Anomaly Detection using Graph Neural Networks

Anshika Chaudhary, Himangi Mittal, Anuja Arora
Computer Science and Engineering
Jaypee Institute of Information Technology
Noida, India
anshika.ch412@gmail.com, himangimittal@gmail.com, anuja.arora29@gmail.com

***Abstract*—Conventional methods for anomaly detection include techniques based on clustering, proximity or classification. With the rapidly growing social networks, outliers or anomalies find ingenious ways to obscure themselves in the network and making the conventional techniques inefficient. In this paper, we utilize the ability of Deep Learning over topological characteristics of a social network to detect anomalies in email network and twitter network. We present a model, Graph Neural Network, which is applied on social connection graphs to detect anomalies. The combinations of various social network statistical measures are taken into account to study the graph structure and functioning of the anomalous nodes by employing deep neural networks on it. The hidden layer of the neural network plays an important role in finding the impact of statistical measure combination in anomaly detection.**

Keywords— Graph Neural Network, Anomaly Detection, Social Network, Enron dataset, twitter dataset

I. INTRODUCTION

Anomaly or outlier detection is a procedure to find data points which have a spurious behaviour. It happens around us in the form of fraud detection [6], network surveillance [7], public safety and security [8], intrusion detection [9], medical problems [10], false advertisement and many more. The term anomalies are used synonymously with outliers, noise, and deviations. Anomalies may occur as point anomalies or group anomalies [11]. Point anomalies can be defined as single data points having deviant behaviour from the rest of the network. Whereas group anomalies are collective anomalous data points, mostly observed in fraudulent activities. Our work is focused on point anomalies.

Graph-based anomaly detection can be helpful in finding the spammers [14], outspread of any information [16], fake reviews [17] or malicious activities [18]. Thus, detecting anomalies is a vital task to ensure safety and security for the users in a network. Analysing large graphs to find out the anomalies can also yield important and interesting information about the graph structure.

Detecting spam profiles is considered as one of the most challenging issues in the online social network. Most recent work in this direction has been done by Farris et. al. in 2018, a hybrid model on SVM-WOA [14] is introduced. This model is applied and tested on different lingual context, collected from Twitter in four languages: Arabic, English, Spanish, Korean to identify the most influencing features/factor. This model can effectively help in designing more accurate and insightful spam detection models for an online social network.

Social networks have become a hot topic today and much of the work has been done on social networks including visualization[24] [25], recommendation, link prediction on spatial as well as temporal networks[26]. However, with the increasing use of these platforms, user come under the threat of several anomalies in which horizontal anomalies are difficult to detect and hazardous for any network. These are the anomalies caused by a user because of his/her anomalous and changing behaviour towards different sources. A self-healing neuro-fuzzy approach is used for the detection, recovery, and removal of horizontal anomalies efficiently and accurately[12]. This approach model is evaluated with three datasets: DARPA'98 benchmark dataset, synthetic dataset, and real-time traffic. The evaluation over DARPA'98 dataset demonstrates that the proposed approach is better than the existing solutions.

In a social network application, anomalous node detection is actually a challenging task. On one side, a number of utilities exist in social networking sites and on the other end, free handed content delivery led to extensive misuse. Many cyber-attacks through social media content show that it has become prime source of malicious activities. These attempts are made to are made to earn illegal profits through rumour spread, enhance the prestige of an unknown product, etc. Therefore, in order to catch and abbreviate security risk in the social network, techniques required to detect anomalous behaviour in a social network.

According to observation, malicious users follow some ambiguous patterns while sharing information. In this research work, few hypotheses are considered to capture the behaviour of anomalous nodes. Initially, adjacency matrix of the dataset is taken as input for graph neural network and then topological characteristics of the targeted datasets are computed. This work is inspired by graph-based anomaly detection. Deep learning technique is utilizing in order to detect nodes containing anomalous behaviour [1]. The outliers are labelled as a distrustful node with the help of social network statistical measures: Between Centrality, Degree, and Closeness. These parameters are taken into account to understand the structure of the graph. These topological characteristics are used to exploit the anomalous node behaviour. Following contributions are made in this research work:

RC1: Uses graph neural network in order to detect anomaly in social network.

RC2: Impact of statistical properties of a social network is tested and empirical validation of results is evaluated on Enron and Twitter dataset.

The paper is divided into five sections. The first section is the same introduction section which discusses the problem domain. Section 2 covers the related works done in the domain of anomaly detection. Following this, the third section presents the considered hypothesis, dataset and graph neural network which is used to detect the anomalies in a social network. The fourth section shows the experimental setup and

978-1-7281-0211-5/19/$31.00 2019 ©IEEE

results of anomaly detection on two datasets. Finally, section 5 concludes the work.

II. Related Work

Recently, there has been a boost in the area of data mining in graphs which is further extended to spatial and temporal graphs[26]. Much work has been done on finding valuable information from the structure of graphs, however, a little work has been done in the area of anomaly detection.

For anomaly detection, techniques of supervised and unsupervised learning [2] require the data consisting of some nodes labelled as outliers and the rest as normal nodes. Surveys [3], [4] have been done which present the various approaches to detect anomalies. Basic techniques for anomaly detection include the statistical methods which find the deviation from common statistical properties such as mean, median, mode, and quantiles. Recent techniques utilize machine learning such as density based clustering, K-nearest neighbour Support Vector Machines (SVM) to serve the purpose of detecting and classifying the anomalies based on an initially large set of features. Techniques using a variation of Bayesian network [5] have been used in finding group anomalies by using point activities data of a user and pairwise communication data. An anomaly can be defined in many terms such as outliers, exceptions or abnormality that represent unusual, illegal or malicious activities. The presence of anomalies is considered on the basis of functional structure which is different from the normal model. It was witnessed that the attacks have a huge distributed effect through engagements in social network sites as illegal users making use of it differently obeying patterns in a different manner from their peers.

The initial impetus has been done by Gori et.al. in 2005 where this term graph neural network (GNN) came in limelight[19]. Further study is continued by Li et. al. in 2016 about Gated graph neural network [20]. Using neural network models like RNN and CNN is a somewhat challenging problem to work upon arbitrarily structured graphs so Kipf et. al. adopted the somewhat similar approach and initiated from the spectral graphs convolutions [1] [22].

Application of anomaly detection are observed widely in the Twitter network to detect spammers. In the work of [27], two algorithms DenStream and StreamKM++ have been employed. The former algorithm is a modified density based clustering method (DBSCAN) to generate p micro clusters. The latter algorithm used k-means clustering method to choose the tightest cluster. Anomaly detection in dynamic networks have also been worked upon. In the survey [28], various types of anomalies in the form of nodes, edges, subgraphs and events have been discussed, along with the detection techniques like communities, probabilistic, compression, representative and distance. Some other latest works of anomaly detection in graphs are enlisted in table 1. It shows that in recent years convolution neural network, graph convolution network, and neuro-fuzzy approaches are mainly used for anomaly detection. The accuracy achieved using neural techniques varies from 81-98 % for various social network applications.

TABLE I: Latest works on Anomaly Detection in Graphs

YEAR	TITLE	TECHNIQUES	RESULTS
2018	Web traffic anomaly detection using C-LSTM neural networks [13]	CNN+LSTM+DNN	Accuracy: 98.60%
2018	Heterogeneous anomaly detection in social diffusion with discriminative feature discovery [15]	Parameter-free framework(HADISD)	Precision: 89.7% Recall: 91.3% F1-score: 90.5%
2018	Network Anomaly Detection Using Recurrent Neural Networks[23]	LSTM	Accuracy: 84%
2017	Neuro-Fuzzy Based Horizontal Anomaly Detection In Online Social Networks [12]	A self-healing neuro-fuzzy approach (NHAD)	Accuracy: 99.98% Precision: 98.1% Detection Rate: 97.97%
2017	Semi-Supervised Classification with graph Convolution Networks[1][21]	GCN	Accuracy: 81.50%

III. Methodology

To detect the anomalies in the graph, simply employing the classification, community detection or clustering techniques will fail to capture the behaviour of the anomalies. An unusual activity or different behaviour of graph exhibits abnormality or outlier in a social media application..Therefore, in order to find out these abnormalities, a graph-based approach is applied to detect the anomalies. The aim of the work is to validate graph neural network for anomaly detection and try to find out the impact of social network statistical properties on anomaly detection. Figure 1 depicts the overview of the graph-based approach which is experimented to detect anomalies. Initially, social network based data has been selected.

TABLE II: Statistics of the dataset

Dataset	Nodes	Edges
Enron	11703	450813
Twitter	76851	342153

This data is augmented by computing and adding its statistical properties. Further, Graph neural network is applied on the

graph adjacency matrix to classify nodes in two categories- anomaly, general(not anomalous).

A. Hypothesis for Social Network Analysis

For anomaly identification, node information in form of its statistical properties has been used as a feature set. The problem of detecting this anomalous subgraph is formulated in terms of a hypothesis between many nodes.

- ***Hypothesis 0:*** *An anomalous node will have a higher degree*

  In a social network, an anomalous network will try to influence maximal nodes by connecting to as many nodes as possible, heaving a higher degree than normal.

- ***Hypothesis 1:*** *An anomalous node will have a higher between centrality*

  If the first hypothesis is true, it will be peculiarly connected a large percent of nodes of a social network and will lie in the shortest paths between many nodes.

- ***Hypothesis 2:*** *An anomalous node will have higher a closeness centrality*

  If the two hypotheses hold true, the node being largely connected in the network will have small paths to the other nodes, hence, will be closer to the nodes in the network.

B. Datasets

The experiments are performed on two datasets- Enron dataset and Twitter dataset.

Enron is an email communication network which has been widely used for anomaly detection in networks. Nodes of the network are email addresses which are changed to numeric id in our work. An undirected edge connects two nodes if an address i send an email to address j. The dataset is available on https://www.cs.cmu.edu/~./enron/. The given Enron dataset contains only five anomalous nodes. We have incorporated and imputed around 40% nodes as abnormal/outlier nodes in Enron dataset based on hypothesis mentioned in section III(A).

Another dataset is from a social networking site Twitter. A Twitter social network consists of followers and followings those are connected to each other based on a posted tweet, mentioned mention, following, and replying. In our work, we have utilized the connections made by the follower network only by using a directed edge. The dataset is available on https://snap.stanford.edu/data/higgs-twitter.html. This dataset is useful to validate our work on large, directed graphs as Enron dataset contains less number of nodes and undirected edges. Dataset details are depicted in table 2 which shows the number of nodes and edges taken in Enron and Twitter datasets respectively.

C. Anomalous Nodes Assignment Criteria

Data augmentation technique is applied and datasets are tweaked. These parameters since they take into account the graph structure and will help to examine the graph structure

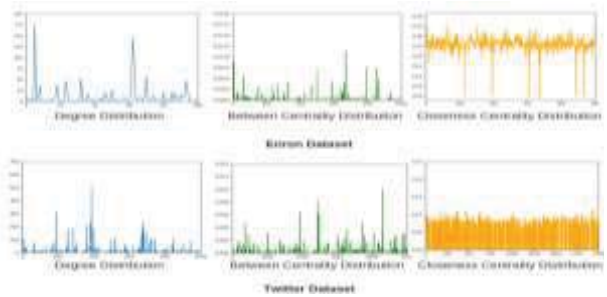

Fig 1. Parameter Statistics on Enron and Twitter Datasets

of an anomaly. Anomalous nodes are assigned to both the datasets based on three statistical graph properties- Betweenness Centrality α(v), Closeness centrality β(v), and Degree centrality γ(v) which are calculated (1), (2) and (3) respectively.

$$\alpha(v) = \Sigma \frac{\sigma(s,t|v)}{\sigma(s,t)} \tag{1}$$

$$\beta(v) = \Sigma A_{ij} \tag{2}$$

$$\gamma(v) = \frac{n-1}{\sum_{v=1}^{n-1} d(v,u)} \tag{3}$$

These three parameters are used to define the characteristics of the anomalous nodes (section III A). Further, all parameters individually and in groups/pairs are used to tune the system and find out accuracy for anomalous nodes identification.

The statistics of the parameters on both the datasets can be seen in Figure 1. The image shows the degree distribution, between centrality distribution and the closeness distribution. The x-axis of the graph shows the number of nodes and the y-axis shows the frequency of the nodes with the same value. Due to a large number of nodes, the parameter value of every node could not be presented, hence, the nodes are taken as bins and the frequency of the bins is shown. The threshold for the data augmentation on the datasets is chosen in a way that 40%-60% nodes can be labeled as outliers. The threshold was decided with reference to these parameter distributions.

D. Graph Neural Network

An anomalous shows peculiar behaviour which has a great deviation from a normal node. We consider the case that in a social network, there will be two extreme behaviours shown by the outliers.

Either, they will be connected to only a few people or will be connected to a large percent of the nodes in the network. We do not follow with the first extreme as a person might join the network but may not be an active node. However, the second extreme behaviour shows signs of anomalous behaviour. Therefore, we consider the assumption that an anomalous node will have a large number of

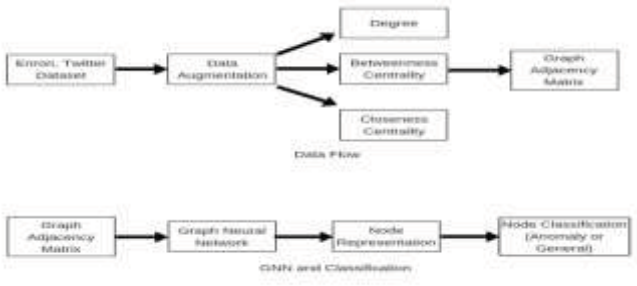

Fig 2: Data Preprocessing/Data-Flow and GNN Block Diagram

connections in an attempt to influence the network as much as possible. It will try to act as a central node in a network so that it can give an impact to its neighbouring nodes. Also, having a large number of connections, it can reach out to the whole network in short paths, thus being close to each and every node in the network. These hypotheses can also be used in detecting the spammers in a network.

The three hypothesis take into the graph structure of the anomalous nodes and yield features incorporating it. This will also be helpful in the application of neural network model. Once the three parameters are calculated and data is augmented, we find out a representation vector of each node in the network with the graph neural network. For the network input and computation, we consider the following:

- Given a graph G = (V, E) having N number of nodes and E number of edges.
- Let A denote the matrix of size N*N, representing the adjacency matrix of the graph.
- Let W denote the weight matrix initialized uniformly.
- Let H(l) denote the l-th hidden neural network layer.

Our goal is to accurately classify the nodes of the graph as anomalous or normal using the graph neural network. The input to the neural network will be the adjacency matrix of the graph and thereafter, we use the layer-wise propagation rule.

$$f(H(l), A) = \sigma(AH(l)W) \quad (4)$$

Here, σ is the ReLU activation function used for the first layer and sigmoid activation for the output layer. We build our neural network using the Keras library. Weights are initialized using uniform random initialization.

IV. Experiments

We divide the dataset into 80-20 ratio and run the graph neural network for 100 epochs. For compiling the Keras model, Adam optimizer and Binary-Cross Entropy are used for optimization and loss computation. Table 3 shows the classification results for Enron dataset for best suitable thresholds of betweenness, closeness and degree centrality.

TABLE III: Results of the parameters on Enron Dataset

Parameter	Threshold	Accuracy
Between Centrality	1*10^-7	0.8615
Degree	70	0.8632
Closeness	0.25	0.8611

TABLE IV: Results of the parameters on Twitter Dataset

Parameter	Threshold	Accuracy
Between Centrality	1*10^-7	0.8126
Degree	70	0.8157
Closeness	0.25	0.8118

Best achieved accuracy corresponding to an individual parameter for a specific threshold is presented in table 3 for Enron dataset. The same threshold was used for the Twitter dataset to mark the nodes as anomalous and general(see table 4). Using a threshold of 1*10^-7 on betweenness centrality, 70 for degree and 0.25 for closeness centrality, nodes having value greater than threshold were labelled as outliers. Thresholds were chosen by the trial and error method to yield around 40% - 50% of the dataset as outliers.

Comparing the accuracy of the parameters found on both the datasets, we can conclude that degree is a better parameter to capture the nature of anomalous nodes and hence, hypothesis 1 holds true.

For carrying out fraudulent activities, anomalies will try to connect with and affect as many people as possible. This justifies the advantage of degree parameter over others. Our hypothesis gives a good accuracy and generalizes well over both the datasets. Thus, we can conclude that our hypotheses hold true to detect anomalies in a social network.

We conduct another experiment by making a combination of two to further study the nature of anomalies. This will rank the parameters to find out which of them is a better measure in observing the behaviour of an anomaly. Table 5 and Table 6 presents the combined parameters based anomaly detection results for Enron and Twitter dataset respectively. Results show that combined parameters help in enhancing the anomaly detection accuracy. For the combination of parameters, we can observe that degree is the best parameter which captures the behavior of

TABLE V: Results on Enron Dataset

Parameter	Threshold	Accuracy
Between Centrality, Degree	1*10^-7, 70	0.9845
Between Centrality, Closeness	1*10^-7, 0.25	0.9006
Closeness, Degree	0.25, 70	0.9749

TABLE VI: Results on Twitter Dataset

Parameter	Threshold	Accuracy
Between Centrality, Degree	1*10^-7, 70	0.9823
Closeness, Degree	0.25, 70	0.9756

anomalous nodes. This also validates our hypothesis 1 and the assumption that anomalous nodes tend to connect to maximal nodes as possible to be a central node and be close to each and every node as much as possible. Our work outperforms the works [6] [12] in a way that it takes the graph structure by

considering the degree, closeness and betweenness. By the definition of anomaly, the node will have a peculiar behaviour of having very large or very few connections, thus, verifying our approach.

V. Conclusions

In this work, we presented a deep learning model, Graph Neural Network to detect the anomalies and outliers in a social network. We also present three hypothesis stating the behaviour of anomalous nodes and try to prove them using our model. Validation of the efficiency of our model was done on two datasets - Enron (email communication network) and Twitter (social networking site). The number of outliers in the dataset were augmented using the node properties - degree, between centrality and closeness centrality. These parameters were chosen since they take into account the structure of the graph. We show the results by taking these parameters individually and as a combination which achieves good accuracy over the datasets and hence, proves our hypothesis true.

VI. Future Work

Detecting anomalies can help to reduce the fraudulent activities or spamming spreading in the network. For this, efficient method need to be developed which take into account the behaviour of anomalies to its core. Graph Neural Network can capture the features and establish well relationships between them due to the hidden layer. Experimenting with more features and testing it on neural networks can broaden the study on the nature of anomalies.

References

[1] Semi-Supervised Classification With Graph Convolutional Networks, Thomas N. Kipf, Max Welling, ICLR 2017

[2] Lili Zhang*, Huibin Wang, Chenming Li, Qing Ye, Yehong Shao, ``Unsupervised Anomaly Detection Algorithm of Graph Data Based on Graph Kernel '', 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing

[3] A Survey on Different Graph Based Anomaly Detection Techniques, Debajit Sensarma, and Samar Sen Sarma, Indian Journal of Science and Technology, Vol 8(31), November 2015

[4] Leman Akoglu, Hanghang Tong and Danai Koutra, ``Graph-based Anomaly Detection and Description: {A} Survey, CoRR, abs/1404.4679, 2014

[5] GLAD: Group Anomaly Detection in Social Media Analysis, Rose Yu, Xinran He, and Yan Liu

[6] Behdad, Mohammad, Luigi Barone, Mohammed Bennamoun, and Tim French. "Nature-inspired techniques in the context of fraud detection." IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 42, no. 6 (2012): 1273-1290.

[7] Alpaydn, G. An Adaptive Deep Neural Network for Detection, Recognition of Objects with Long Range Auto Surveillance.

[8] Yang, J., Zhou, C., Yang, S., Xu, H., \& Hu, B. (2018). Anomaly detection based on zone partition for security protection of industrial cyber-physical systems. IEEE Transactions on Industrial Electronics, 65(5), 4257-4267.

[9] Karami, A. (2018). An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities. Expert Systems with Applications, 108, 36-60.

[10] Kodama, T., Kamata, K., Fujiwara, K., Kano, M., Yamakawa, T., Yuki, I., \& Murayama, Y. (2018). Ischemic stroke detection by analyzing heart rate variability in rat middle cerebral artery occlusion model. IEEE Transactions on Neural Systems and Rehabilitation Engineering.

[11] Ahmed, Mohiuddin, Abdun Naser Mahmood, and Jiankun Hu. "A survey of network anomaly detection techniques." Journal of Network and Computer Applications 60 (2016): 19-31.

[12] KUMAR, RAVINDER, et al. "NHAD: Neuro-Fuzzy Based Horizontal Anomaly Detection In Online Social Networks." IEEE Transactions on Knowledge and Data Engineering (2018).

[13] Kim, Tae-Young, and Sung-Bae Cho. "Web traffic anomaly detection using C-LSTM neural networks." Expert Systems with Applications 106 (2018): 66-76.

[14] AlaM, A. Z., Faris, H., \& Hassonah, M. A. (2018). Evolving Support Vector Machines using Whale Optimization Algorithm for spam profiles detection on online social networks in different lingual contexts. Knowledge-Based Systems, 153, 91-104.

[15] Liu, Siyuan, Qiang Qu, and Shuhui Wang. "Heterogeneous anomaly detection in social diffusion with discriminative feature discovery." Information Sciences 439 (2018): 1-18.

[16] Prado-Romero, M. A., Oliva, A. F., & Hernández, L. G. (2018, September). Identifying Twitter Users Influence and Open Mindedness Using Anomaly Detection. In International Workshop on Artificial Intelligence and Pattern Recognition(pp. 166-173). Springer, Cham.

[17] Ramalingam, D., &Chinnaiah, V. (2018). Fake profile detection techniques in large-scale online social networks: A comprehensive review. Computers & Electrical Engineering, 65, 165-177.

[18] Al-Qurishi, M., Hossain, M. S., Alrubaian, M., Rahman, S. M. M., &Alamri, A. (2018). Leveraging Analysis of User Behavior to Identify Malicious Activities in Large-Scale Social Networks. IEEE Transactions on Industrial Informatics, 14(2), 799-813.

[19] Scarselli, F., Tsoi, A. C., Gori, M., & Hagenbuchner, M. (2005). A new neural network model for graph processing. Department of Information Engineering, University of Siena, Tech. Rep, 502, 01-05.

[20] Li, Y., Tarlow, D., Brockschmidt, M., & Zemel, R. (2015). Gated graph sequence neural networks. arXiv preprint arXiv:1511.05493.

[21] Monti, F., Boscaini, D., Masci, J., Rodola, E., Svoboda, J., & Bronstein, M. M. (2017, July). Geometric deep learning on graphs and manifolds using mixture model CNNs. In Proc. CVPR (Vol. 1, No. 2, p. 3).

[22] Radford, B. J., Apolonio, L. M., Trias, A. J., & Simpson, J. A. (2018). Network Traffic Anomaly Detection Using Recurrent Neural Networks. arXiv preprint arXiv:1803.10769.

[23] Aggrawal, N., & Arora, A. (2016, October). Visualization, analysis and structural pattern infusion of DBLP co-authorship network using Gephi. In Next Generation Computing Technologies (NGCT), 2016 2nd International Conference on(pp. 494-500). IEEE.

[24] Aggrawal, N., & Arora, A. (2016). Vulnerabilities issues and melioration plans for online social network over Web 2.0. Commun. Dependability Qual. Manag. Int. J, 19(1), 66-73.

[25] Miller, Zachary, et al. "Twitter spammer detection using data stream clustering." Information Sciences 260 (2014): 64-73.

[26] Ranshous, Stephen, et al. "Anomaly detection in dynamic networks: a survey." Wiley Interdisciplinary Reviews: Computational Statistics 7.3 (2015): 223-247.G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April,1955.