Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3766810, 17 pages
https://doi.org/10.1155/2022/3766810

Research Article

Abnormal User Detection via Multiview Graph Clustering in the Mobile e-Commerce Network

HangYuan Du,[1] **Duo Li**,[1] **and WenJian Wang**[1,2]

[1]*School of Computer and Information Technology, Shanxi University, Taiyuan 030006, China*
[2]*Key Laboratory of Computational Intelligence and Chinese Information Processing (Shanxi University), Ministry of Education, Taiyuan 030006, China*

Correspondence should be addressed to HangYuan Du; duhangyuan@sxu.edu.cn

Received 17 May 2022; Accepted 23 July 2022; Published 9 August 2022

Academic Editor: Barbara Guidi

In recent years, Internet of Things has not only promoted the continuous development of e-commerce transaction but also brought loop-hole to the fraud gangs who always utilize mobile devices to commit fraud crimes. For example, fraud gangs are usually organized to purchase commodities at low prices in e-commerce promotions. They benefit from the price spread by reselling commodities at high prices. In the past few years, the transaction fraud caused serious financial losses to merchants in e-commerce platform. To detect the fraudulent user and behavior effectively, a multiview graph clustering-based abnormal detection model is developed in this paper. In the proposed model, two fraudulent behavior patterns are proposed by abstracting the e-commerce network as a heterogeneous information graph. On this basis, two user-similarity graphs are reorganized from the heterogeneous graph with the help of different metapaths. Subsequently, in order to capture the corresponding fraudulent behavior patterns, the above two graphs are encoded into user embeddings and assigned to specific clusters in respective views. Finally, the consensus detection result is produced by fusing the complementary information of different views in a joint multiview learning framework. As we know, our work is the first one that uses multiview graph clustering in e-commerce fraud detection, which will provide a new research perspective for fraud detection in e-commerce platform. Extensive experiments are conducted on real and semisynthetic datasets, and the results demonstrate the effectiveness and superiority of the proposed model.

1. Introduction

The rapid development of Internet of Things (IoT) has brought much convenience for our life over the past years. The IoT is constructed on the basis of multiple sensor networks, and its essence is to realize the information interaction between users and various devices or terminals. The development of mobile communication, sensor technology, and computer networks greatly enriched the contents covered by IoT, especially the mobile e-commerce. By means of mobile terminals, such as phones and tablet computers, people can realize online shopping or transactions anytime and anywhere.

With the promotion of IoT, the transaction size of the mobile e-commerce is increasing continuously, as well as the number of online users. Many merchants in the e-commerce platform always initiate sales promotions to attract and get more customers. In order to gain illegal benefits, fraud gangs always manipulate a large number of mobile devices to register new users, and they frequently purchase promotional commodities at zero or low cost. Then, they earn profit by reselling promotional commodities at high prices in the second-hand market. This fraudulent behavior will cause a considerable marketing loss for the merchants in the e-commerce platform and may damage the market order of the e-commerce platform seriously. To address the problem in the above fraudulent scene, it is particularly urgent to design effective antifraud strategies and technologies. As an important data mining technique, anomaly detection has been successfully applied in various fields [1, 2]; it

also reveals enormous potential in the e-commerce fraud recognition.

The anomaly detection methods used in e-commerce fraud recognition can be divided into three categories: rule-based strategy, machine learning-based strategy, and graph-based strategy. The rule-based strategy performs anomaly detection by generating inference rule from experts' experiences, in which some indicators or indexes are designed to evaluate fraudulent behaviors [3]. However, abnormal users always evade the detection rules by implementing some technical measures such as GSM sniffer and IP obfuscation, which makes it harder for rule-based methods to detect fraudulent behaviors [4]. Compared with rule-based methods, machine learning-based methods show stronger performance and better adaptability in many complex tasks [3]. Meanwhile, they have to face several challenges in some applications. Firstly, most machine learning algorithms can only deal with the input in terms of vector. However, e-commerce data always includes many complex information, such as timestamps, geographic locations, and evaluations, which cannot be represented by vector efficiently. Secondly, the sizes of e-commerce data are usually very large; as a result, the performance degradation will appear in the machine learning-based models. Thirdly, abnormal users usually maliciously imitate normal transaction behaviors to hide their identities. This indistinct pattern of fraudulent behavior is difficult to be recognized automatically by the detection model. Subsequently, researchers find that in spite of hiding their identities, abnormal users would inevitably leave some traces about fraudulent behavior in the network of interactions. Based on this idea, some studies model the e-commerce users and their interactive relationships by graph structure and propose a series of graph-based detection methods. In these models, many graph data mining algorithms are employed to identify fraudulent user by recognizing abnormal nodes, edges, or subgraphs whose distributions or patterns are different from others [5]. To address the data representation problem in the graph model, deep learning methods are introduced into graph-based e-commerce fraud detection recently due to their powerful representation ability [4, 6, 7]. All above methods assume that the abnormal user or behavior always implies a certain pattern or regularity. However, with the constantly evolution of technical means in e-commerce fraud, the intrinsic patterns implied in fraudulent behaviors are becoming diversified and increasingly difficult to be recognized.

Multiview learning methods provide an effective means of describing and recognition abnormal pattern from different perspectives. In this paper, we propose a multiview clustering-based abnormal user detection model for mobile e-commerce network, namely, Deep Multiview Clustering Detection Model (DM-VCDM), in order to comprehensively capture intrinsic patterns for abnormal user or behavior in the fraud scene. By organizing the records of user behavior in an interaction-constraint graph, the proposed model utilizes two metapaths to seek the behavioral patterns and interaction regularity of abnormal users from different perspectives. Within a joint learning framework, complementary and consensus information from these perspectives can be effectively combined to improve the detection ability of the model. To sum up, the main contributions of our work are as follows:

(1) Two important behavior patterns are developed for depicting abnormal users in e-commerce fraud, i.e., device aggregation and consumption aggregation. These two patterns can effectively assist the model to identify the interaction trace of abnormal user

(2) A multiview clustering-based abnormal user detection model is proposed, in which the behavior patterns in different views are encoded and fused in a dual encoder-decoder framework. The complementary and consensus information between multiple views can be integrated with the help of a multiview auxiliary target distribution, in the clustering process. In the proposed model, the anomaly detection result is generated by predicting the cluster assignment with the multiview fusion mechanism

(3) Extensive experiments on several real and semisynthetic datasets demonstrate the validity and superiority of our DM-VCDM model, in comparison with several traditional anomaly detection methods, convolutional autoencoder-based detection models, and deep graph anomaly detection algorithms

The rest of this paper are organized as follows. Section 2 introduces several related works. Section 3 illustrates details of the proposed model. In Section 4, the proposed model is compared with several reference algorithms in the experiments. Finally, conclusion of this work and future plan are given in Section 5.

2. Related Work

In this section, some important contents that provide foundation for the construction of our framework are introduced. Firstly, we review the recent studies about pattern recognition and graph anomaly detection. Subsequently, we introduce the concepts and applications of heterogeneous information networks and metapaths. Finally, we describe related theories and applications of multiview clustering in detail.

2.1. Pattern Recognition in IoT Data. The development and application of IoT technology make various data and information in terms of image, video, and operation log more accessible than ever before. Implementing multiple pattern recognition studies on these extremely large amounts of IoT data will help people gain a better understanding of intrinsic characteristics, activity mechanics, and evolution rules for the complex system. With the rapid development of computer technology and IoT, a large majority of data such as image, video, and graph are growing and obtained easily, which widely exist in the field of computer vision and machine learning. These data contain rich information, and mining its useful information has important theoretical and practical value in the field of pattern recognition, such as

human activity recognition, intention recognition, and video semantic recognition. Luo et al. [8] proposed a novel semisupervised feature analyzing framework for video semantic recognition by integrating the adaptive optimal similarity matrix learning into the procedure of feature selection. In the framework, the sensitivity of the model to the input affinity matrix is alleviated, and the intrinsic manifold structure of the original feature space is captured through adaptive neighbor assignment. Zhang et al. [9] employed spatiotemporal representations to enhance the EEG-based intention recognition in a cross-subject, multiclass scenario, and developed two unified, end-to-end trainable deep learning frameworks for human intention recognition. Chen et al. [10] developed a pattern-balanced semisupervised framework to extract and preserve diverse latent patterns of activities. By designing a recurrent convolutional attention network, they exploited the independence of multimodalities of sensory data and attentively identified salient regions that are indicative of human activities from inputs.

Inspired by the above studies, we focus on the e-commerce fraud detection problem and define two behavioral patterns for abnormal users: device aggregation and consumption aggregation. These behavior patterns can be expressed as special relationships in a graph structure, and they can effectively enhance the detection ability of the model. Based on this idea, we reorganize the users' behavioral as a mobile e-commerce network to explore the semantic and structural information of abnormal users, which can be helpful for fraud detection.

2.2. Graph Anomaly Detection. Graph is an abstract form of the real world, which has natural advantage in describing the data with complex interaction relationships. In many scenes, these relationships can provide abundant valuable information for anomaly detection. For example, in e-commerce fraud, abnormal users often disguise their identities by imitating normal users. By describing the relationships between different entities in a graph, it can be seen that no matter how abnormal users disguise, their fraudulent behaviors will inevitably expose some traces in the graph. Therefore, some anomaly detection techniques were proposed from the graph perspective and attracted extensive attentions from both academic and industrial fields.

Graph anomaly detection models the original problem with a graph structure and utilizes graph learning algorithms to find out abnormal nodes, edges, or subgraphs, whose distributions and patterns are different from other parts of the graph [11], as shown in Figure 1. Graph anomaly detection not only needs to consider the similarities between data objects but also needs to pay attention to their associations. In earlier studies, most graph anomaly detection methods employed manual feature engineering or statistical models [12, 13], but their generalization abilities are often insufficient. Afterwards, many machine learning technologies [14, 15] were used to improve the performance of graph anomaly detection. In many complex detection tasks, it is difficult to recognize abnormal objects from the raw data space due to the non-Euclidean structure and complicated intrinsic pattern [16]. To this end, several recent studies attempt to utilize deep learning models to learn appropriate representations for the anomaly detection objective [17, 18]. Specifically, deep graph representation learning and graph neural networks (GNNs) provide powerful tools to graph anomaly detection and produce a new research perspective for this field [19, 20].

In fact, research of graph anomaly detection for abnormal user recognition in the mobile e-commerce network is a relative new field. Due to the urgency of the e-commerce fraud problem, many research achievements have emerged in recently years. Jiang et al. [21] developed a detection method for abnormal users based on graph convolutional neural network. In order to quantify structure information between users, this method designs a weighting function to act on the user adjacency matrix, which can detect the behavior features of fraudulent groups. Wang et al. [22] proposed novel deep structure learning model for suspicious user recognition, which can preserve the nonlinear graph structure and user behavior information simultaneously. To capture the highly nonlinear relationship between vertexes in a user-item bipartite graph, Zheng et al. [23] designed a joint deep structure embedding framework for fraud detection. The framework embeds different types of vertexes jointly in the same latent space; it can preserve the highly nonlinear structural information of networks. Liu et al. [24] presented a heterogeneous GNN-based malicious account detection approach at Alipay. Based on two behavior patterns of attackers, i.e., device aggregation and activity aggregation, it adaptively learns discriminative embeddings from heterogeneous account-device graphs. In order to detect and prevent fraudulent insurance claims, Liang et al. [25] developed a data-driven procedure to identify fraudulent accounts, in which an automated fraud detection solution is designed based on graph learning. Specifically, groups of fraudster are uncovered and separated from normal customers by introducing a device-sharing network among claimants.

2.3. Heterogeneous Graph. Recently, many studies model the data with complex interaction relationships as heterogeneous information networks or heterogeneous graphs, which can comprehensively retain the original semantic and interaction pattern of objects. Heterogeneous information network represents a graph consisting of different types of entities (nodes) or relations (edges), whose definition is given as [26]:

Definition 1. Heterogeneous information network (or heterogeneous graph). A heterogeneous information network is defined as a graph $G = \{V, E\}$, where $V = \{v\}$ and $E = \{e\}$ represent the node set and the edge set, respectively. The network schema can be seen as a metatemplate of the graph, which is defined as $\mathcal{S} = (\mathcal{A}, \mathcal{R})$ with the node type mapping function $\phi(v)$: $V \longrightarrow \mathcal{A}$ and the edge type mapping function $\varphi(e)$: $E \longrightarrow \mathcal{R}$. $\mathcal{A}$ and $\mathcal{R}$ represent the node types and edge types, where $\mathcal{A} + \mathcal{R} > 2$.

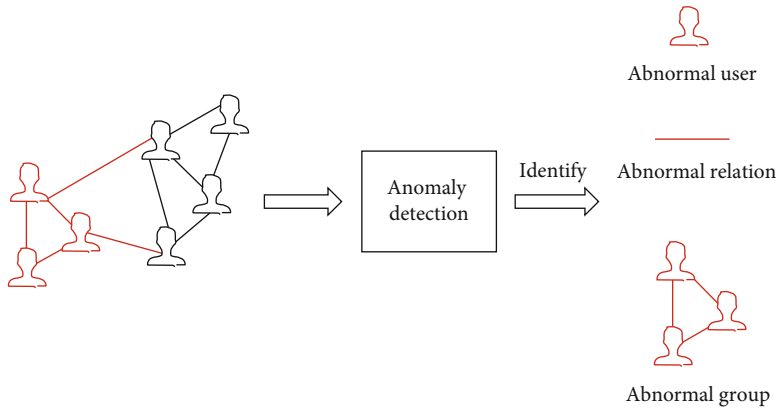


Figure 1: Schematic diagram of graph-based anomaly detection.

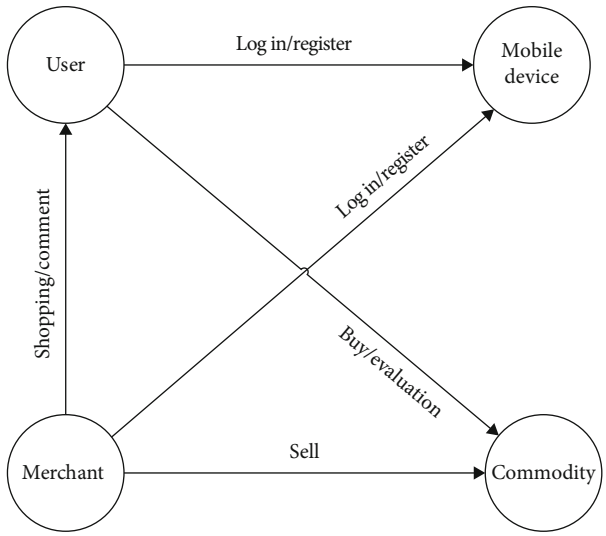


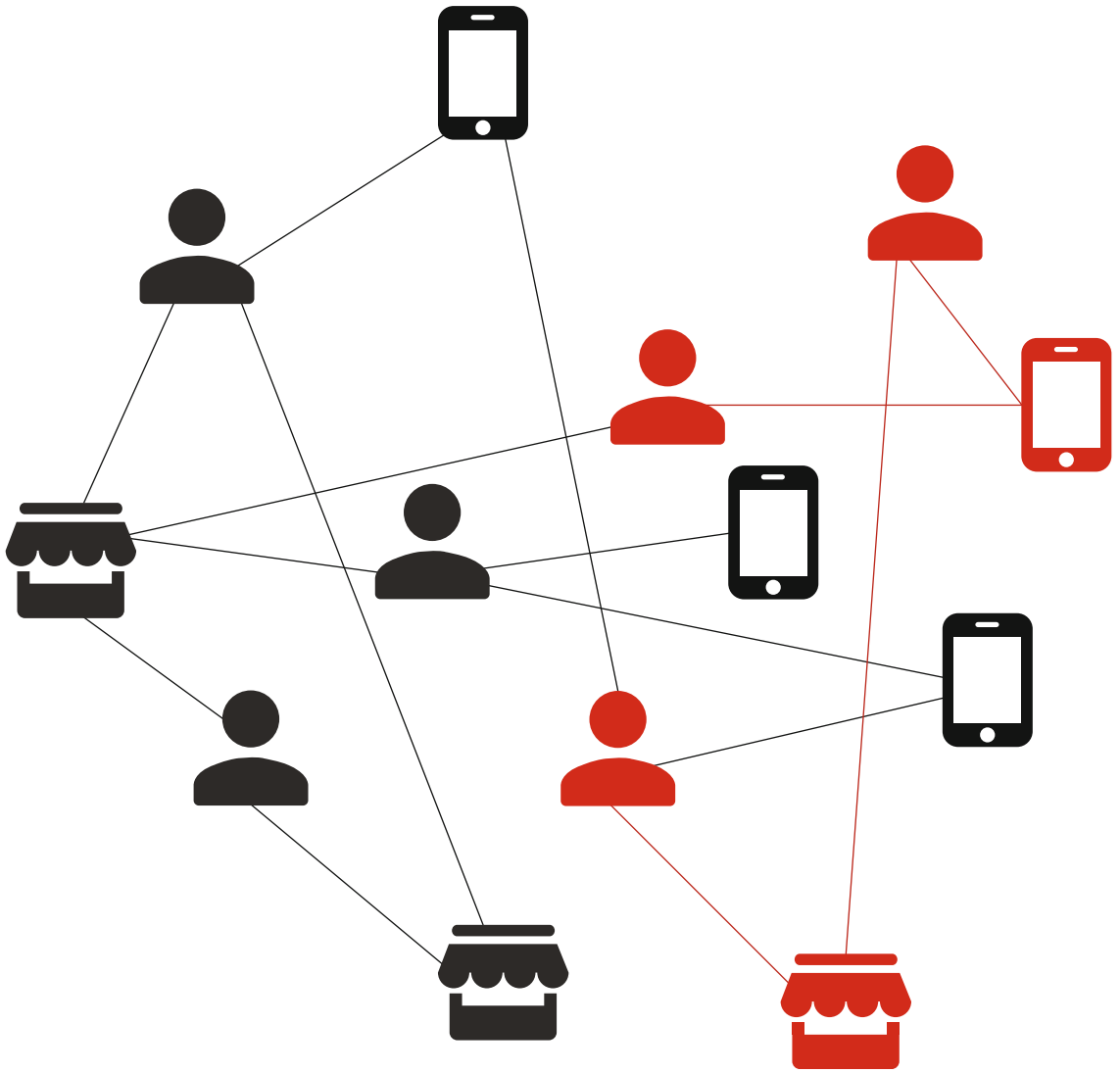
Figure 2: An illustrative example of a mobile e-commerce network.

Heterogeneous information networks provide a powerful data structure for modeling the entities in complex system and association relationships between them, as well as the high-level semantics of the data. To this end, many recent works focus on learning and predicting tasks on heterogeneous information network. Zhang et al. [27] introduced a structured heterogeneous information network to construct interactions between threads, users, replies, and topics to detect cybercriminal suspect threads. Fan et al. [28] designed a heterogeneous information network to model the relationship between users and tweets in Twitter. They also used a metagraph representation-based method to embed semantic correlations between users, in order to detect narcotic drug users. Zhu et al. [29] utilized passengers' taxi records to predict their short-term personalized transport demand based on deep heterogeneous network embeddings. To design a news recommendation system, Hu et al. [30] constructed a heterogeneous graph about user-news-topic and applied graph convolution networks to learn embeddings for user and news with high-order information endcoded by propagating embeddings over the graph. To improve the performance of visual question answering system, Li et al. [31] modeled the association relationships between different entities in the image as a heterogeneous information network. On this basis, they adopted a representation learning method based on graph attention mechanism to learn the relationship representation for visual question answering.

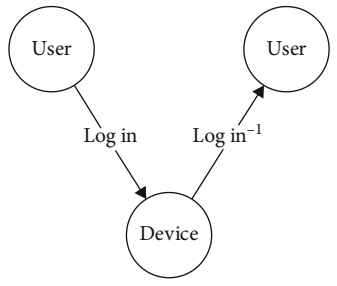
As an information network constituted by users and their behavior interactions, the mobile e-commerce network has prominent characteristics of heterogeneous structure. Figure 2 illustrates an example of a mobile e-commerce network. There are four types of object in the network, such as users, mobile devices, merchants, and products, as well as various association relationships between these objects. In this paper, we seek the solution for the mobile e-commerce fraud detection problem with the help of the heterogeneous network structure, in order to comprehensively capture the behavioral semantic and interaction pattern of abnormal users in the e-commerce platform.

2.4. Metapath. The heterogeneous information network consists of different types of object and different types of relationships between these objects. To effectively describe the rich semantic information in the heterogeneous information network, metapath is always used to represent the combination of relationships between different types of objects [32–34]. The definition of metapath is given as follows [26]:

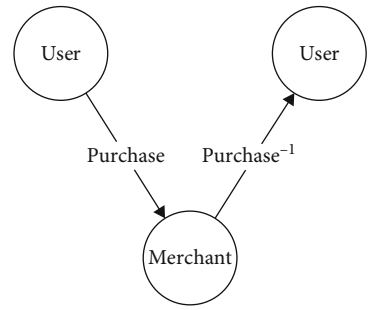
Definition 2 Metapath. Based on a network schema $\mathcal{S} = (\mathcal{A}, \mathcal{R})$, we can express a metapath as a sequence of binary relationships between two objects. In a network $S = (A, R)$, a metapath m is defined as $m = A_1 \longrightarrow^{R_1} A_2 \longrightarrow^{R_2} \cdots \longrightarrow^{R_l} A_{l+1}$ (recorded as $A_1A_2 \cdots A_{l+1}$), where $A_1, A_2, \cdots A_{l+1} \in \mathcal{A}$ and $R_1, R_2, \cdots R_l \in \mathcal{R}$ denote node types and edge types, respectively. Significantly, semantic relationships in the heterogeneous information network can be described in different views by different metapaths. For example, Figure 3 illustrates a mobile e-commerce network organized by a heterogeneous graph and the metapaths in the network. Figure 3(a) is a heterogeneous graph composed by users, merchants, and mobile devices. If two users login the e-



(a) A heterogeneous graph for e-commerce network



(b) UDU metapath

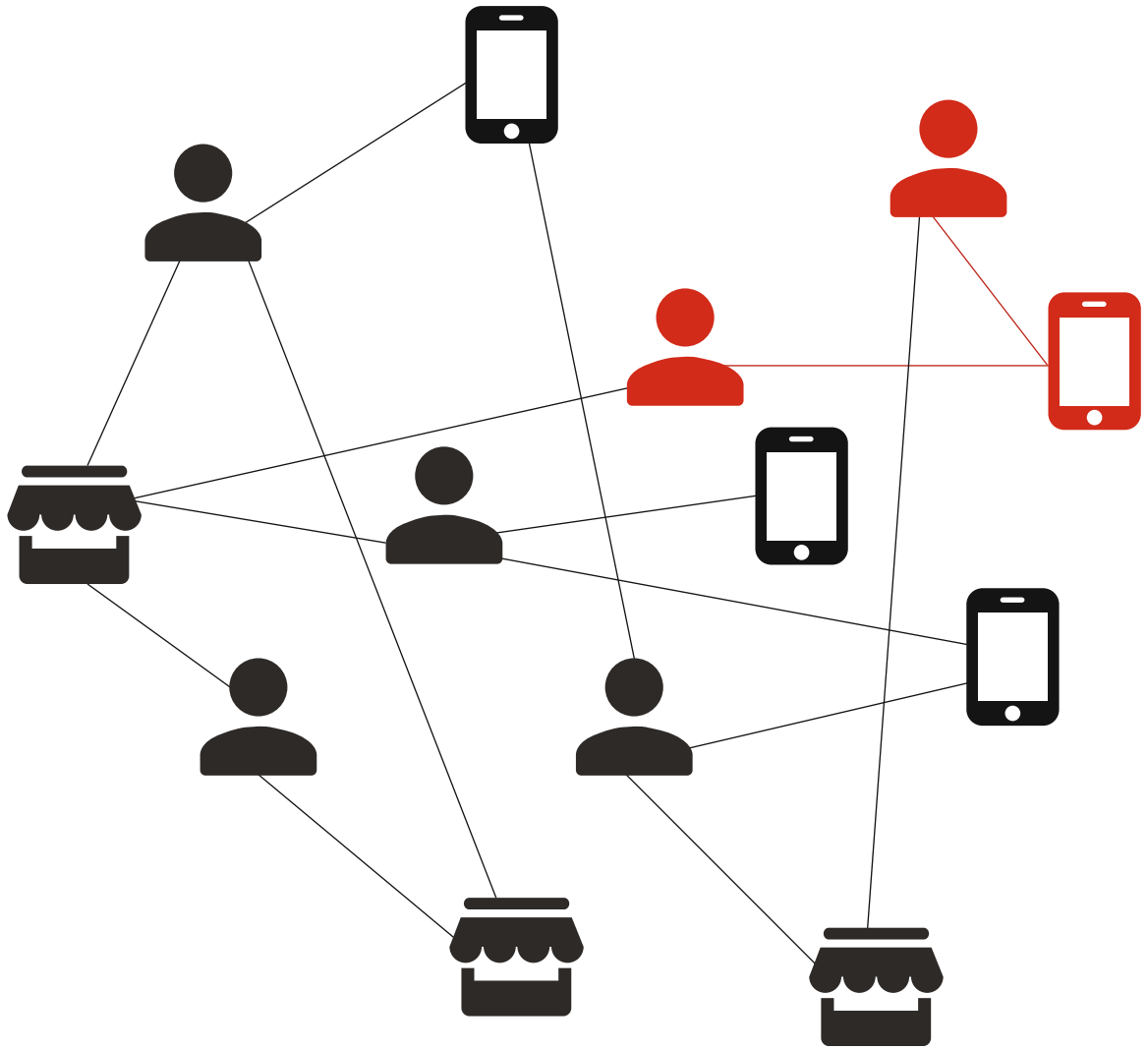


(c) UMU metapath

Figure 3: A mobile e-commerce network organized by a heterogeneous graph.

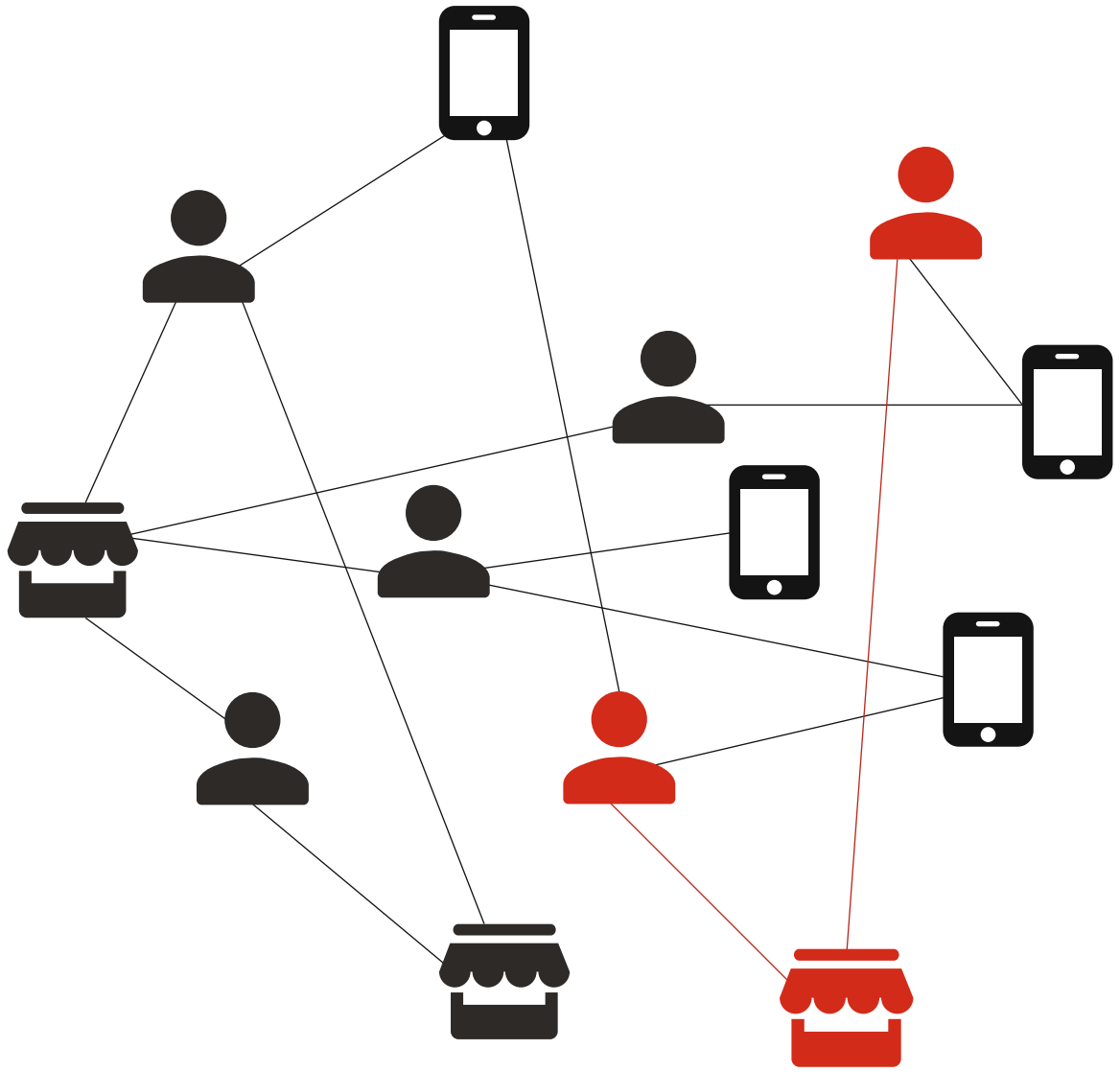
commerce platform from a same mobile device, the user-device-user (UDU) metapath shown in Figure 3(b) can be used to represent the logging connection between users. In another view, if two users buy commodity from a same merchant, the user-merchant-user (UMU) metapath shown in Figure 3(c) can be used to denote the purchase connection between users.

As an appropriate description for semantic information, metapath has been widely applied in the analyzing and mining of heterogeneous information networks. Fan et al. [35] constructed an e-commerce network including users, items, and queries, and they proposed a user representation learning method based on the metapath. Hu et al. [36] employed an attribute heterogeneous information network to model



(a) Semantic with UDU

Figure 4: Continued.



(b) Semantic with UMU

Figure 4: Semantic relationships of e-commerce network captured by different metapaths.

different entities, attributes, and associations in the credit payment service. They adopted a representation learning method based on metapath and hierarchical attention mechanism to learn user representations. Hosseini et al. [37] utilized the heterogeneous information network to model clinical data and captured important semantics for disease diagnosis with the help of metapath.

2.5. Multiview Clustering. Driven by the widely application of IoT and sensor network, the multiview data is becoming more and more common and easier to acquire. Compared with the traditional data which describe objects from a single view, the multiview data with rich semantic information is more useful and more complex [38]. Traditional clustering algorithms are not applicable to deal with the multiview data; thus, more and more attentions have been paid to multiview clustering, in order to explore potential information among different views. In [39], Zhang et al. presented a multiview fuzzy clustering algorithm based on the consistency constraint of representative points. The algorithm utilizes the consistency constraints of representative points to realize multiview collaborative learning, which ensures the improvement of the clustering effect. Luo et al. [40] proposed a subspace learning-based clustering approach, in which a shared consistent representation is used to constrain the multiview self-representation attributes to mine the subspace structure of the data. Xia et al. [41] developed a multiview clustering algorithm based on the neighborhood multikernel learning to perform information fusion in the class partition space. In [42], Tang et al. presented a joint graph learning method for multiview subspace clustering, in which the LRR model is employed to learn a common representation coefficient matrix from different views, and a diversity regularization term is used both to enforce the diversity and to reduce the redundancy of views. Based on that, the learned representation coefficient matrix is converted to an affinity graph for

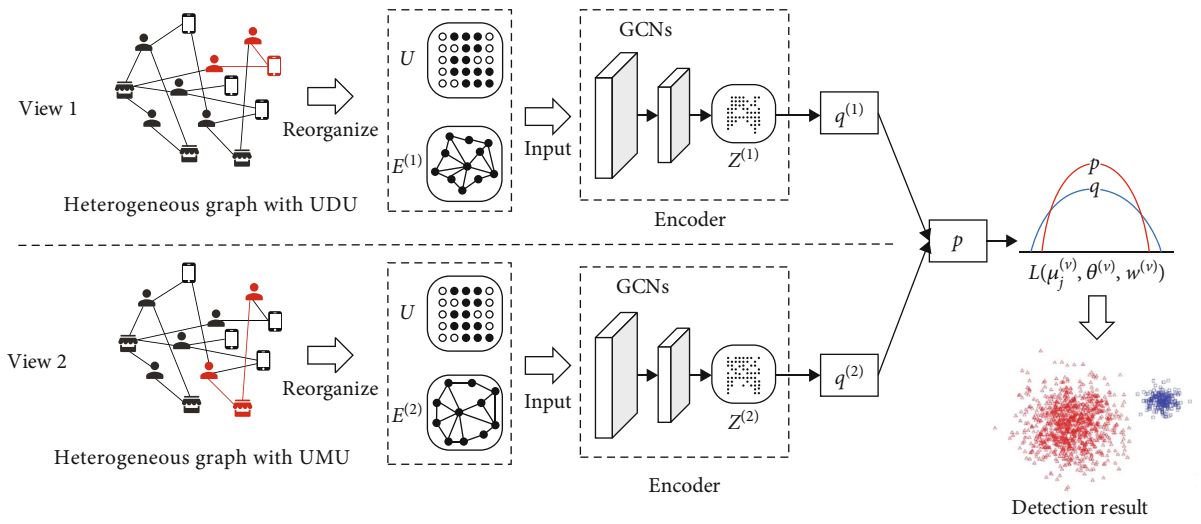


Figure 5: The overall framework of DM-VCDM.

Input: user-similarity graph $G^{(v)}(U, E^{(v)})$, number of iterations L, number of clusters K;
Output: The abnormal user detection results;
Initialize the parameter of the GCNs $\theta^{(v)}$, and $w_1 = w_2 = 1/2$;
for v =1 to 2:
    Encode $G^{(v)}(U, E^{(v)})$ to get latent embedding $Z^{(v)}$ by Equation (3)
    Initialize cluster assignments and $\{\mu_k^{(v)}\}_{k=1}^{K}$ using K-means++ in each view;
    Initialize $q_{ik}^{(v)}$ and $p_{ik}^{(v)}$ by Equation (5) and Equation (6) respectively;
end for;
for l =1 to L:
    for v =1 to 2:
        Update $\theta^{(v)}$ and $\{\mu_k^{(v)}\}_{k=1}^{K}$ using backward propagate SGD according to Equation (10) and Equation (11);
        Update latent embedding $Z^{(v)}$ by Equation (3);
        Update $q_{ik}^{(v)}$ and $p_{ik}^{(v)}$ by Equation (5) and Equation (6) respectively;
    end for;
    Calculate p_{ik} according to Equation (7);
    Update w_1 and w_2 by Equation (12);
end for;
Calculate the detection results by Equation (7);
Return cluster assignments for all users

Algorithm 1: Implementation of the DM-VCDM.

subspace clustering. To solve the multiview spectral clustering problem, Tang et al. [43] designed a novel model by jointly utilizing the information of view-specific graphs and embedding matrices, in which a unified graph is introduced by combining view-specific graphs and embedding matrices.

In this paper, we design a multiview clustering-based abnormal user detection model for the mobile e-commerce network, which can be used to solve the problem of e-commerce fraud by detecting abnormal user more reasonably from multiple perspectives.

3. The Proposed Model

3.1. Basic Consideration of the Work. Based on the analysis of a large number of e-commerce fraud cases, we find that many fraud gangs utilize disguised phone numbers or emails to register a large amount of accounts on different mobile devices, and they login these accounts buy promotional commodities at relative low prices. Afterwards, they resell these commodities at higher prices in the second-hand market to gain huge illegal profits. In order to effectively

Table 1: e-commerce datasets used in experiments.

Datasets	Records	Users	Features	Devices	Merchants	Relationships	Abnormal rate
Dataset 1	32 K	3458	12	2998	2097	55 K	5.15%
Dataset 2	20 K	2785	12	2218	1989	34 K	6.07%
Dataset 3	15 K	2542	12	2145	1795	25 K	7.76%
Dataset 4	27 K	3054	10	2742	2502	50 K	5.44%

Table 2: Confusion matrix.

Confusion matrix		Predicted	
		1	0
Real	1	True positive (TP)	False negative (FN)
	0	False positive (FP)	True negative (TN)

recognize fraudulent users in the e-commerce platform, we first summarize two behavior patterns of abnormal users corresponding to the above fraud scenes: device aggregation and transaction aggregation.

3.1.1. Device Aggregation. Device aggregation means a significant quantity of accounts register or login on the same device or a common set of devices. Abnormal users usually have a device pool consisting of a certain number of mobile phones, tablets, computers, and other terminal devices. For cost considerations, the large amounts of accounts are always registered and logged through a limited number of devices in the pool.

3.1.2. Transaction Aggregation. The basic idea of transaction aggregation is that plenty of purchase transactions on the e-commerce intensively occur between certain accounts and merchants that implement promotions, when the fraud activity takes place. This is mainly because fraud gangs generally pay their attention to certain merchants with promotion, and they will intensively buy commodities with large discounts in a short time.

Device aggregation and transaction aggregation describe typical behavior patterns of fraud gangs from two perspectives; thus, abnormal user detection can be realized by recognizing these behavior patterns. To this end, we capture semantic relationships from heterogeneous graph of mobile e-commerce network using different metapaths as shown in Figures 4(a) and 4(b), respectively. In the former one, the abnormal users are connected by corresponding devices, while in the latter one, the suffered merchants take on the role of correlating fraud accounts. Based on these semantic relationships, we construct a multiview framework to detect the abnormal behavior patterns of device aggregation and transaction aggregation in corresponding views, in order to discover fraudulent users in the e-commerce network.

3.2. Construction of the Model. The overall framework of the proposed model, i.e., DM-VCDM, is illustrated in Figure 5. In general, the semantic relationships captured from heterogeneous graph of mobile e-commerce network are transferred and explored through two tunnels corresponding to two views, in which the two abnormal behavior patterns will be recognized, respectively. In each view, a user-similarity graph is reorganized from semantic relationships by using a certain metapath. Subsequently, the node (user) embeddings of each graph in the latent space are learned by the encoder formed by GCNs. Then, soft clustering is applied on latent embeddings in each view, in order to divide users' behavior patterns into different categories from the particular perspectives. At last, the abnormal detection result is produced by integrating assignments of behavior pattern in different views in a multiview fusion mechanism. In the DM-VCDM model, the behavior patterns of abnormal user are described and explored comprehensively from two different views. And, the detection decision is made by fusing the complementary information into a consensus prediction. The details of the model are presented as follows.

According to the UDU and UMU metapaths, the similarities between two users in different views can be calculated by the following equation:

$$\mathrm{Sim}_{ij}^{(v)} = \frac{2 \times \left| \left\{ r_{i \longrightarrow j}^{(v)} : r_{i \longrightarrow j}^{(v)} \in R^{(v)} \right\} \right|}{\left| \left\{ r_{i \longrightarrow i}^{(v)} : r_{i \longrightarrow i}^{(v)} \in R^{(v)} \right\} \right| + \left| \left\{ r_{j \longrightarrow j}^{(v)} : r_{j \longrightarrow j}^{(v)} \in R^{(v)} \right\} \right|}, \tag{1}$$

where $v = 1$ or 2 is the ID of the view. In the v^{th} view, $\mathrm{Sim}_{ij}^{(v)}$ is the similarity between the user i and the user j, $r_{i \longrightarrow j}^{(v)}$ denotes a route in the graph between these two users constrained by the metapath, and $R^{(v)}$ denotes the set of routes in the graph. By calculating the similarity between users in different metapaths, the user-similarity matrixes in different views can be constructed, respectively, as shown in Equation (2), where m denotes the number of users in the e-commerce network. Based on that, two user-similarity graphs $G^{(v)}(U, E^{(v)})$ with N user nodes can be reorganized from semantic relationships in the corresponding views, respectively, where U is matrix composed of attributes of users in the e-commerce network.

$$E^{(v)} = \begin{bmatrix} \mathrm{Sim}_{11}^{(v)} & \mathrm{Sim}_{12}^{(v)} & \cdots & \mathrm{Sim}_{1N}^{(v)} \\ \mathrm{Sim}_{21}^{(v)} & \mathrm{Sim}_{22}^{(v)} & \cdots & \mathrm{Sim}_{1N}^{(v)} \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{Sim}_{N1}^{(v)} & \mathrm{Sim}_{N2}^{(v)} & \cdots & \mathrm{Sim}_{NN}^{(v)} \end{bmatrix}. \tag{2}$$

Table 3: Reference models used in the experiments.

Models	Model description
IF	Isolation Forest (IF) [44] is a tree-based anomaly detection model, which assumes that the abnormal objects can be isolated from others by fewer random feature segmentations compared with normal objects.
KNN	The K-nearest neighbor (KNN) model [45] recognizes the outliers as abnormal objects by comparing distances between objects.
LOF	The local outlier factor (LOF) algorithm [46] is based on an assumption that the local density of a normal object should be close to its neighbor's density, while the local density of an abnormal object will be remarkably different from its neighbor's density.
CAE+IF/CAE+KNN/ CAE+LOF	These models are all composed of two components: a convolutional autoencoder is used to obtain low-dimensional embeddings, and an abnormal detector (IF/KNN/LOF) is used to discover abnormal objects based on the embeddings.
DeepFD	The model encodes the user-item bipartite graph into low-dimensional user representations with behavioral features using an autoencoder and employs DBSCAN to detect fraud block based on the representations [22].
FraudNE	The model captures the high-nonlinear characteristics from the user-item bipartite graph by an autoencoder and recognizes multiple fraudulent groups by predicting the cluster assignments based on the user representations [23].

Table 4: Detection results of different models in dataset 1.

Models	P	R	F1	AUC
IF	0.8712	0.8804	0.8789	0.7878
KNN	0.8498	0.8657	0.8562	0.7369
LOF	0.8511	0.8796	0.8657	0.7542
GAE+IF	0.9086	0.9178	0.9105	0.8298
GAE+KNN	0.8765	0.8814	0.8809	0.7921
GAE+LOF	0.8847	0.8998	0.8921	0.8096
DeepFD	0.9229	0.9548	0.9401	0.8556
FraudNE	0.9393	0.9201	0.9305	0.8438
DM-VCDM	**0.9502**	**0.9708**	**0.9628**	**0.8801**

Table 5: Detection results of different models in dataset 2.

Models	P	R	F1	AUC
IF	0.8344	0.8172	0.8245	0.7326
KNN	0.821	0.8045	0.8153	0.7216
LOF	0.8492	0.8207	0.8355	0.7452
GAE+IF	0.8847	0.8379	0.8622	0.7764
GAE+KNN	0.8679	0.844	0.8547	0.7629
GAE+LOF	0.8705	0.881	0.8776	0.7850
DeepFD	0.9246	0.8779	0.9071	0.8121
FraudNE	0.9054	0.8655	0.8886	0.7954
DM-VCDM	**0.9398**	**0.9033**	**0.9222**	**0.8315**

In each view, the user-similarity graph is embedded into latent representations by an encoder constructed by GCNs according to the following equation:

$$Z^{(v)} = \mathrm{GCNs}\left(X, E^{(v)}\right). \tag{3}$$

$Z^{(v)}$ denotes the latent embedding of the user-similarity graph in v^{th} view, and the framework of the GCNs is formulated as the following equation:

$$\mathrm{GCNs}\left(X, E^{(v)}\right) = \mathrm{Gconv}\left(\mathrm{ReLU}\left(\mathrm{Gconv}\left(X, E^{(v)}; W_0^{(v)}\right)\right); W_1^{(v)}\right), \tag{4}$$

where $\mathrm{Gconv}(\cdot)$ denotes the graph convolutional layer and $W_0^{(v)}$ and $W_1^{(v)}$ are learnable weight matrixes in the two graph convolutional layers, respectively.

In the latent space, we employ K-means++ to initialize the cluster assignments for user embeddings and alternately enhance the clustering in respective views. In the abnormal user detection context, the users are categorized as normal users and abnormal users. Thus, the number of cluster K is considered as 2. Given a set of user embeddings $Z^{(v)} = \{z_i^{(v)}\}_{i=1}^{N}$ and the initial cluster centroids $\{\mu_k^{(v)}\}_{k=1}^{K}$, the soft assignment between the embedded users and the cluster centroids in each view can be calculated using a Students' t-distribution according to the following equation:

$$q_{ik}^{(v)} = \frac{\left(1 + \left\|z_i^{(v)} - \mu_k^{(v)}\right\|^2/\alpha\right)^{-\alpha+1/2}}{\sum_k \left(1 + \left\|z_i^{(v)} - \mu_k^{(v)}\right\|^2/\alpha\right)^{-\alpha+1/2}}, \tag{5}$$

where $q_{ik}^{(v)}$ denotes the soft assignment distribution and α is the degree of freedom of the Student t-distribution. $q_{ik}^{(v)}$ can be interpreted as the probability that assigns the i^{th} user embedding to the k^{th} cluster. Due to the lack of labels, we design an auxiliary target distribution to

Table 6: Detection results of different models in dataset 3.

Models	P	R	F1	AUC
IF	0.8011	0.8263	0.8100	0.7207
KNN	0.8206	0.8053	0.8114	0.7298
LOF	0.7862	0.7967	0.7901	0.6924
GAE+IF	0.8401	0.8654	0.854	0.7610
GAE+KNN	0.8605	0.8202	0.8417	0.7513
GAE+LOF	0.8252	0.8367	0.8304	0.7458
DeepFD	0.8580	0.9003	0.8803	0.7892
FraudNE	0.8771	0.9066	0.8954	0.8045
DM-VCDM	**0.9056**	**0.9351**	**0.9241**	**0.8386**

Table 7: Detection results of different models in dataset 4.

Models	P	R	F1	AUC
IF	0.7640	0.7366	0.7512	0.6641
KNN	0.7532	0.7181	0.7305	0.6372
LOF	0.7398	0.7257	0.7321	0.6424
GAE+IF	0.826	0.801	0.8155	0.7254
GAE+KNN	0.8036	0.7834	0.7903	0.7025
GAE+LOF	0.7957	0.7767	0.7825	0.6987
DeepFD	0.9003	0.8866	0.8954	0.8052
FraudNE	0.8760	0.8564	0.8662	0.7758
DM-VCDM	0.9204	**0.9398**	**0.9301**	**0.8468**

iteratively refine the cluster assignments in different views in the following equation:

$$p_{ik}^{(v)} = \frac{{q_{ik}^{(v)}}^2 / f_k^{(v)}}{\sum_k {q_{ik}^{(v)}}^2 / f_k^{(v)}}, \tag{6}$$

where $f_k^{(v)} = \sum_i q_{ik}^{(v)}$ is the soft cluster frequency in the v^{th} view.

To produce a consensus detection result, we design a multiview fusion mechanism to integrate the complementary information in respective views according to the following equation:

$$p_{ik} = w_1 p_{ik}^{(1)} + w_2 p_{ik}^{(2)}, \tag{7}$$

where p_{ik} is the integrated auxiliary target distribution and $w_1 > 0$ and $w_2 > 0$ are the information weights of the two views, respectively, with the constraint $w_1 + w_2 = 1$. The integrated target distribution predicts the probability of user assignment more comprehensively than that generated in any single view. Finally, the user detection result is produced by the following equation:

$$y_i = \arg\max_k p_{ik}, \tag{8}$$

where y_i means the clustering assignment of i^{th} user.

Table 8: Ordinal values of different models' F1 score.

Models	Dataset 1	Dataset 2	Dataset 3	Dataset 4	Average value
IF	7	8	8	7	7.5
KNN	9	9	7	9	8.5
LOF	8	7	9	8	8
GAE+IF	4	5	4	4	4.25
GAE+KNN	6	6	5	5	5.5
GAE+LOF	5	4	6	6	5.25
DeepFD	2	2	3	2	2.25
FraudNE	3	3	2	3	2.75
DM-VCDM	1	1	1	1	1

3.3. The Optimization Model. The DM-VCDM can be trained in a recursive optimization process. The joint optimization model of the DM-VCDM can be established as the following equation:

$$\begin{aligned} &L\left(\mu_k^{(v)}, \theta^{(v)}, w_v\right) \\ &= \min_{\mu^{(v)}, \theta^{(v)}, w_v} \left\{ \sum_i \sum_k \left(w_1 p_{ik}^{(1)} + w_2 p_{ik}^{(2)}\right) \log \frac{w_1 p_{ik}^{(1)} + w_2 p_{ik}^{(2)}}{q_{ik}^{(1)}} \right. \\ &\quad \left. + \sum_i \sum_k \left(w_1 p_{ik}^{(1)} + w_2 p_{ik}^{(2)}\right) \log \frac{w_1 p_{ik}^{(1)} + w_2 p_{ik}^{(2)}}{q_{ik}^{(2)}} \right\}, \end{aligned} \tag{9}$$

where the cluster centroid $\mu_k^{(v)}$, the encoder's parameters $\theta^{(v)}$, and the information weight in each view are optimized alternately by the stochastic gradient descent (SGD). In each iteration, the encoder's parameters $\theta^{(v)}$ and the cluster centroids $\mu_k^{(v)}$ in each view are firstly updated using the user embeddings by the following equations:

$$\begin{aligned} \frac{\partial L}{\partial z_i^{(v)}} = \frac{\alpha + 1}{\alpha} \sum_k \left(1 + \frac{\left\| z_i^{(v)} - \mu_k^{(v)} \right\|^2}{\alpha}\right)^{-1} \\ \cdot \left(w_1 p_{ik}^{(1)} + w_2 p_{ik}^{(2)} - q_{ik}^{(v)}\right) \left(z_i^{(v)} - \mu_k^{(v)}\right), \end{aligned} \tag{10}$$

$$\begin{aligned} \frac{\partial L}{\partial \mu_k^{(v)}} = -\frac{\alpha + 1}{\alpha} \sum_k \left(1 + \frac{\left\| z_i^{(v)} - \mu_k^{(v)} \right\|^2}{\alpha}\right)^{-1} \\ \cdot \left(w_1 p_{ik}^{(1)} + w_2 p_{ik}^{(2)} - q_{ik}^{(v)}\right) \left(z_i^{(v)} - \mu_k^{(v)}\right). \end{aligned} \tag{11}$$

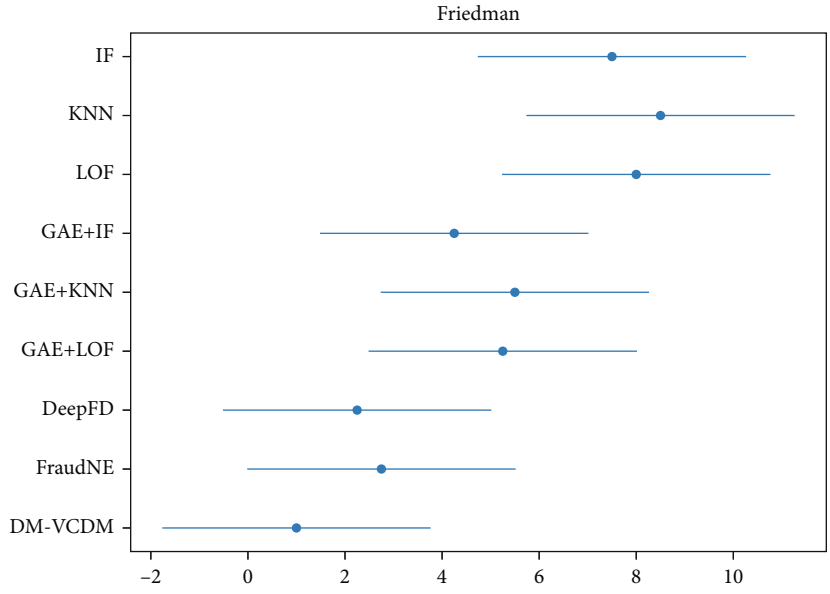


Figure 6: Friedman test diagram.

Then, the information weights can be acquired according to the optimization objective shown in the following equation:

$$L(w_v) = \min_{w} \left(\sum_i \sum_k p_{ik} \log \frac{p_{ik}}{q_{ik}^{(1)}} + \sum_i \sum_k p_{ik} \log \frac{p_{ik}}{q_{ik}^{(2)}} \right). \quad (12)$$

On this basis, the implement process of the DM-VCDM model is listed in Algorithm 1.

4. Experiments and Analysis

In this section, a series of experiments are conducted on several e-commerce data sets to evaluate the validity of the proposed model.

4.1. Experimental Setup

4.1.1. Datasets. Four e-commerce datasets are used in the experiments including three real-world datasets and one semisynthetic dataset. The real-world datasets are subsets sampled from an e-commerce transaction dataset on Kaggle, which is consisted of 400 K transaction records collected from an e-commerce platform. Each record includes several transaction information such as IDs of user, mobile device, commodity, merchant, and transaction time. And some of users in the dataset are labeled as fraudsters. Based on the sampled subsets, we capture the login relationships between user and device and transaction relationships between user and merchant and construct the three real datasets. The semisynthetic dataset is generated from a dataset of user consumption records collected from a large online store. The raw dataset is consisted of 15 K records including 2487 users, 1996 devices, 1564 merchants, and 27 K relationships. Due to the lack of available user labels, we uniformly select 5% of users from the whole dataset as the fraudulent users and mimic the behaviors of fraudsters. And we also randomly select a certain number of merchants as targets in our experiments. The details of these datasets are shown in Table 1.

4.1.2. Evaluation Indexes. In the experiments, we employ precision (P), recall (R), F1-score (F1), and AUC, which are widely utilized in clustering and classification tasks, to evaluate performances of different models. In this paper, the abnormal user detection is treated as a binary classification problem. Based on the confusion matrix in Table 2, the precision and recall indexes are defined as Equations (13) and (14), respectively.

$$P = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}, \quad (13)$$

$$R = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}. \quad (14)$$

On this basis, the F1-score is defined as follows:

$$\mathrm{F1} = \frac{2 \times P \times R}{P + R}. \quad (15)$$

As a common evaluation index for binary classification problem, the AUC is also introduced in the experiments, which means the area under the ROC curve. The horizontal axis and vertical axis of the ROC curve are set as false positive rate (FPR) and true positive rate (TPR), respectively. The FPR and the TPR are defined as follows:

$$\begin{aligned} \mathrm{FPR} &= \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}}, \\ \mathrm{TPR} &= \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}. \end{aligned} \quad (16)$$

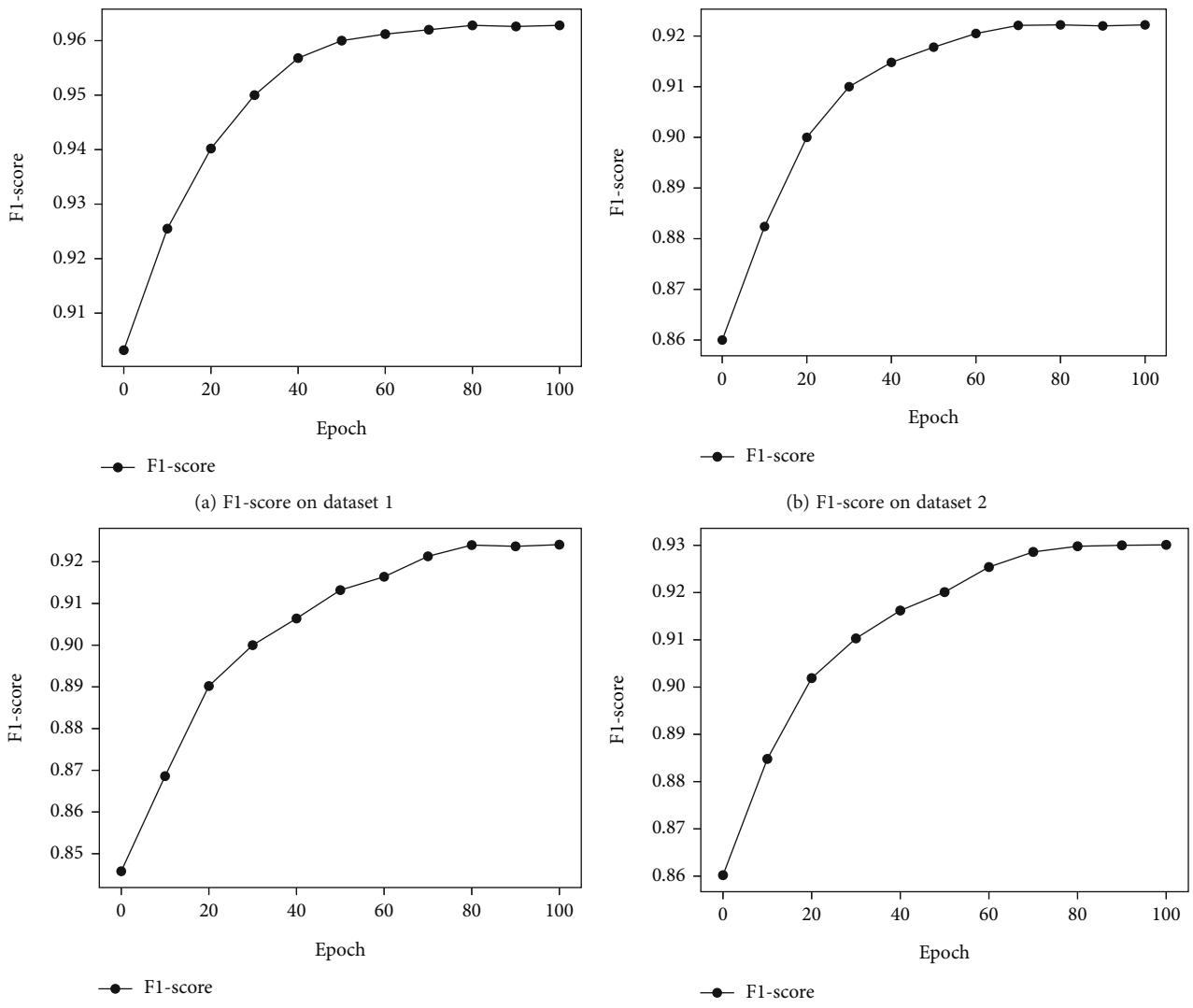
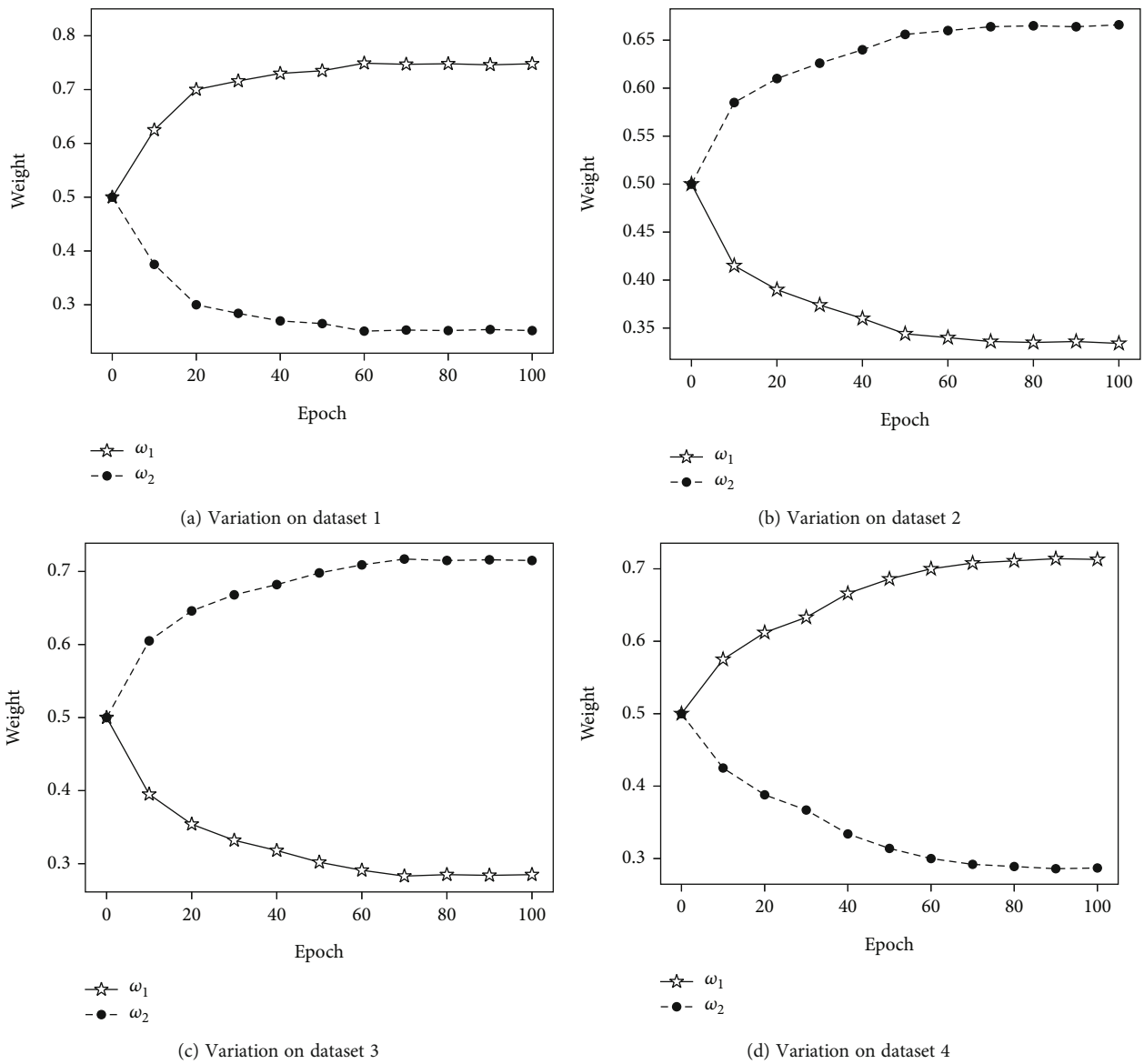


Figure 7: Changes of the F1-score in the optimization process of the DM-VCDM on different datasets.

4.1.3. Reference Models. Three categories of reference model are used for comparison in the experiments. In the first category, three traditional anomaly detection models are selected. In the second category, the traditional models are combined with the convolutional autoencoder. And the third category includes two deep graph anomaly detection models, namely, DeepFD [22] and FraudNE [23]. Parameters of all these reference models are set according to their authors' suggestions. The details of these reference models are listed in Table 3.

4.2. Performance Comparison. All the experiments are programed by Pytorch and conducted on a computer with Intel Core i5-4200H CPU 2.80 GHz, 12 GB RAM, and 64-bit Win 10 system. On each dataset, we run all the algorithms 50 times and use their average results for comparison. The detection results on different datasets are listed in Tables 4–7, in which the best results are highlighted in boldface. The numerical results in these tables show that the proposed DM-VCDM significantly outperforms both traditional algorithms and deep models with all the indexes on the 4 datasets. The traditional algorithms recognize the abnormal user by searching the isolated distribution patterns in the original feature space. However, the abnormal patterns of fraudulent behavior in the e-commerce context are usually difficult to be recognized directly in the original feature space. As a result, their detection results are not very reliable. Combine these traditional algorithms with a convolutional autoencoder can learn effective representations for abnormal detection; thus, their performances are improved to a certain extent. The DeepFD and the FraudNE introduce the relationships between different objects by using the user-item bipartite graph; consequently, capture the abnormal patterns more reliably. Compared with these two graph-based models, the proposed DM-VCDM comprehensively describes the fraudulent behavior patterns in two different views and produces the detection decision by fusing the complementary information in a joint multiview learning framework. The superior



(a) Variation on dataset 1

(b) Variation on dataset 2

(c) Variation on dataset 3

(d) Variation on dataset 4

Figure 8: Variation of the information weight in DM-VCDM on different datasets.

results over reference models demonstrate the effectiveness of the proposed DM-VCDM for describing and recognizing abnormal behavior pattern.

To further compare performances of different models in the experiments comprehensively, we perform the Friedman test on F1-score results of these models. Based on the results in Tables 4–7, the ordinal values of different models on each dataset in terms of F1-score are presented in Table 8.

The null hypothesis is set as H_0: the performances of all the models in the experiments are essentially the same in terms of F1-score. And the alternative hypothesis is set as H_1: there are significant differences between F1-score results of these tested models. Assuming k models are tested on M datasets, we use τ_i to denote the average ordinal value of the i^{th} model, which is normally distributed with the mean $(k+1)/2$ and variance $(k^2-1)/12$. And the variate τ_F defined in Equation (17) obeys an F distribution with the degrees of freedom $k-1$ and $(k-1)(M-1)$.

$$\tau_F = \frac{(N-1)\tau_{\chi^2}}{N(k-1)-\tau_{\chi^2}}, \tag{17}$$

where the variate τ_{χ^2} defined in Equation (18) obeys an χ^2 distribution with the degree of freedom $k-1$.

$$\tau_{\chi^2} = \frac{12M}{k(k+1)}\left(\sum_{i=1}^{k}\tau_i^2 - \frac{k(k+1)^2}{4}\right). \tag{18}$$

In our experiments, 9 models are compared on 4 datasets. For the significance level $\alpha = 0.05$, the calculation result of testing variate is $\tau_F = 14.45$, which is significantly bigger

Table 9: Results of running time tests (s).

Models	Dataset 1	Dataset 2	Dataset 3	Dataset 4
IF	1.3835	0.9491	1.8997	1.3946
KNN	0.9694	0.6118	1.9562	0.9261
LOF	0.3776	0.2199	0.4463	0.4444
CAE+IF	109.6416	60.5061	132.0117	107.1775
CAE+KNN	69.8979	46.4376	116.7697	67.4992
CAE+LOF	57.9402	29.6497	54.1312	43.5095
DeepFD	30.9515	37.2577	32.6546	22.5648
FraudNE	33.6465	45.6109	41.3464	28.8446
DM-VCDM	53.7763	61.9759	50.9191	42.8212

than the corresponding critical value and denotes the negation of the null hypothesis. The results of the Friedman test show that the performances of the models compared in the experiments are significantly different. That is to say, the superiority of the DM-VCDM model is of statistically significant. For further analysis, we illustrate the testing results of different model in a Friedman test diagram, as shown in Figure 6. From the figure, it can be proved that the proposed DM-VCDM can actually achieve a superior detection performance compared in contrast to the reference models.

4.3. Optimization Process Analysis. In the proposed DM-VCDM, the final detection decision is produced by fusing multiview information in a joint learning framework. To investigate how the model works, we test the learning process of the joint framework and the impact of each view on the model in this section.

In Figure 7, we illustrate the change of the F1-score during the optimization process of the DM-VCDM on each dataset. From the figure, we can easily find that during the optimization process, the F1-score results are boosted on the datasets as the number of iterations increases. The results demonstrate that the proposed DM-VCDM model can effectively capture the behavioral patterns and semantic relationships of abnormal user, and the multiview fusion mechanism also helps to enhance its ability of recognizing anomaly target in the e-commerce network. It is notable that the F1-score on each datasets achieves relatively outstanding value and stays in a stable state after a certain epoch of optimization. This apparent performance proves that the DM-VCDM model has relative better convergence speed and stability.

To investigate the impact of different views on the proposed model, we present the variation of the information weights of different views during the optimization process in Figure 8. As we can see, based on the same initializations, the information weights can be adjusted adaptively as the optimization progresses. The variation of the curves indicates that the better view whose information is more useful will gradually dominate the final detection result in the learning process. For example, in Figure 8(a), w_1 keeps getting bigger in the optimization process, and w_2 decreases as the iteration goes on, while in Figure 8(b), the variation of the weights reveals an opposite trend. This is mainly because the device aggregation is more useful for recognizing the abnormal behaviors in dataset 1, while in dataset 2, the transaction aggregation becomes the dominant pattern of the fraudulent behavior.

4.4. Running Time Test. In this section, we compare the running time of different models on each dataset for a more sufficient analysis of the proposed DM-VCDM. As shown in Table 9, it can be proved that our proposed model can achieve outstanding detection performance with acceptable computational cost compared to the traditional algorithms or deep models. As a result, the DM-VCDM can be applied to some abnormal detection tasks for large-scale e-commerce networks.

5. Conclusion

To cope with the problem of rampant network fraud in e-commerce platform, two typical behavior patterns are introduced to capture the semantic relationships for fraud gangs from two perspectives by abstracting the e-commerce network as a heterogeneous information graph. On this basis, we develop a joint multiview abnormal detection model, in which the two behavior patterns are captured in different views of the model, respectively. Finally, the abnormal detection result is produced by fusing the complementary information from different views in a multiview fusion mechanism. We conduct experiments by comparing the proposed model with several traditional algorithms and deep models on several e-commerce datasets. The experimental results demonstrate the validity and superiority of the proposed model.

In further work, we plan to improve our work from the perspective of exploring the intrinsic mechanism behind e-commerce fraud by drawing support from the studies of intention recognition and semantic recognition.

Data Availability

The data used to support the findings of this study have been deposited in the OSF repository (doi:10.17605/OSF.IO/KYQN9).

Disclosure

Our work was preregistered in an independent, institutional registry, i.e., http://osf.io/. And the registration DOI is doi:10.17605/OSF.IO/KYQN9.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Nos. 61902227, 62076154, 62022052, and U21A20513).

References

[1] Y. Wang, W. Yu, P. Teng, G. Liu, and D. Xiang, "A detection method for abnormal transactions in e-commerce based on extended data flow conformance checking," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 4434714, 14 pages, 2022.

[2] J. Ren, J. Guo, W. Qian, H. Yuan, X. Hao, and H. Jingjing, "Building an effective intrusion detection system by using hybrid data optimization based on machine learning algorithms," *Security and Communication Networks*, vol. 2019, Article ID 7130868, 11 pages, 2019.

[3] R. Cao, G. Liu, Y. Xie, and C. Jiang, "Two-level attention model of representation learning for fraud detection," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 6, pp. 1291–1301, 2021.

[4] Y. Ren, H. Zhu, J. Zhang, P. Dai, and L. Bo, "EnsemFdet: an ensemble approach to fraud detection based on bipartite graph," in *2021 IEEE 37th International Conference on Data Engineering (ICDE)*, pp. 2039–2044, IEEE, Chania, Greece, 2021.

[5] C. Shi, R. J. Wang, and X. Wang, "Survey on heterogeneous information networks analysis and applications," *Journal of Software*, vol. 33, no. 2, pp. 598–621, 2021.

[6] B. Hooi, H. A. Song, A. Beutel, N. Shah, K. Shin, and C. Faloutsos, "Fraudar: bounding graph fraud in the face of camouflage," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 895–904, ACM, San Francisco, America, 2016.

[7] S. Sanober, I. Alam, S. Pande et al., "An enhanced secure deep learning algorithm for fraud detection in wireless communication," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6079582, 14 pages, 2021.

[8] M. Luo, X. Chang, L. Nie, Y. Yang, A. G. Hauptmann, and Q. Zheng, "An adaptive semisupervised feature analysis for video semantic recognition," *IEEE Transactions on Cybernetics*, vol. 48, no. 2, pp. 648–660, 2018.

[9] D. Zhang, L. Yao, K. Chen, S. Wang, X. Chang, and Y. Liu, "Making sense of spatio-temporal preserving representations for EEG-based human intention recognition," *IEEE Transactions on Cybernetics*, vol. 50, no. 7, pp. 3033–3044, 2020.

[10] K. Chen, L. Yao, D. Zhang, X. Wang, X. Chang, and F. Nie, "A semisupervised recurrent convolutional attention model for human activity recognition," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 5, pp. 1747–1756, 2020.

[11] Z. Li, X. Jin, C. Zhuang, and Z. Sun, "Overview on graph based anomaly detection," *Journal of Software*, vol. 32, no. 1, pp. 167–193, 2021.

[12] L. Ruff, R. A. Vandermeulen, N. Görnitz et al., "Deep semi-supervised anomaly detection," 2019, https://arxiv.org/abs/1906.02694.

[13] D. Eswaran, C. Faloutsos, S. Guha, and N. Mishra, "Spotlight: detecting anomalies in streaming graphs," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, pp. 1378–1386, ACM, London, UK, 2018.

[14] J. Li, H. Dani, X. Hu, and H. Liu, "Radar: residual analysis for anomaly detection in attributed networks," in *International Joint Conference on Artificial Intelligence (IJCAI)*, pp. 2152–2158, Melbourne, Australia, 2017.

[15] S. M. Erfani, S. Rajasegarar, S. Karunasekera, and C. Leckie, "High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning," *Pattern Recognition*, vol. 58, pp. 121–134, 2016.

[16] S. Thudumu, P. Branch, J. Jin, and J. Singh, "A comprehensive survey of anomaly detection techniques for high dimensional big data," *Journal of Big Data*, vol. 7, no. 1, pp. 1–30, 2020.

[17] Y. Li, N. Liu, J. Li, M. Du, and X. Hu, "Deep structured cross-modal anomaly detection," in *2019 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, IEEE, Budapest, Hungary, 2019.

[18] K. Shin, B. Hooi, and C. Faloutsos, "Fast, accurate, and flexible algorithms for dense subtensor mining," *ACM Transactions on Knowledge Discovery from Data*, vol. 12, no. 3, pp. 1–30, 2018.

[19] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and S. Y. Philip, "A comprehensive survey on graph neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 1, pp. 4–24, 2021.

[20] P. Cui, X. Wang, J. Pei, and W. Zhu, "A survey on network embedding," *IEEE Transactions on Knowledge and Data Engineering*, vol. 31, no. 5, pp. 833–852, 2019.

[21] J. Jiang, J. Chen, T. Gu et al., "Anomaly detection with graph convolutional networks for insider threat and fraud detection," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*, pp. 109–114, IEEE, Norfolk, USA, 2019.

[22] H. Wang, C. Zhou, J. Wu, W. Dang, X. Zhu, and J. Wang, "Deep structure learning for fraud detection," in *2018 IEEE International Conference on Data Mining (ICDM)*, pp. 567–576, IEEE, Sentosa, Singapore, 2018.

[23] M. Zheng, C. Zhou, J. Wu, S. Pan, J. Shi, and L. Guo, "FraudNE: a joint embedding approach for fraud detection," in *2018 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, IEEE, Rio de Janeiro, Brazil, 2018.

[24] Z. Liu, C. Chen, X. Yang, J. Zhou, X. Li, and L. Song, "Heterogeneous graph neural networks for malicious account detection," in *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*, pp. 2077–2085, ACM, Atlanta, USA, 2018.

[25] C. Liang, Z. Liu, B. Liu, J. Zhou, and X. Li, "Who stole the postage? Fraud detection in return-freight insurance claims," in *The 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco, America, 2018ACM.

[26] X. Wang, D. Bo, C. Shi, S. Fan, Y. Ye, and S. Y. Philip, "A survey on heterogeneous graph embedding: methods, techniques, applications and sources," 2020, https://arxiv.org/abs/2011.14867.

[27] Y. Zhang, Y. Fan, S. Hou, J. Liu, Y. Ye, and T. Bourlai, "Idetector: automate underground forum analysis based on heterogeneous information network," in *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 1071–1078, IEEE, Barcelona, Spain, 2018.

[28] Y. Fan, Y. Zhang, Y. Ye, and X. Li, "Automatic opioid user detection from Twitter: transductive ensemble built on different meta-graph based similarities over heterogeneous information network," in *International Joint Conference on Artificial Intelligence (IJCAI)*, pp. 3357–3363, Stockholm, Sweden, 2018.

[29] Z. Zhu, R. Li, M. Shan et al., "TDP: personalized taxi demand prediction based on heterogeneous graph embedding," in *Proceedings of the 42nd International ACM SIGIR Conference on*

Research and Development in Information Retrieval, pp. 1177–1180, ACM, Paris, French, 2019.

[30] L. Hu, C. Li, C. Shi, C. Yang, and C. Shao, "Graph neural news recommendation with long-term and short-term interest modeling," *Information Processing & Management*, vol. 57, article 102142, no. 2, 2020.

[31] L. Li, Z. Gan, Y. Cheng, and J. Liu, "Relation-aware graph attention network for visual question answering," in *Proceedings of the IEEE/CVF international conference on computer vision (ICCV)*, pp. 10313–10322, IEEE, Seoul, Korea, 2019.

[32] Y. Sun, J. Han, X. Yan, P. S. Yu, and T. Wu, "PathSim," *Proceedings of the Vldb Endowment*, vol. 4, no. 11, pp. 992–1003, 2011.

[33] C. Shi, X. Kong, P. Yu, S. Xie, and B. Wu, "Relevance search in heterogeneous networks," in *Proceedings of the 15th international conference on extending database technology (EDBT)*, pp. 180–191, ACM, Berlin, Germany, 2012.

[34] X. Kong, P. S. Yu, Y. Ding, and D. J. Wild, "Meta path-based collective classification in heterogeneous information networks," in *Proceedings of the 21st ACM international conference on Information and knowledge management*, pp. 1567–1571, ACM, Hawaii, USA, 2012.

[35] S. Fan, J. Zhu, X. Han et al., "Metapath-guided heterogeneous graph neural network for intent recommendation," in *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining*, pp. 2478–2486, ACM, Dublin, Ireland, 2019.

[36] B. Hu, Z. Zhang, C. Shi, J. Zhou, X. Li, and Y. Qi, "Cash-out user detection based on attributed heterogeneous information network with a hierarchical attention mechanism," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 33, pp. 946–953, 2019.

[37] A. Hosseini, T. Chen, W. Wu, Y. Sun, and M. Sarrafzadeh, "Heteromed: heterogeneous information network for medical diagnosis," in *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*, pp. 763–772, ACM, Atlanta, USA, 2018.

[38] C. Tang, X. Zheng, X. Liu et al., "Cross-view locality preserved diversity and consensus learning for multi-view unsupervised feature selection," *IEEE Transactions on Knowledge and Data Engineering*, 2021.

[39] Y. Zhang, J. Zhou, Z. Deng et al., "Multi-view fuzzy clustering approach based on medoid invariant constraint," *Journal of Software*, vol. 30, no. 2, pp. 282–301, 2019.

[40] S. Luo, C. Zhang, W. Zhang, and X. Cao, "Consistent and specific multi-view subspace clustering," in *Proceedings of the 32nd AAAI Conference on Artificial Intelligence*, pp. 3730–3737, AAAI, New Orleans, USA, 2018.

[41] D. Xia, Y. Yang, H. Wang, and S. Yang, "Late fusion multi-view clustering based on local multi-kernel learning," *Journal of Computer Research and Development*, vol. 57, no. 8, pp. 1627–1638, 2020.

[42] C. Tang, X. Zhu, X. Liu et al., "Learning a joint affinity graph for multiview subspace clustering," *IEEE Transactions on Multimedia*, vol. 21, no. 7, pp. 1724–1736, 2018.

[43] C. Tang, Z. Li, J. Wang, X. Liu, W. Zhang, and E. Zhu, "Unified one-step multi-view spectral clustering," *IEEE Transactions on Knowledge and Data Engineering*, 2022.

[44] F. Liu, K. Ting, and Z. Zhou, "Isolation-based anomaly detection," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 6, no. 1, pp. 1–39, 2012.

[45] J. Ren, X. Liu, Q. Wang, H. He, and X. Zhao, "An multi-level intrusion detection method based on KNN outlier detection and random forests," *Journal of Computer Research and Development*, vol. 56, no. 3, pp. 566–575, 2019.

[46] C. Hu and X. Qin, "Density-based local outlier detection algorithm DLOF," *Computer Research and Development*, vol. 47, no. 12, pp. 2110–2116, 2010.