Anomalous node detection in attributed social networks using dual variational autoencoder with generative adversarial networks

Wasim Khan, Shafiqul Abidin, Mohammad Arif, Mohammad Ishrat, Mohd Haleem, Anwar Ahamed Shaikh, Nafees Akhtar Farooqui, Syed Mohd Faisal

PII: S2666-7649(23)00048-6

DOI: https://doi.org/10.1016/j.dsm.2023.10.005

Reference: DSM 77

To appear in: *Data Science and Management*

Received Date: 29 April 2023

Revised Date: 19 October 2023

Accepted Date: 22 October 2023

Please cite this article as: Khan, W., Abidin, S., Arif, M., Ishrat, M., Haleem, M., Shaikh, A.A., Farooqui, N.A., Faisal, S.M., Anomalous node detection in attributed social networks using dual variational autoencoder with generative adversarial networks, *Data Science and Management* (2023), doi: https://doi.org/10.1016/j.dsm.2023.10.005.

KeAi
CHINESE ROOTS
GLOBAL IMPACT

Contents lists available at ScienceDirect

Data Science and Management

journal homepage: www.keaipublishing.com/en/journals/data-science-and-management

Anomalous node detection in attributed social networks using dual variational autoencoder with generative adversarial networks

Wasim Khan [a*], Shafiqul Abidin [b], Mohammad Arif [c], Mohammad Ishrat [a], Mohd Haleem [d], Anwar Ahamed Shaikh [a], Nafees Akhtar Farooqui [a], Syed Mohd Faisal [e]

[a] Koneru Lakshmaiah Education Foundation Vaddeswaram, AP, India
b Aligarh Muslim University, Aligarh, India
c Vellore Institute of Technology, Vellore, India
d Era University, Lucknow, India
e Sandip Foundation, Nashik

ARTICLE INFO

Keywords:

Anomaly detection
Deep learning
Attributed networks
Autoencoder
Dual variational-autoencoder
Generative adversarial networks

ABSTRACT

Many types of real-world information systems, including social media and e-commerce platforms, can be modelled by means of attribute-rich, connected networks. The goal of anomaly detection in artificial intelligence is to identify illustrations that deviate significantly from the main distribution of data or that differ from known cases. Anomalous nodes in node-attributed networks can be identified with greater precision if both graph and node attributes are taken into account. Almost all of the studies in this area focus on supervised techniques for spotting outliers. While supervised algorithms for anomaly detection work well in theory, they cannot be applied to real-world applications owing to a lack of labelled data. Considering the possible data distribution, our model employs a dual variational autoencoder (VAE), while a generative adversarial network (GAN) assures the model is robust to adversarial training. The dual VAEs are used in another capacity: as a fake-node generator. Adversarial training is used to ensure that our latent codes have a Gaussian or uniform distribution. To provide a fair presentation of the graph, the discriminator instructs the generator to generate latent variables with distributions that are more consistent with the actual distribution of the data. Once the model has been learned, the discriminator is used for anomaly detection via reconstruction loss it has been trained to distinguish between the normal and artificial distributions of data. First, using a dual VAE, our model simultaneously captures cross-modality interactions between topological structure and node characteristics and overcomes the problem of unlabeled anomalies, allowing us to better understand the network sparsity and nonlinearity. Second, the proposed model considers the regularization of the latent codes while solving the issue of unregularized embedding techniques that can quickly lead to unsatisfactory representation. Finally, we use the discriminator reconstruction loss for anomaly detection as the discriminator is well-trained to separate the normal and generated data distributions because reconstruction-based loss does not include the adversarial component. Experiments conducted on attributed networks demonstrate the effectiveness of the proposed model and show that it greatly surpasses the previous methods. The area under the curve scores of our proposed model for the BlogCatalog, Flickr, and Enron datasets are 0.83680, 0.82020, and 0.71180, respectively, proving the effectiveness of the proposed model. The result of the proposed model on the Enron dataset is slightly worse than the other models; we attribute this to the dataset's low dimensionality as the most probable explanation.

1. Introduction

Anomaly detection often searches for anomalies to learn more about the underlying distribution of data. A typical attributed network has a wealth of information, such as user features and connections between users (Khan and Haroon, 2022a). Anomaly detection in attributed networks, is the process of locating nodes in a network that are significantly dissimilar from the rest, has recently attracted considerable interest owing to the growing prevalence of attributed data structures in practical applications like social networks, protein data analysis, and financial services (Khan, 2021; Koutra and Faloutsos, 2022; Kundra et al., 2022). Numerous applications have used the method, including the identification of social spammers (Hu et al., 2014), detection of financial fraud (Huang et al., 2018), and detection of intrusions (Chen et al., 2016; Khan et al., 2023).

Traditional machine learning algorithms like supervised anomaly detection approaches can only work with labelled data and typically only achieve satisfactory results when the data is well balanced (Khan and Haroon, 2022b). However, they are disproportionately affected by the issue of class imbalance. In recent years, researchers have developed a variety of methods to identify anomalies. As obtaining ground-truth anomalies is prohibitively expensive, many systems attempt to detect them unsupervised (Khan et al., 2022d). Unsupervised anomaly detection techniques often classify the least fit examples as outliers on the premise that the rest of the data is typical. Since the introduction of neural networks, various neural network-inspired techniques have been used to solve the anomaly detection problem (Rasool and Khan, 2015). In terms of performance, autoencoders contributed to the cutting edge of anomaly detection methods. The addition of variational inference to neural networks has made it possible to use probabilistic methods, like those used by variational autoencoders to perform anomaly detection tasks more systematically by relying on reconstruction probability instead of reconstruction error (Kingma and Welling, 2014).

Finding data anomalies is the primary focus of most anomaly detection challenges, which are solved by analyzing samples of normal data. Several anomaly detection methods routinely model data distribution and then report samples that are out of the ordinary as anomalies (Chalapathy and Chawla, 2019; Gupta et al., 2013). As an adaptable model for learning data distributions, Goodfellow et al. (2014) offer a new method for spotting anomalies using generative adversarial network (GAN). The GAN framework utilizes a min-max optimization framework to train a generator G and discriminator D. The generator's primary function is to generate representative examples that accurately reflect the distribution of the data, given a random input. Meanwhile, the discriminator learns to distinguish between genuine and fake samples. Numerous model learning tasks, such as those involved in recommender systems (Tang et al., 2019), query expansion (Lee et al., 2018), and network embedding (Wang et al., 2018), have benefited from the use of this approach. To spot anomalies, GAN-based techniques have demonstrated remarkable performance.

Typical anomaly detection methods are examples of non-regularized methods whose primary concern is either maintaining the connection between structures (probabilistic methods) or reducing the amount of error introduced by reconstruction (matrix factorization or deep learning methods).

data distribution. When coping with sparse and noisy graph data in the real world, unregularized embedding techniques can quickly lead to unsatisfactory representation because they find an identity mapping that has degenerated to the point where the latent code space is completely unstructured. Regularization of the latent codes, wherein they are forced to conform to a predetermined distribution of the underlying data, is a common solution to this issue (Makhzani et al., 2015). There have been recent advancements in learning robust latent representation using generative adversarial-based frameworks (Donahue et al., 2016; Dumoulin et al., 2017; Radford et al., 2015).

In this study, we suggest a technique, called the adversarial regularized dual graph VAE, to detect anomalies in social networks. Our proposed model is an unsupervised method for dealing with the issue of unknown anomalies in datasets. To solve the issues of data nonlinearity and network sparsity, dual VAEs are employed. Autoencoder-based methods cannot handle variation as their representations of latent variables are deterministic mappings; however, VAE, being a stochastic generative model, may provide calibrated probabilities for doing so. Apart from employing the dual VAE for embedding the structural information and attributes into a vector representation, these dual VAEs are also used as generators for creating fake nodes. We employ the adversarial training approach to guarantee that our latent codes follow a predetermined Gaussian or uniform distribution. To develop an accurate representation of the graph, the discriminator controls the generator while producing latent variables whose distributions are closer to the actual distribution of the data.

Effective anomaly detection has several significant contributions to the field of data science and management. Anomalies, also known as outliers or novelties, are data points that deviate significantly from the norm or expected patterns. Detecting anomalies is valuable across various domains and applications, such as Fraud detection, Cybersecurity, Healthcare, and Network Monitoring. Anomaly detection enhances decision-making by highlighting deviations from normal behavior or expected patterns. It contributes to early detection, reduced risks, improved operational efficiency, better resource allocation, and the ability to respond promptly to emerging issues. In the context of data science and management, anomaly detection is a powerful tool for gaining insights from data and ensuring the reliability, security, and optimization of various processes and systems. To be more precise, this study makes the following valuable contributions:

- For unsupervised learning, we used dual VAEs (Khan and Haroon, 2022c). The use of the dual VAEs improves the graph embedding learning performance, reduces the amount of error introduced into the graph structure reconstruction, and successfully models the non-linear nature of the network.
- The adversarial component we introduce to the dual variational graph autoencoder helps to regularize the encoding process by influencing the distribution of the encoded data. This part can distinguish between data obtained from the low-dimensional graph network representation and data obtained from the actual distribution of samples. To obtain an accurate representation of the graph, the discriminator motivates the encoder to produce low-dimensional variables with distributions that are closer to the true distribution of the data.
- After the model is learned, discriminator reconstruction loss is employed for anomaly detection as the discriminator is well-trained to separate the normal and generated data. This is because a discriminator can help an encoder develop a more accurate representation of a graph by encouraging it to produce low-dimensional variables whose distributions more closely match those of the data.

nizes both the dual VAE learning and the adversarial regularization learning in parallel.

2. Related work

Identifying anomalies is complex, and numerous methods have been developed to tackle this problem (Habeeb et al., 2019; Khan et al., 2015; Lavin and Ahmad, 2015; Naseer et al., 2018). Principal component analysis (PCA) is one classical unsupervised method developed in recent years (Shyu et al., 2003); it seeks a low-dimensional projection that accounts for most of the variance in the data. For this projection, the reconstruction error is the anomaly score. It is a method of linear algebra that can dynamically perform dimension reduction. Over-sampling PCA was proposed by Lee et al. (2012), and it uses online platforms to solve massive challenges. Their proposed technique helps identify the target instance's outlier by systematically sampling its underrepresented subgroup.

Autoencoder is one of the newest methods for dimensionality reduction and a widely used strategy for spotting outliers (Aggarwal, 2015). The encoder and decoder of an autoencoder work together to reassemble data samples and calculate an anomaly score based on the reconstruction error (Borghesi et al., 2019). The deep autoencoder proposed by Zhou and Paffenroth (2017) combines robust PCA with deep autoencoders. In doing so, it separates the data into two categories: the part that can be reconstructed by autoencoders and the noise (outliers). The deep autoencoder and Gaussian mixture model work together in the deep autoencoding Gaussian mixture model (DAGMM) to simulate the density distribution of data in several dimensions (Zong et al., 2018).

To reconstruct the topological structure and node properties, Ding et al. (2019) uses a graph convolution network (GCN) to compress the input network into low-dimensional embedding representations. Local representations of nodes are learned in spectral autoencoder for anomaly detection in attributed networks by employing a graph convolution encoder and decoder (Li et al., 2019).

The adversarial strategy of our method is based on GAN, wherein a generator and a discriminator engage in a minimax game to optimize each other (Goodfellow et al., 2020). GraphGAN (Wang et al., 2018) was the first to employ an adversarial strategy for graph learning. As an alternative to traditional network embedding algorithms, Hu et al. (2019) uses GAN as an additional regularization term to impose the distribution of the real data as a prior distribution on embedding vectors. To learn the latent embedding, Makhzani et al. (2015) introduced an adversarial autoencoder, which incorporates the adversarial process within the autoencoder. By contrast, this method works well with simple data and not graph data. Though several adversarial models have found success in computer vision, they are unable to deal with graph-structured data without some modification.

The remainder of this paper is organized as follows. Section 4, introduces the anomaly detection methodology that we have proposed. Section 5, compares and contrasts several assessment measures to demonstrate the practical efficacy of the proposed methods for detecting anomalies in real-world networks. Section 6 concludes the paper.

3. Proposed model

We propose a novel anomaly detection approach for attributed social networks utilizing the dual VAE and generative adversarial networks (GAN), where dual VAEs solve the problems of sparsity and nonlinearity while considering the embedding distribution, and GAN is used for adversarial training and finally calculating the anomaly scores of nodes. When combined with dual VAEs, GAN offers improved robustness against adversarial training. The model development workflow is depicted in Fig. 1

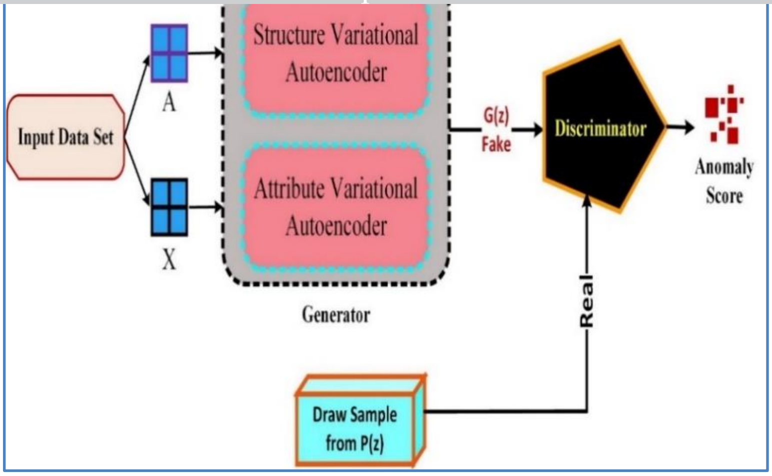

Fig. 1. Proposed dual VAE with GAN model.

3.1. Structure reconstruction

Our model initially transforms the node attribute X into a low-dimensional latent representation $\mathrm{Z^S}$ to acquire a large number of notable high-level node features. During encoding, we employ a two-layer GCN to generate the following parameters:

$$\mu = \mathrm{GCN}_{\mu}(\mathrm{X}, \mathrm{A}) \text{ and } \log \sigma = \mathrm{GCN}_{\sigma}(\mathrm{X}, \mathrm{A}) \qquad (1)$$

μ_n and σ_n are the mean and standard deviation vectors of embedding z_j. The GCN decoder for two layers is defined as:

$$\mathrm{Z^D} = \mathrm{f}_{linear}(\mathrm{Z^S}, \mathrm{A}|\mathrm{W}_s^{(1)}) \text{ and } \widehat{\mathrm{A}} = \mathrm{f}_{linear}(\mathrm{Z^D}, \mathrm{A}|\mathrm{W}_s^{(2)}) \qquad (2)$$

where $\mathrm{Z^S}$ represents the embedding of encoder and $\mathrm{Z^D}$ and $\widehat{\mathrm{A}}$ represent the first- and second-layer decoder outputs.

3.2. Attribute reconstruction

Using the two subsequent non-linear feature transform layers, the observable attribute data is transferred to the $\mathrm{Z^A}$.

$$\mathrm{Z^{A(1)}} = \mathrm{f}\,(\mathrm{X^T}\,\mathrm{W}_\mathrm{A}^{(1)} + \mathrm{b}^{(1)}), \text{ and } \mathrm{Z^A} = [\,\mu_\mathrm{A}, \sigma_\mathrm{A}\,] = \mathrm{Z^{A(1)}}\,\mathrm{W}_\mathrm{A}^{(2)} + \mathrm{b}^{(2)}) \quad (3)$$

Subsequently, the $\widehat{\mathrm{X}}$ is reconstructed using a simplistic inner product decoder, as shown below.

$$\widehat{\mathrm{X}} = Sigmoid(\,\mathrm{Z^S}\,(\mathrm{Z^A})^\mathrm{T}) \qquad (4)$$

Finally, an embedding $\mathrm{Z^F}$ is built by fusing the $\mathrm{Z^S}$ and $\mathrm{Z^A}$.

3.3. Adversarial training

A generating model, G, and a discriminative model, D, play a min-max adversarial game with each other within the GAN model. In contrast to the generative model, which generates data from scratch, the discriminator model, calculates the probability that a sample of the distribution we are seeking to model is present at some point x in the data space. In parallel, the generator makes use of $G(\mathbf{z})$ that transforms z-samples from the previous p(z) into the underlying data space. The goal of training for $G(\mathbf{z})$ is to fool the discriminator into assuming the data it creates are representative of the data distribution as much as possible. During training, the generator's parameters are adjusted based on information obtained from the gradient of $D(\mathrm{x})$ with respect to x. Consequently, the following expression may be used to provide the solution for this game:

$$\min_{G}\max_{D} \mathrm{E}_{\mathbf{x}\sim p_\mathrm{data}}[\log D(\mathbf{x})] + \mathrm{E}_{\mathbf{z}\sim p(\mathbf{z})}[\log(1 - D(G(\mathbf{z}))] \qquad (5)$$

Our proposed model comprises dual VAEs, which collectively act as generator, and a separate discriminator network. The generator $G(.)$ is designed as a dual VAE. A fake sample is generated by the embedding generated with the dual VAE architecture. Conversely, a discriminator $D(.)$ is trained to identify the difference between a real data sample and a fake one. Our model is predicated on the use of an adversarial training method to force the latent representation Z to follow a predetermined distribution. A standard multi-layer processing (MLP) network serves as the basis for the adversarial model, but its output layer is flat and uses a sigmoid function instead of a conventional linear one. As a discriminator, the adversarial model can distinguish between genuine and spoofed data.

3.4. Training objective

The following loss functions are offered to perform anomaly detection:

3.4.1. Adversarial loss

Data reconstruction quality is maximized by the adversarial loss function for the generator. According to Eq. (6) while training generator $G(.)$, this loss function will minimize the gap between x, the input data, and $G(x)$, the fake data produced by the generator, while $D(\,.\,)$, the discriminator, will maximize the difference between the real and fake data to distinguish them. Specifically, we want to maximize the adverse loss of discriminator $D(.)$ while minimizing the adverse loss of the generator $G(.)$. One possible expression for the adversarial loss is:

$$L_A = E_{x\sim p_x}[\,||D(x) - D(G(x))||_2] \qquad (6)$$

3.4.2. Dual variational autoencoder loss

The proposed method leverages a dual VAE loss to characterize the dissimilarity between x and $G(x)$, hence improving the generator $G(.)$ for data reconstruction. This loss is used to represent the L2 distance between real data, x, and fake data, $G(x)$. This step ensures that the fake data accurately reflects the real data. The equation for the generator's contextual loss is as follows:

$$L_G = [(1 - \theta)\,[\mathbb{E}_{q(\mathrm{Z^S}|\mathrm{X,A})}(\log p(\mathrm{A}|\mathrm{Z^S})] + \theta\,[\mathbb{E}_{q(\mathrm{Z^A}|\mathrm{X})}(\log p(\mathrm{X}|\mathrm{Z^S}, \mathrm{Z^A})]] - \mathrm{KL}[q(\mathrm{Z^S}|\mathrm{X}, \mathrm{A})\,||\,p(\mathrm{Z^S})] - \mathrm{KL}[q(\mathrm{Z^A}|\mathrm{X})\,||\,p(\mathrm{Z^A})] \qquad (7)$$

3.4.3. Contextual loss of discriminator

A contextual loss of discriminator is used during training to get to the optimum balance state as quickly as possible. The discriminator's output data $D(x)$ is compared with the input data x, and the L2 distance between the two is represented by this loss. This guarantees that the output data from the discriminator closely matches the input data. Discriminator contextual loss is represented as follows:

$$L_D = E_{x\sim p_x}[\,||x - D(x)||_2] \qquad (8)$$

A weighted sum of these three loss functions can be used to train the proposed model. The weighted summation loss function is defined as follows:

$$L = \emptyset_A L_A + \emptyset_G L_G + \emptyset_D L_D \qquad (9)$$

where, $\emptyset_A$, $\emptyset_G$, $\emptyset_D$ are the weights of three loss functions.

3.5. Anomaly detection using GAN

As the discriminator is trained to distinguish between the normal and created data distributions, we use the reconstruction error as the anomaly score. As the model converges, the discriminator will have developed distribution X. Typically, the discriminator would be able to recover the original data once it has passed through the generator. However, the discriminator would not successfully reconstruct anomalous inputs. Subsequently, the discriminator, which had concluded that the generator's inputs did not follow the normal data distribution, would amplify the reconstruction error. The formula for determining the anomalous score $\mathcal{A}(\hat{x})$ for a given input, $\hat{x}$ is as follows:

$$\mathcal{A}(\hat{x}) = ||\hat{x} - D(G(\hat{x})) \qquad (10)$$

We then define a threshold ϕ from which anomalies are determined. A test input $\hat{x}_i$ is considered to be anomalous if $(\hat{x}_i)>\phi$. After the training objective function has been optimized, our proposed method could be utilized to identify anomalies within attributed networks. Each node in our test data is then scored based on its degree of anomaly using the reconstruction error calculated with the help of discriminator loss.

Algorithm 1: Dual VAE with GAN for anomaly detection

Input: The node feature matrix X ∈ $\mathbb{R}^{N\times M}$ and the adjacency matrix A ∈ $\mathbb{R}^{N\times N}$, E=Number of Epochs, K= number of steps for iterating discriminator

Output: List of anomalous nodes.

```
s samples with normal behavior from n instances are chosen at
random and used as training samples.
for each epoch = 1 to E do
    Generate latent variables matrix $Z^F$;
    for n=1,2, …., K do
        Sample p entities {$z^{(1)}$, …., $z^{(p)}$} from latent matrix $Z^F$;
        Sample p entities {$a^{(1)}$, …., $a^{(p)}$} from the prior
        distribution;
        Update the adversarial model via Eq. (9):
            $L = \emptyset_A L_A + \emptyset_G L_G + \emptyset_D L_D$
    end for
end for
Calculate the normality score via Eq. (10);
Return the list of anomalous nodes;
End
```

4. Experiments and Discussion

The experimental setups are first presented here, detailing the datasets, baseline approaches, parameters, and metrics used for analysis. We then show experimental results on the anomaly detection task and compare them to state-of-the-art methods to gauge the efficacy of the suggested approach.

4.1. Experimental Design

In this study, we conduct experiments on three publicly available attributed social network datasets: BlogCatalog, Flickr, and Enron.

- BlogCatalog is a platform for bloggers to build a community through mutual following. The user and the blog are defined based on blogger characteristics, and the node attributes are made up of attribute data (Ding et al., 2019).
- Flickr is a photo-sharing platform similar to Instagram. By interacting with one another, people create a network that functions much like BlogCatalog. Node properties are defined by tags, which are chosen by the user and reflect their interests (Asperti and Trentin, 2020).
- Enron is a system for exchanging electronic mail in which "edges" represent the transmission of e-mails from one user to another (Metsis et al., 2006).

In this approach, we use the commonly-used assessment indicator, the area under the curve (AUC) score, alongside Precision and Recall, to assess the efficacy of several anomaly detection techniques.

- The Receiver operating characteristic (ROC) curve compares the detection system's true positive rate to its false positive rate in light of empirical data and the results of the detection process. The area under the curve (AUC) value indicates the probability that an abnormal node will be given a higher score than a typical node in a random sample. If the AUC value is near one, the method is of good quality.
- Precision is the proportion of true positives (positive samples proportion of positive samples that were identified.
- To determine the recall, we divide the number of positive samples that were correctly labelled as "positive" by the total number of positive samples. The proportion of positive samples correctly identified by a model is called its recall.

The proposed model was created in Python, and training was performed with 180 epochs throughout all datasets. For this, we employed Adam optimizer with a 0.001 percent learning rate. To maintain consistency across all datasets, we decided to keep the embedding dimension at 128.

4.2. Experimental results

The training set comprises normal examples. Test data, which comprises both normal and anomalous instances, is used to quantify the results. Several benchmarks are used to evaluate the proposed model's ROC-AUC performance. The ROC curve and loss curve for the BlogCatalog dataset are displayed in Fig. 2 and 3, respectively. The training loss on BlogCatalog flattens out between epochs 160 and 200 and then begins to rise again after epoch 200. However, the validation loss tends to stabilize around 180 epochs of training; thus, optimal performance is achieved around 180 epochs.

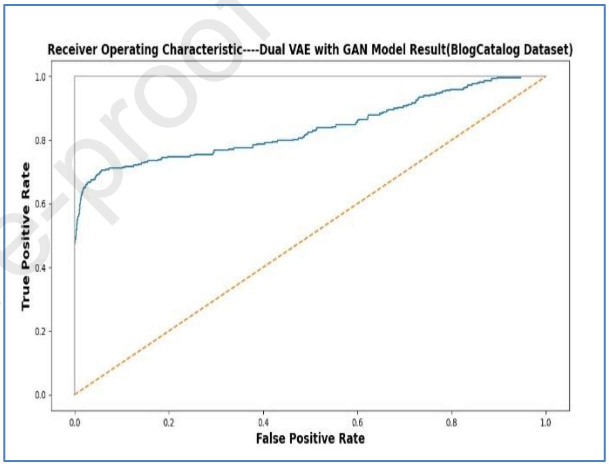

Fig. 2. ROC curve on BlogCatalog.

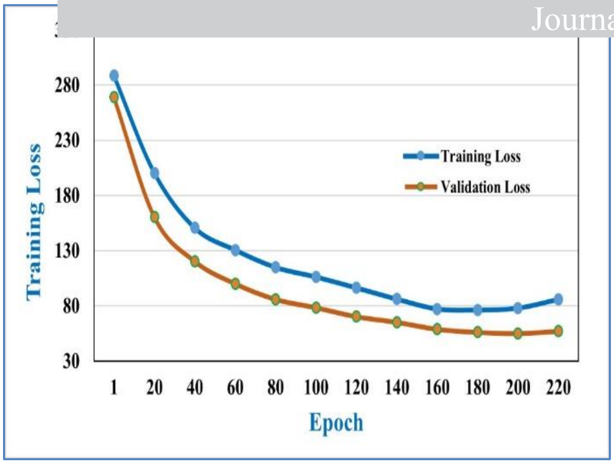

Fig. 3. Loss curve on BlogCatalog.

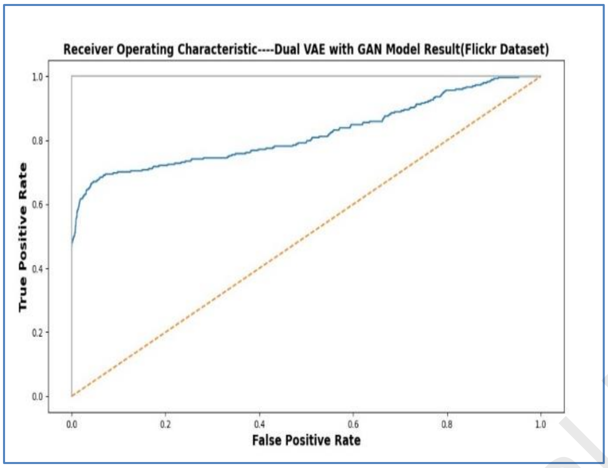

Fig. 4. ROC curve on Flickr.

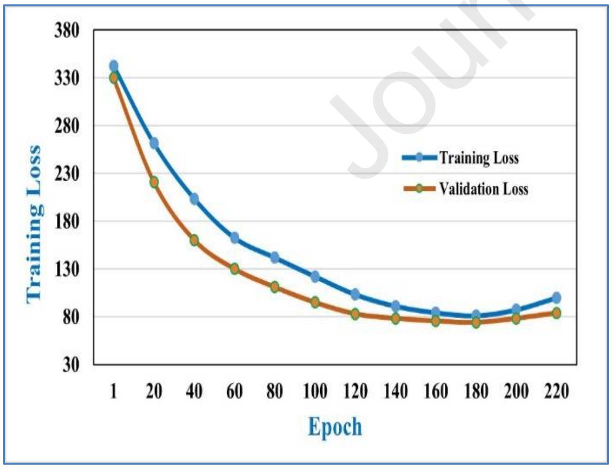

Fig. 5. Loss curve on Flickr.

Fig. 4 and 5, illustrate the ROC curve and the loss curve for the Flickr dataset, respectively. In the loss curve for the Flickr dataset, training loss keeps decreasing but then starts rising again around 180 epochs, and as validation loss also starts rising again after 180 epochs, we considered the results on 180 epochs as well. Additionally, optimal performance on the Enron dataset's loss curve was observed at roughly 180 epochs. Fig. 6 and 7, present the ROC curve and the loss curve for the Enron dataset, respectively.

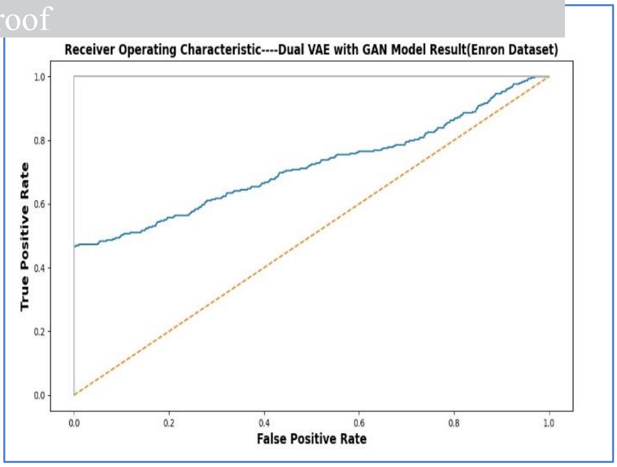

Fig. 6. ROC curve on Enron.

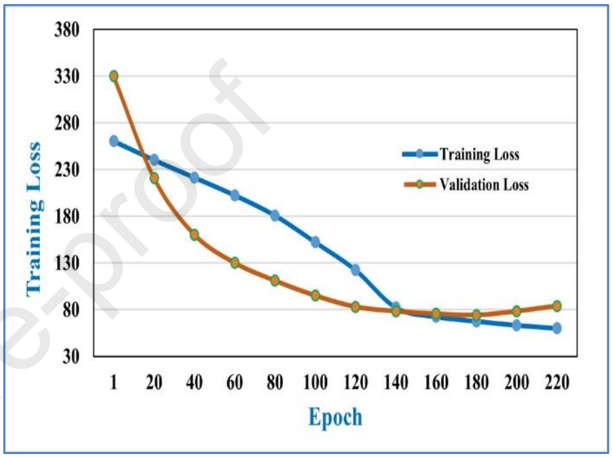

Fig. 7. Loss curve on Enron.

4.3. Comparison with baselines

Several benchmarks are used to evaluate the proposed model's ROC-AUC performance. The results of the different methods in terms of AUC, precision, and recall for each dataset are displayed in Tables 1, 2, and 3, respectively.

Table 1: Proposed model AUC comparative result.

Method	BlogCatalog	Flickr	Enron
ADAE	0.80370	0.78380	**0.71940**
EGAN	0.81830	0.81640	0.69450
Proposed	**0.83680**	**0.82020**	0.71180

Table 2: Proposed model precision comparative result.

Method	BlogCatalog	Flickr	Enron
ADAE	0.85350	0.81540	0.66540
EGAN	0.80950	0.79550	0.72540
Proposed	**0.89340**	**0.84180**	**0.75230**

Table 3: Proposed model recall comparative result.

Method	BlogCatalog	Flickr	Enron
ADAE	0.89530	0.85250	**0.79250**
EGAN	0.79550	0.82530	0.76240
Proposed	**0.93500**	**0.86950**	0.77250

The R Enron datasets are depicted in Fig. 8, 9, and 10, respectively. Our proposed model has a larger area under the receiver operating characteristic curve than other well-known anomaly detection algorithms. On the BlogCatalog dataset, AUC is enhanced by 1.85% compared to EGAN and 3.31% compared with the ADAE technique. Similarly, the AUC on the Flickr dataset is higher than that of EGAN (by 0.38%) and the ADAE (by 3.64%); however, the AUC on the Enron dataset was lower than others.

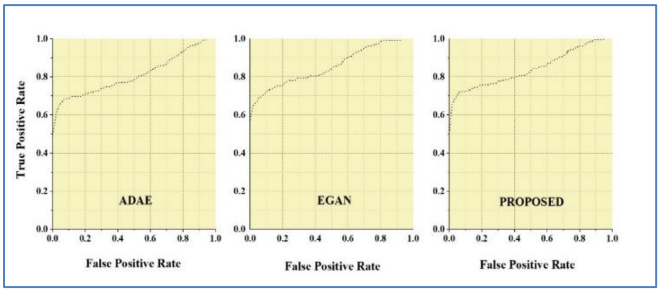

Fig. 8. Proposed model-ROC curve comparison on BlogCatalog with baselines.

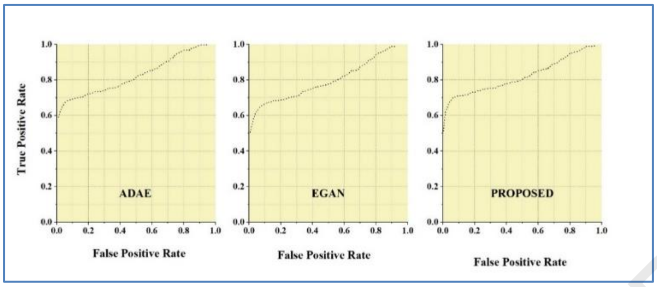

Fig. 9. Proposed model-ROC curve comparison on Flickr with baselines.

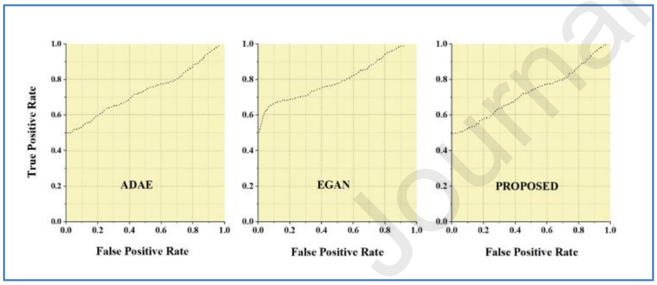

Fig. 10. Proposed model-ROC curve comparison on Enron with baselines.

Fig. 11 displays the results of a comparison of AUC. Precision and recall performance comparisons are displayed in Fig. 12 and 13. Compared with the ADAE and EGAN on the BlogCatalog dataset, the proposed model improves precision by at least 3.99% and over 8.4%, respectively. The BlogCatalog dataset shows similar improvements in recall, with a 3.97% increase relative to the ADAE and a 13.95% increase compared with the EGAN.

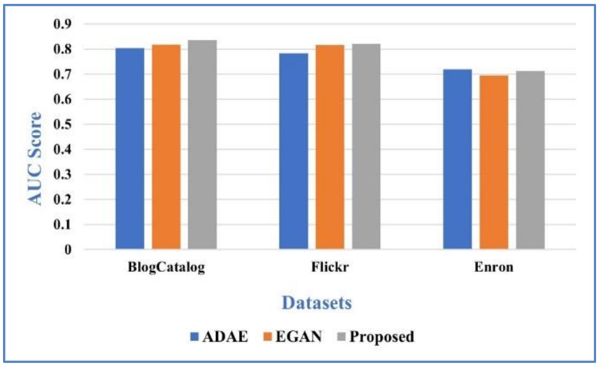

Fig. 11. AUC score comparison.

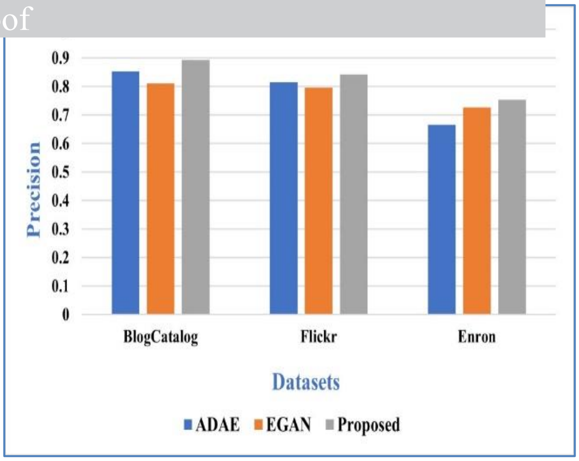

Fig. 12. Precision comparison.

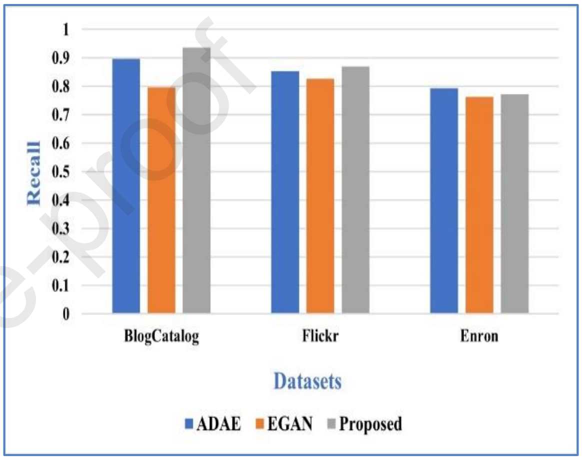

Fig 13. Recall comparison.

4.4. Result analysis

Analyzing the results presented in the previous section, in the context of theoretical and applied aspects, while also dialoguing with existing literature, helps highlight the strengths of our work compared with past research.

4.4.1. Theoretical aspect

- Our proposed model has discriminative power in spotting abnormalities inside attribute-rich, connected networks, as evidenced by its higher AUC values acquired on the BlogCatalog and Flickr datasets. The theoretical underpinnings of anomaly identification are consistent with these findings, as they emphasize the importance of training the model to better identify outliers.
- Our model is theoretically novel as it combines a GAN with a pair of VAEs. The importance of representing both topological structure and node properties in real-world networks highlights the theoretical merits of this combined approach. This is a significant improvement as it broadens the theoretical arsenal for detecting anomalies in complex data sets.
- The disparity in Enron dataset AUC performance highlights the significance of understanding context. This theoretical understanding emphasizes the need for anomaly detection algorithms that can be tailored to the unique features and data distributions of the study field. All of this fits neatly into the theoretical framework of “context-aware modeling.”

4.4.2 Applied aspect

- With a higher AUC, our model is promising for practical usage in scenarios including fraud detection, recommendation systems, and network security. The proposed methodology can be implemented by businesses to better their security and decision-making procedures.
- Decision-makers and practitioners can use our study as a reference point. Our findings can serve as a benchmark against which other anomaly detection models can be evaluated and improved. This is of

cons detection of anomalies are paramount, such as the financial and healthcare sectors.

4.4.3 Comparison with state-of-the-art

- By combining dual VAEs and GANs, our study overcomes the shortcomings of previous approaches. Our method potentially improves upon prior research in the field of anomaly detection, which may have focused on unimodal methods or lacked the flexibility shown in the proposed model.
- Results are put into perspective, especially the lower AUC on the Enron dataset, demonstrating a nuanced grasp of anomaly detection. In contrast to some earlier studies, which may have presented results without considering context, this is a significant change. Our study demonstrates a dedication to practical relevance.

4.4.4 Management implications

Based on the results and findings presented in the manuscript, there are several important discussions and implications for management practice in the context of data science:

- This study tackles the problem of detecting anomalies in practical applications, such as online marketplaces and social media networks. This has serious repercussions for companies and groups active in these fields. The proposed model is an example of an advanced anomaly detection technique that management teams can use to detect and prevent fraudulent actions on their platforms. Increased safety, better user experience, and protection of corporate interests are all possible outcomes.
- As observed in the Enron dataset, dataset dimensionality can affect model performance, highlighting the need for context-specific investigation. Management must understand that not all datasets are the same and that the data and model they choose must fit the unique characteristics of the problem at hand. This highlights the significance of flexibility in data science projects.
- Adversarial training can be used to strengthen models in important ways. The administration needs to understand the value of dependable and secure data-driven apps. Adversarial training, or a method very similar to it, can be used to protect systems from adversarial attacks and guarantee their consistent performance in the real world.
- The relevance of regularizing latent codes in the model is emphasized. This idea can be implemented in management theory and practice by emphasizing the value of high-quality, consistent data. The suboptimal representations that may result from using unregularized embedding techniques can be avoided by ensuring that data sources are well-structured and cleansed. Data quality can be managed by allocating resources and implementing processes.

In conclusion, there are several directions in which the management practices of data scientists could make use of the results of this study. They emphasize the need for reliable anomaly detection, high-quality data, and flexibility when dealing with complex real-world data problems. By considering these observations, businesses may boost their data-driven decision-making processes, tighten up their security, and get more use out of their data assets.

4.5. Parameter sensitivity

The sensitivity of the balance parameter and various embedding dimensions to an anomaly is examined in this section. The BlogCatalog dataset was used to conduct the analysis. The typical AUC trend for various embedding layer sizes is shown in Fig. 14. We find that higher-dimensional embeddings perform better because they may encode more information. However, if the dimension's value is either too low or too high, overfitting occurs, performance worsens, and the modelling capacity is compromised. It is obvious that there are substantial relationships between the node attributes of the attributed network and the network's structure as the efficiency for anomaly detection would be low if only attribute or structure reconstruction were considered. The AUC trend for various θ values is shown in Fig. 15, demonstrating how a strong balance factor can considerably improve efficiency.

5. Conclusion

This study aimed to offer a unique adversarial model for detecting anomalies in social networks. The majority of currently available graph embedding techniques are unregularized approaches that fail to account for the data distributions of the latent representation, resulting in subpar

codes are consistent with a given prior distribution, we presented an adversarial training technique. The adversarial module is jointly learned with dual VAEs to create a robust representation.

First, the dual VAEs are used to better capture the highly non-linear network structure, enhance the graph embedding learning performance, and reduce reconstruction errors of the graph's underlying structure. Subsequently, we add an adversarial component to the dual variational graph autoencoder to regularize the distribution of the encoded data. This segment can distinguish between input from the low-dimensional graph network representation and the actual distribution of data. The discriminator motivates these dual encoders to learn an efficient representation of the graph by producing low-dimensional variables with distributions that are more similar to the true distribution of the data. As the discriminator has been well-trained to distinguish between the normal and generated distributions of data, it may be used for anomaly detection through the discriminator's reconstruction loss.

The proposed method was evaluated on three different datasets: BlogCatalog, Flickr, and Enron. The experimental findings prove the viability of the proposed model in comparison to the standard approaches. Experiment results demonstrated that GAN models can be used to achieve state-of-the-art performance for anomaly detection on high-dimensional, complex datasets. In future studies, we also hope to perform a deeper analysis of low-dimension datasets and aspire to offer a much more comprehensive analysis of our adversarial approach and its effectiveness in real-world settings.

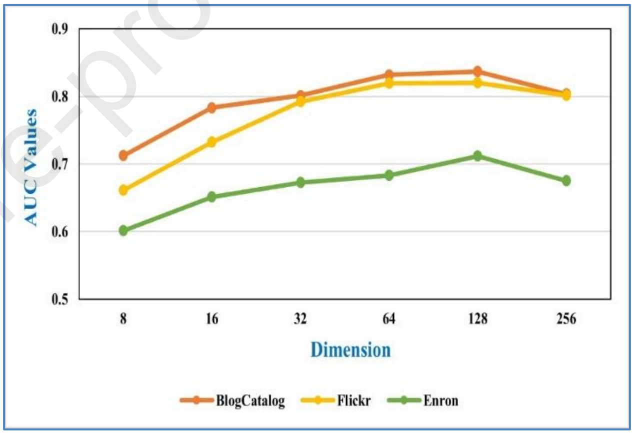

Fig. 14. Embedding dimension effect.

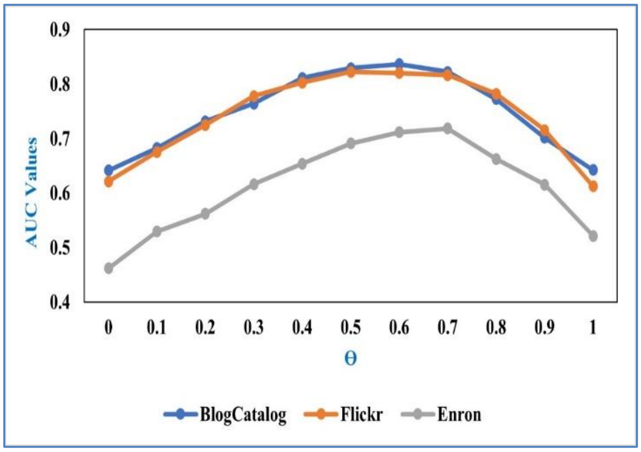

Fig. 15. Balance parameter effect.

Availability of data and materials

The data supporting the findings of the article is available within the article.

Conflict of interest

The author declares no conflict of interest, financial or otherwise.

References

Aggarwal, C.C., 2015. Data mining: the textbook. Springer.

Asperti, A., Trentin, M., 2020. Balancing reconstruction error and kullback-leibler divergence in variational autoencoders. IEEE Acc. 8, 199440-199448.

Borghesi, A., Bartolini, A., Lombardi, M., et al., 2019. Anomaly detection using autoencoders in high performance computing systems. In: 2019 AAAI Conference on Artificial Intelligence. ACM, pp. 9428–9433.

Chalapathy, R., Chawla, S., 2019. Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407. Jan 10.

Chen, P., Choudhury, S., Hero, A., 2016. Multi-centrality graph spectral decompositions and their application to cyber intrusion detection. In: 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, pp. 4553–4557.

Ding, K., Li, J., Bhanushali, R., 2019. Deep anomaly detection on attributed networks. In: 2019 SIAM International Conference on Data Mining. SIAM, pp. 594–602.

Donahue, J., Krähenbühl, P., Darrell, T., 2016. Adversarial feature learning. arXiv preprint arXiv:1605.09782. May 31.

Dumoulin, V., Belghazi, I., Poole, B., et al., 2017. Adversarial learned inference. arXiv preprint arXiv:1606.00704. Jun 2.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., et al., 2020. Generative adversarial networks. Commun ACM. 63(11), 139–144.

Gupta, M., Gao, J., Aggarwal, C., et al., 2013. Outlier detection for temporal data: A survey. IEEE Trans. Knowl. Data. Eng. 26(9), 2250–2267.

Habeeb, R.A.A., Nasaruddin, F., Gani, A., et al., 2019. Real-time big data processing for anomaly detection: A survey. Int J. Inf. Manag. 45(C), 289–307.

Hu, B., Fang, Y., Shi, C., 2019. Adversarial learning on heterogeneous information networks. In: 2019 International Conference on Knowledge Discovery & Data Mining. ACM, pp. 120–129.

Hu, X., Tang, J., Liu, H., 2014. Online social spammer detection. In: 2014 AAAI Conference on Artificial Intelligence, AAAI, Vol. 28(1).

Huang, D., Mu, D., Yang, L., et al., 2018. CoDetect: Financial fraud detection with anomaly feature detection. IEEE Acc, 6, 19161–19174.

Khan, W., 2021. An exhaustive review on state-of-the-art techniques for anomaly detection on attributed networks. Turkish J. Comp. Math. Ed (TURCOMAT), 12(10), 6707–6722.

Khan, W., Ansari, H., Shaikh, A.A., 2015. Log Files Utility for Software Maintenance. Int J. Adv. Res. Comp. Eng. Tech (IJARCET), 4(19), 3714-3718.

Khan, W., Haroon, M., 2022a. A Pilot Study and Survey on Methods for Anomaly Detection in Online Social Networks. In: 2022 Human-Centric Smart Computing: Proceedings of ICHCSC 2022. Springer, pp. 119–128.

Khan, W., Haroon, M., 2022b. An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks. Int J. Cogn. Comp. Eng, 3, 153–160.

Khan, W., Haroon, M., 2022c. An efficient framework for anomaly detection in attributed social networks. Int J. Info. Tech, 14(6), 3069-3076.

Khan, W., Haroon, M., Khan, A.N., et al., 2022d. DVAEGMM: Dual Variational Autoencoder with Gaussian Mixture Model for Anomaly Detection on Attributed Networks. IEEE Acc, 10, 91160–91176.

Khan, W., Ishrat, M., Haleem, M., et al., 2023. An Extensive Study and Review on Dark Web Threats and Detection Techniques. In: 2023 Advances in Cyberology and the Advent of the Next-Gen Information Revolution. IGI Global, pp. 202–219.

Kingma, D.P., Welling, M., 2014. Auto-encoding variational bayes. In: 2014 2nd International Conference on Learning Representations, ICLR, pp. 1–14.

Koutra, D., Faloutsos, C., 2022. Individual and collective graph mining: principles, algorithms, and applications. Springer Nature, Jun 1.

Kundra, H., Khan, W., Malik, M., et al., 2022. Quantum-inspired firefly algorithm integrated with cuckoo search for optimal path planning. Int J. Mod. Ph. C, 33(2), 2250018.

Lavin, A., Ahmad, S., 2015. Evaluating real-time anomaly detection algorithms--the Numenta anomaly benchmark. In: 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA). IEEE, pp. 38–44.

Lee, M. C., Gao, B., Zhang, R., 2018. Rare query expansion through generative adversarial networks in search advertising. In: 2018 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. ACM, pp. 500–508.

Lee, Y. J., Yeh, Y. R., Wang, Y.C.F., 2012. Anomaly detection via online oversampling principal component analysis. IEEE Trans. Knowl. Data. Eng, 25(7), 1460–1470.

Li, Y., Huang, X., Li, J., et al., 2019. SPECAE: Spectral autoencoder for anomaly detection in attributed networks. In: 2019 28th ACM International Conference on Information and Knowledge Management. ACM, pp. 2233–2236.

Makhzani, A., Shlens, J., Jaitly, N., et al., 2015. Adversarial autoencoders. arXiv

Metsis, V., Androutsopoulos, I., Paliouras, G., 2006. Spam filtering with naive bayes-which naive bayes?. In: 2006 Third Conference on Email and Anti-Spam (CEAS). Mountain View, CA, pp. 28–69.

Naseer, S., Saleem, Y., Khalid, S., et al., 2018. Enhanced network anomaly detection based on deep neural networks. IEEE acc, 6, 48231–48246.

Radford, A., Metz, L., Chintala, S., 2015. Unsupervised representation learning with deep convolutional generative adversarial networks. arXiv preprint arXiv:1511.06434.

Rasool, M., Khan, W., 2015. Big data: Study in structured and unstructured data. HCTL Open Int. J Tech. Inno. Res (IJTIR), 14, 1–6.

Shyu, M., Chen, S., Sarinnapakorn, K., et al., 2003. A novel anomaly detection scheme based on principal component classifier. In: 2003 IEEE foundations and new directions of data mining workshop. IEEE pp. 172-179.

Tang, J., Du, X., He, X., et al., 2019. Adversarial training towards robust multimedia recommender system. IEEE Trans. Knowl. Data. Eng, 32, 855–867.

Wang, H., Zhao, M., Zhang, W., et al., 2018. GRAPHGAN: Graph representation learning with generative adversarial nets. In: 2018 AAAI conference on artificial intelligence. AAAI, Vol. 32(1).

Zhou, C., Paffenroth, R., 2017. Anomaly detection with robust deep autoencoders. In: 2017 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, pp. 665–674.

Zong, B., Song, Q., Min, M., et al., 2018. Deep autoencoding gaussian mixture model for unsupervised anomaly detection. In: 2018 6th International Conference on Learning Representations.

Anomalous Node Detection in Attributed Social Networks using Dual Variational Autoencoder with Generative Adversarial Networks.

Author declaration

No conflict of interest exists.

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

No funding was received for this work.