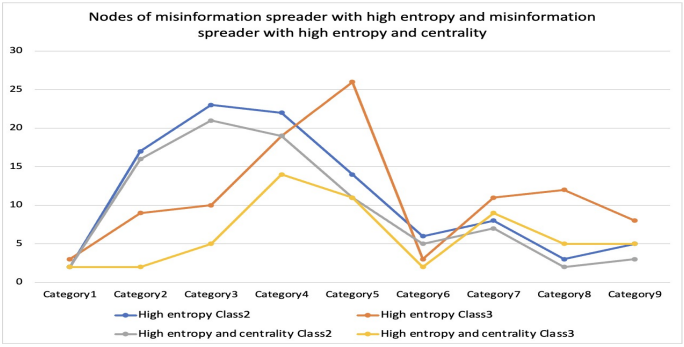

Fig. 1. Number of nodes for misinformation spreader in different category on the twitter network with high entropy only as well as high entropy and centrality

acteristics based on their embedding representations, facilitating the detection of noteworthy patterns or anomalies. Moreover, in cases where these high-entropy nodes also demonstrate high centrality, we deduce that these nodes are acting as aggressive and detrimental agents in the propagation of misinformation within the network. Additionally, we delve into the intriguing question of whether anomalous nodes characterized by high entropy but lacking high centrality still exert substantial influence in the dissemination of misinformation.

References

1. Shannon, C. E. (1948). A mathematical theory of communication. The Bell System Technical Journal, 27(3), 379-423.
2. Chen, Y., Wu, L., & Zaki, M. (2020). Iterative deep graph learning for graph neural networks: Better and robust node embeddings. Advances in neural information processing systems, 33, 19314-19326.
3. Žalik, K. R., & Žalik, B. (2018). Memetic algorithm using node entropy and partition entropy for community detection in networks. Information Sciences, 445, 38-49.
4. Pogorelov, K., Schroeder, D. T., Brenner, S., Maulana, A., & Langguth, J. (2022). Combining tweets and connections graph for fakenews detection at mediaeval 2022. In Multimedia Benchmark Workshop.
5. Langguth, J., Filkuková, P., Brenner, S., Schroeder, D. T., & Pogorelov, K. (2023). COVID-19 and 5G conspiracy theories: long term observation of a digital wildfire. International Journal of Data Science and Analytics, 15(3), 329-346.
6. Langguth, J., Schroeder, D. T., Filkuková, P., Brenner, S., Phillips, J., & Pogorelov, K. (2023). COCO: an annotated Twitter dataset of COVID-19 conspiracy theories. Journal of Computational Social Science, 1-42.
7. Wen, T., Duan, S., & Jiang, W. (2019). Node similarity measuring in complex networks with relative entropy. Communications in Nonlinear Science and Numerical Simulation, 78, 104867.
8. Tee, P., Parisis, G., & Wakeman, I. (2017). Vertex entropy as a critical node measure in network monitoring. IEEE Transactions on Network and Service Management, 14(3), 646-660.