doi:10.3772/j.issn.1006-6748.2020.03.003

Fraud detection on payment transaction networks via graph computing and visualization①

Sun Quan (孙 权)[*,**], Tang Tao②[*,**], Zheng Jianbin[**], Lin Jiale[***], Zhao Jintao[**], Liu Hongbao[**]
([*] School of Computer Science, Fudan University, Shanghai 200433, P. R. China)
([**] China UnionPay Research Institute of Electronic Payment, Shanghai 201201, P. R. China)
([***] School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, P. R. China)

Abstract

With the fast development of Internet technology, more and more payments are fulfilled by mobile Apps in an electrical way which significantly saves time and efforts for payment. Such a change has benefited a large number of individual users as well as merchants, and a few major players for payment service have emerged in China. As a result, the payment service competition becomes even fierce, and various promotion activities have been launched for attracting more users by the payment service providers. In this paper, the problem focused on is fraud payment detection, which in fact has been a major concern for the providers who spend a significant amount of money to popularize their payment tools. This paper tries the graph computing-based visualization to the behavior of transactions occuring between the individual users and merchants. Specifically, a network analysis-based pipeline has been built. It consists of the following key components: transaction network building based on daily records aggregation; transaction network filtering based on edge and node removal; transaction network decomposition by community detection; detected transaction community visualization. The proposed approach is verified on the real-world dataset collected from the major player in the payment market in Asia and the qualitative results show the efficiency of the method.

Key words: payment fraud detection, graph computing, graph embedding, machine learning

0 Introduction

Payment has been evolving to a new era whereby the mobile Apps have taken a dominant role in many emerging areas. There are multiple big giants for payment in China including Alipay, UnionPay, etc. With the propensity of the payment mobile Apps, more and more individual users, merchants, and other players have entered this area, many persons are benefiting from the advanced and convenient mobile payment technology and business.

As a matter of fact, the payment giants have spent large amounts of investment in promoting their payment tools and one of the main promoting ways is to give discount or back cash to individuals who use their payment Apps when do purchase. The payment can either be fulfilled by online and offline, while the online especially mobile Apps are becoming the major channel to attract the public to get used to the new payment habit. The promotion naturally incurs the attackers including both individual users and merchants that take advantage of the promotion events to obtain extra rewards in an unjustified way. For example, the users may intentionally repeat 10 purchase on the same goods in a merchant, which can, in turn, get back cash from the payment service provider, and the user may share this reward with the merchant. In fact, such fraud has become the major concern for payment campaign, which can cause significant loss to payment service providers. As a result, how to effectively detect the underlying fraud makers (including both individual users and merchants) has been a hot research topic in literature, though many focused on other relevant but different domains. This work also focuses on this important problem, and conducts the empirical study on a major payment service provider in China, to verify the idea and the proposed technical approach. In general, this paper aims to make the following highlights:

- A graph computing-based approach is proposed

① Supported by the National Natural Science Foundation of China (No. 61972250), National Key Research and Development Program of China (No. 2018AAA0100700, 2016YFB1001003) and the Program of Shanghai Academic/Technology Research Leader (No. 19XD1433700).
② To whom correspondence should be addressed. E-mail: tangtao2@unionpay.com
Received on Sep. 18, 2019

for payment fraud detection, particularly in the setting of mobile Apps payment tools. The proposed approach is unsupervised and can work on large-scale transaction networks, whereby the nodes denote both individual users and merchants, and the edges denote the transaction records.

- Specifically, the proposed approach consists of the 2 main steps: the first step is to use graph computing to break the giant network into small communities, and the second step is to adopt data visualization to help the investigators pinpoint the risk nodes and edges in a certain time period.
- Case study with preliminary experimental results is provided on the real-world dataset from a major payment player in China. The results show that the proposed approach can effectively detect suspicious frauds on large-scale payment networks.

The rest of the paper is organized as follows. This paper discusses the related work in Section 1. The major technical approach based on network analysis is presented in Section 2. Case study and preliminary experiments are given in Section 3. Conclusion is in Section 4.

1 Related work

In this section, related work on fraud detection is presented. In particular, the review will cover different business area for fraud detection as well as the technical approaches including both supervised and unsupervised learning-based methods.

1.1 Fraud detection business requirements

Fraud detection has been a long standing task in financial related business. It ranges across multiple industry sectors and researchers from different disciplines have devoted considerable efforts.

One major business scenario is credit card fraud detection, whereby unlawful transactions by credit cards need be timely detected. Ref. [1] studied the fraudulent credit card transactions occurring among the retail companies in Chile whereby the association rule method is employed. In Ref. [2], the fraud detection score was specially focused to transform it to a probability, which is important for decision making in credit card risk management. Another typical and important sector is automobile. Ref. [3] proposed an expert detection system against the group of collective automobile insurance fraudulent activities. The entities involved in the car insurance fraud can be drivers, chiropractors, garage mechanics, lawyers, police officers, insurance workers and others. In the more recent Ref. [4] showed the fraud detection experience on large-scale e-commerce platforms, based on Alibaba's large-scale computing system called Open Data Processing Service (ODPS). An anti-fraud system has been developed and verified on 2 large e-commerce datasets with the size of tens of millions of users and items, which is further deployed to Alibaba's online business Taobao. Fraud can also happen in the online customer reviews, which are assumed to be unbiased opinion of other consumers' experiences with the items or services. In fact, it is possible that the publishers, writers and vendors consistently manipulate online consumer reviews. And these manipulations can incur significant bias to the potential buyers such that the customers may purchase goods under misleading. To address this issue, Ref. [5] analyzed typical patterns of review manipulation and provided an empirical study on the real-world data from Amazon and Barnes & Noble. For telecom fraud detection, it has been a serious problem in many developing countries, e. g. China, and it is rather difficult to coordinate multiple agencies to avoid fraudulent activities thoroughly. Thus machine learning methods are applied in Ref. [6] to detect the fraudsters. More specifically, they proposed to use generative adversarial network (GAN)[7] based model to estimate the likelihood of a fraud transaction, as such the bank can take some measures to prevent monetary loss. The GAN based model shows promising results against traditional supervised learning models. In the setting of healthcare service, fraud detection has also been a central issue especially given the trend that more and more online payment channels are becoming available. For instance, Ref. [8] disclosed the typical online healthcare service delivery process in China. The fraudsters i. e. third party agents use software robots and script to obtain hospital appointments from the authorized platforms, and then the agents ask for unjustified high price to resell them to the true clients. To tackle this problem, they first use clustering based models to discover the potential user groups from agents, then the profile of user groups are extracted from the event sequence of the users to provide evidence for fraud detection. Moreover, a case study is deployed in a real-world hospital to show its effectiveness and reliability.

On the other hand, unsupervised models are developed and used for fraud detection, partly due to the lack of labeled samples for training an effective supervised model. Among them, clustering[9,10] is a mainly used technique. The clustering is usually performed on the user profiles to help identify the abnormal users, and the recent advance of deep network-based cluste-

ring techniques[11] can be of more help in this direction.

There are also some technically relevant work on abnormal detection and prediction. For temporal data, Ref. [12] showed a dictionary learning-based model for robust time series anomaly detection. While a more recent work[13] showed failure prediction using both event sequence and time series data. However, this technique can be difficult to be applied in the setting. The main reason is that fraudulent transactions at the individual level are a rare event, which can hardly form a long sequence of events across a long-time period, and so for time series. In addition, it is useful to predict fraud detection rather than detection after fraudulent transactions have happened. In this sense, the early risk prediction model of fraudulent transactions are needed, and there are also a line of work[14-17] on event prediction over time, based on statistical learning models. These directions involving more complicated models are left for future study, given more data can be collected as the business spans.

1.2 Fraud detection technologies

From the technical perspective, fraud detection has been a challenging task partly due to the fact that the supervised learning-based models call for enough positive samples including transactions, client individuals and merchants, in comparison with the normal samples. However, in fact, many frauds may happen without being detected hence the positive samples are often a subset of the true whole fraud samples set. This leads to the following problems: 1) the distribution of the positive samples (fraud) and negative samples can be biased; 2) the number of positive samples becomes even smaller as some are not detected, especially compared with those unlimited number of normal samples.

In literature, different methods are adopted for fraud detection in both supervised and unsupervised learning based ways. When supervision is given, as 2 rather popular machine learning methods, support vector machine (SVM) and Logistic regression (LR) have been applied in fraud detection. While in reality, supervision information is often difficult to acquire, in such cases, unsupervised methods have attracted lots of attention whereby clustering methods have been the dominant techniques.

1.3 Remarks

As discussed above, though fraud detection has been a long-standing problem in different financial areas while the study in the context of mobile payment Apps has not been fully explored. In particular, it is an emerging area and China has been one of the major countries for payment tools promotion. Hence it is motivated to take an in-depth study based on real-world business need (as one of the biggest payment players in the world) and rich transaction-related data. In the subsequent sections, a model based on network analysis whereby graph computing has been applied is proposed and case studies are given in detail.

2 Graph computing based approach for fraud detection

In this section, the graph computing based pipeline for fraud detection for unjustified profits will be discussed. The deployed method for building the transaction graph will be first described, whereby the graph computing procedure can be performed. This section also briefly discusses other alternative techniques that have been tried while not really adopted for stability and computational tractability issues.

2.1 Transaction network construction and processing

In the approach, the transaction network for the payments on a daily basis is built. An overview working flow of the transaction network processing and visualization is shown in Fig. 1. The input transaction data is used to build the transaction network first, which is followed by filtering to remove some unimportant edges and nodes. Then community detection e. g. fast-unfolding (Fig. 2) is performed to narrow down the study on relatively small communities. In the final stage, there are multiple ways of further analysis, including graph embedding (Fig. 3), and rule driven community visualization (Fig. 4) for fraud detection.

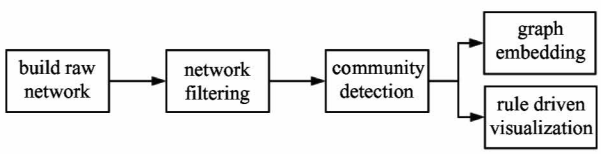


Fig. 1 Working flow of the transaction network processing and visualization

2.1.1 Transaction network construction

Specifically, when there are multiple transactions in one day for a pair of nodes, e. g. between a user and a merchant, these transactions will be aggregated into one edge (or 2 directed edges if the direction is considered), whose attributes store the average transaction amount, mean transaction time, mean transaction between time, and the total number of transactions (in one direction). Note the above statistics can also

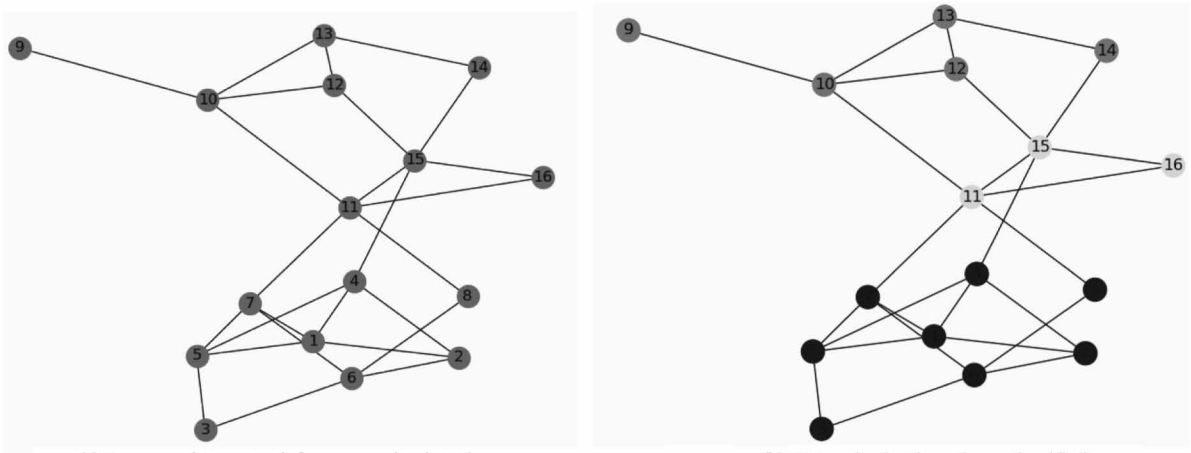


Fig. 2 Illustration for network community detection e. g. via FastUnfolding[18]. The input raw network has been divided by the 3 detected communities by the FastUnfolding method

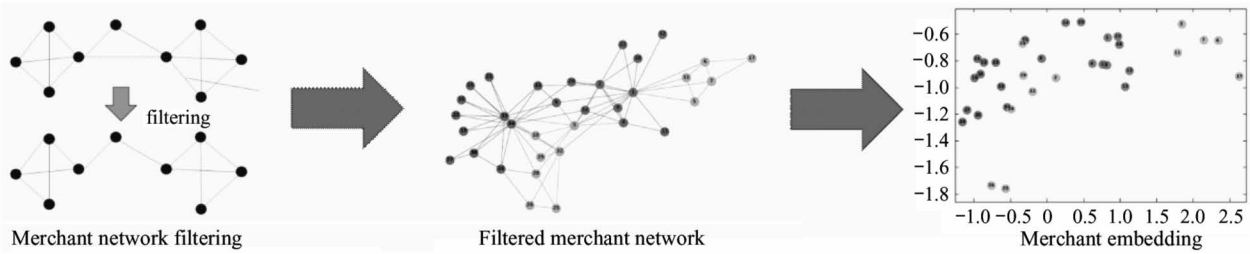


Fig. 3 Network embedding on the detected community using node2vec[19] for merchants' transaction networks

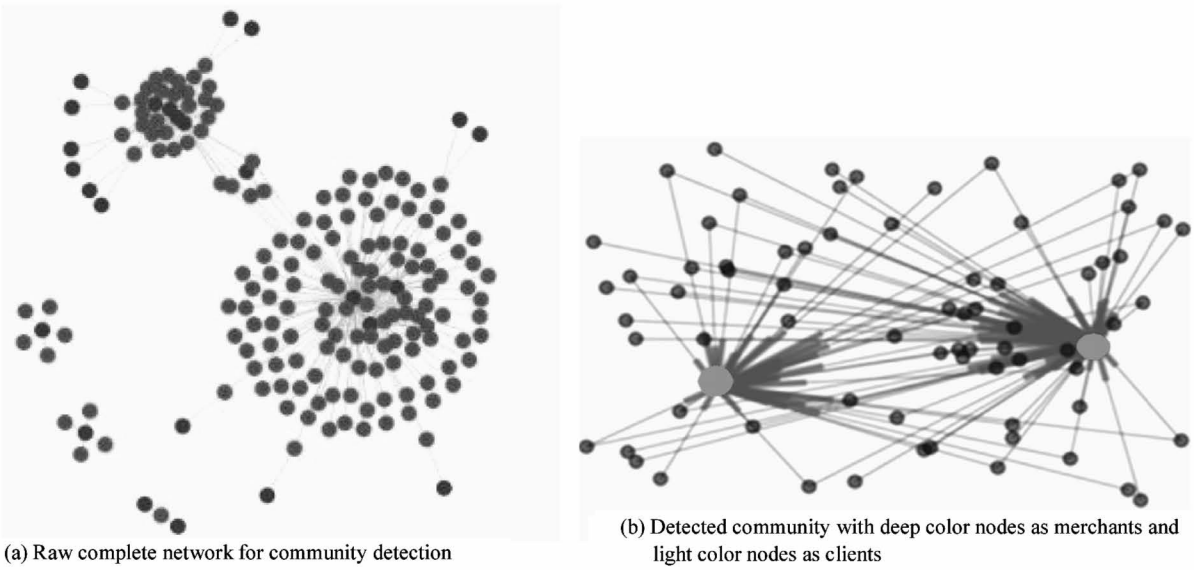


Fig. 4 Network visualization and rule checking based on the detected community from the raw networks

be conducted on a longer period than one day, e. g. one week or month, which can be applied dependently.

2.1.2 Transaction network filtering

Then filtering is performed on the formed (aggregated) transaction network, whereby the typical filtering criterion includes the total transaction count, amount, discount, and the between time. The purpose of filtering is to reduce the size of the network by sparsifying its edges and removing some less important nodes. As such the whole network can be cut into a collection of sub-networks, each of which is of a reasonable size for further processing. The filtering mainly involves 2 steps: the first step is to remove the edges

whose attributes as stated above are smaller than given thresholds. The nodes with a very limited number of out/in degrees will also be removed in the second step.

2.2 Fast community detection

Community detection can be applied on the filtered network as shown in Fig. 2, to further break down the large-scale network into small sub networks. As such, more sophisticated measurements can be computed within a reasonable time period to quickly detect the risks. There are many available community detection algorithms, of which one popular method is FastUnfolding[18]. Here is a detailed description of FastUnfolding, whereby the modularity score Q is defined as follows:

$$Q = \frac{1}{2m}\sum_{i,j}[A_{i,j} - \frac{k_i k_j}{2m}]\delta(c_i, c_j) \quad (1)$$

where i and j indicate the 2 nodes in the network, and $A_{i,j}$ denotes the weight between the 2 nodes. While c_{ij} denotes the community ID that a node is tagged, and the delta function $\delta(c_i, c_j)$ returns 1 if the 2 nodes are assigned to the same community; otherwise it is set 0.

- Initialization: label each node to different communities;
- For each node, label it to the community that one of its neighboring nodes belongs to, such that the corresponding modularity score by Eq. (1) is maximized. Then the difference ΔQ compared with the original modularity score is calculated;
- If $\Delta Q > 0$, accept the latest community division; otherwise, keep the original division;
- Repeat the above steps until the modularity score Q cannot be improved anymore.

2.3 Detected community embedding and visualization

One popular method is to embed the community network into vectorized feature representation, for which the scalability issue need be particularly addressed for real-world applications. In fact, there are many new network embedding methods[19-21] which can convert graph vertex into a vectorized feature points in the new space. As such, traditional machine learning methods such as support vector machine, logistic regression and decision tree can be easily reused.

Another direct and powerful method for fraud detection based on the detected communities is visualization as will also be shown in the case studies. In general, in the detected community, the scale of the graph as well as the edge density is relatively small, hence it is easier to do graph visualization, whereby the bank card accounts and merchants can be shown in different colors to help the investigators quickly discern the abnormal patterns.

3 Experiments and case study

In this section, case study and preliminary experimental results on real-world payment data are provided. The data is collected from the major payment service player in China whose registered users have surpassed the number for 2 billion, and every day there are around 3 million transactions. In the proposed approach, the large-scale transaction network has been formed and graph based computing methods are used to detect the potential fraudsters. In consequence, subsequent followups can be taken to further verify the illness of the detected fraudsters.

3.1 Platform infrastructure

As the platform needs to support large-scale and efficient (sometimes even real-time) computing and storage, distributed system is used based on popular tools including Hadoop, HIVE, etc. The general overview of the infrastructure system is shown in Fig. 5. The data is updated on a daily basis, whereby the daily records are stored on their respective nodes to ensure fast access and consistency. In addition, because the HIVE data warehouse is not friendly to interactive SQL query, the tool Impala is used for the more efficient query, which can achieve a speedup about 10 times.

3.2 Protocol

The proposed heterogeneous network involves individual users, merchants, as well as bank card for redistribution of the earned unjustified (monetary) credits.

3.3 Preliminary qualitative results

The network has been built by the definition of entities and their relationships. Then some particular sub networks can be visualized. Fig. 6 shows 4 typical cases for fraudulent conspiracy among the merchants, individual users with their payment account and the bank card for monetary redistribution. More specifically:

- In Fig. 6(a), there are 2 central merchants (in light color) to which many payment transactions have been conducted from a large number of individual users (in dark color), and it can be easily discovered that these 2 merchants have high risk for fraudulent behavior and appropriate measures can be taken to perform further investigation on the 2 merchants and the relevant individual accounts.
- In Fig. 6(b), many individual users pay to the

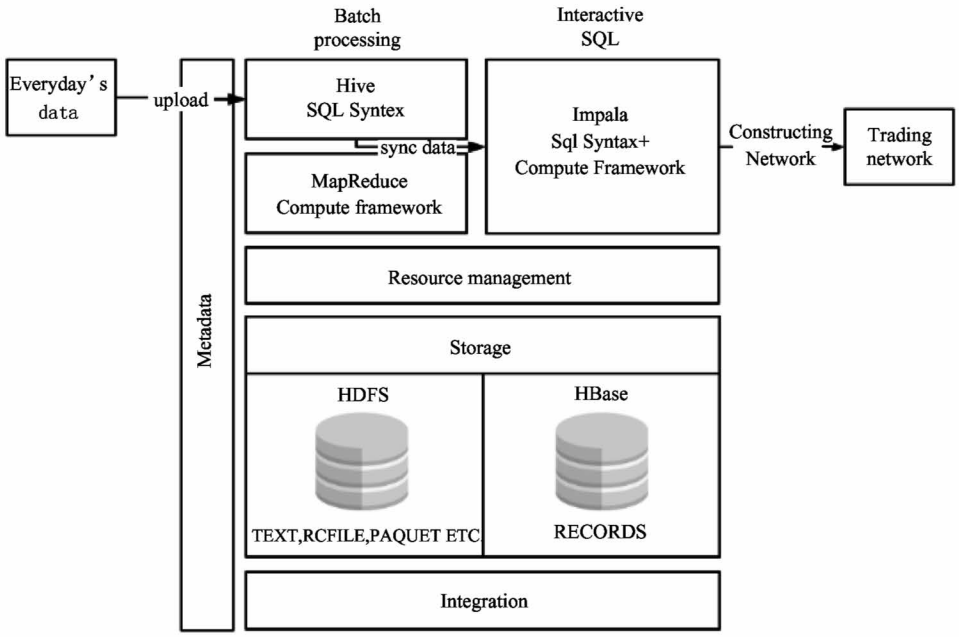
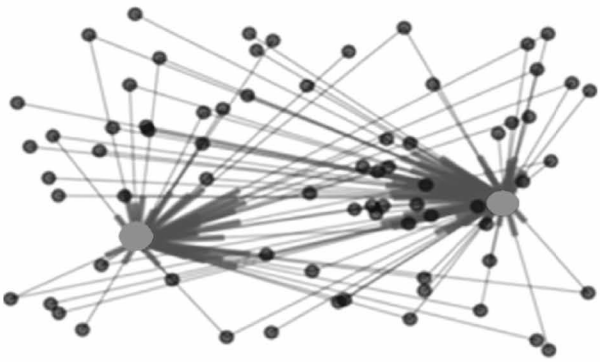
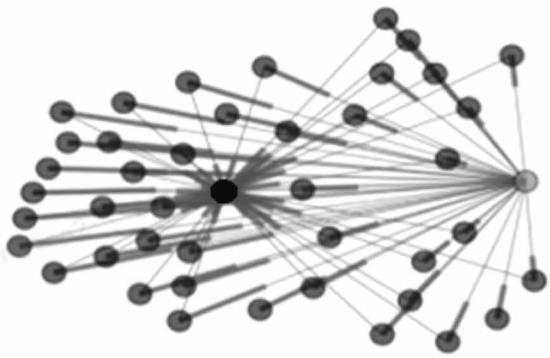


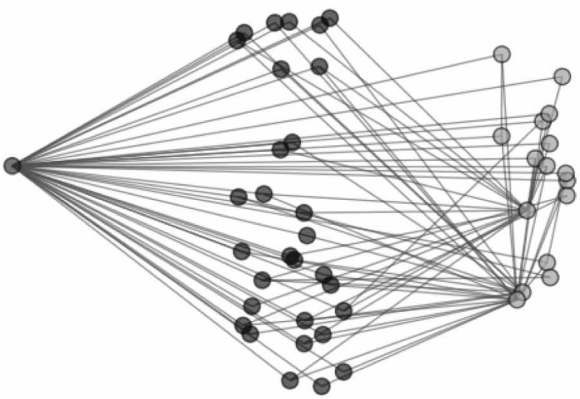
Fig. 5 Overview of the infrastructure system for graph computing based fraud detection on the transaction network



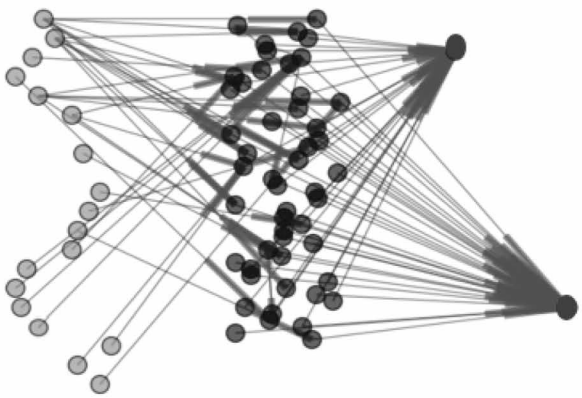
(a) Two fraudulent merchants (in light color) and their associated users(in deep color), best viewed in color



(b) Fraudulent patterns by the suspect single bank card for money redistribution (in light color), the users (in deep color) and the merchant (in black)



(c) Fraudulent patterns by the suspect multiple bank cards for money redistribution (in right nodes), the users (in midnodes) and the merchant (in left nodes)



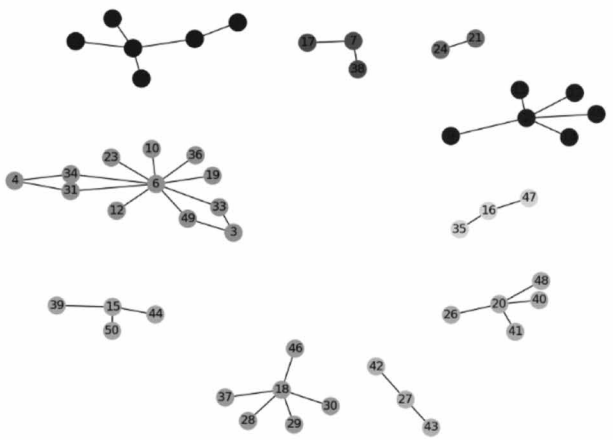
(d) Group fraudulent patterns formed by the suspect redistribution bank cards (in left nodes), the users (in midnodes) and the merchant (in right nodes)

Fig. 6 The typical fraud pattern among the merchants, individual users and card accounts. These entities form a network which is typically very large and frequently changed in reality making fraud detection more challenging

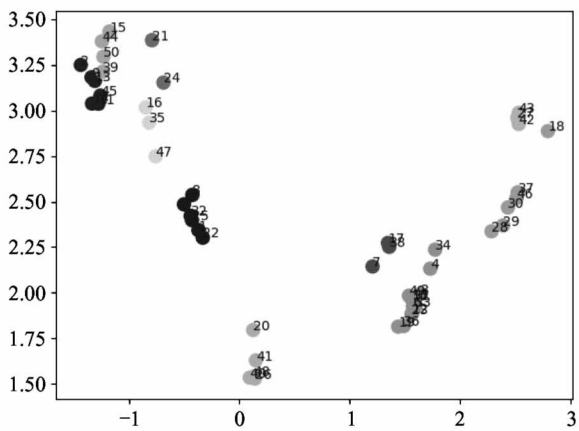
merchant at the promotion period, such that they receive discount or backcash from the payment service provider. And the merchant gets back the unjustified fraud money from the users by a certain ratio, e. g. 50 percentages.

- While in the example of Fig. 6(c), there is no explicit merchant in the network, while the bank cards have an active link with many shared users in a short time period. This suggests the potential fraud group among these entities, such that the earned backcash may be redistributed through this network.
- In the 4th example as shown in Fig. 6(d), there are also only 4 merchants which have attracted many transactions within a group of users. In addition, there are multiple bank cards for redistribution of the money, this scenario is often more difficult to detect as more entities are involved.

The network embedding using the node2vec method[19] on a segmented network of merchants is also used. In this way, each merchant is represented by a feature vector. For the convenience and effect of the display, 50 merchants and their associated users project their feature representation further into the 2D plane. The edges in the projected network are created by certain means of the common clients shared by the 2 merchants (when the number exceeds a certain threshold). As shown in Fig. 7, on the left, the raw network shows multiple clustering pattern regarding connected components, and such clustering behavior is well preserved in the projected 2D space on the right. This result shows the effectiveness of the adopted node2vec method.



(a) The input networks with 10 connected components in different colors



(b) The projection on 2D plane from the embedded feature representation of each node using node2vec[19]

Fig. 7 A typical example of the projection of multiple connected components of a raw network by node embedding

3.4 Summary and discussion

This paper gives 4 typical cases of fraud pattern which are extracted from a series of network processing including raw transaction network construction based on daily records aggregation, transaction network decomposition based on edge and node filtering and community detection to focus on suspicious networks based on data visualization.

4 Conclusions

This paper proposes a principled and effective approach for automatic payment fraud detection in the context of individuals and merchants, whereby a payment transaction network can be established for further analysis of the payment behavior to find suspicious fraud transactions and their latent individuals and merchants in an unsupervised learning manner.

Specifically, this paper develops a network analysis method to discover the abnormal patterns of transactions over the network in a certain period of time. The design is based on the fact that little labeled data samples are available and there also lacks systematic rules for summarizing the behavior of fraud.

There are many possible directions for future work. First, in this paper, an unsupervised approach is mainly adopted due to the lack of labels for fraud merchants and individuals. While as the data accumulates, more labels can be obtained and then it is possible to develop supervised learning methods such as decision tree and deep neural networks. Second, fusing multiple networks with different definitions to form a more effective detection pipeline is future direction. For this need, graph matching, especially for multiple graph matching[22,23], and online graph matching[24], can be a possible solution infusing networks with corresponding structures. Third, recently there are many temporal models for behavioral modeling, and one of

the promising technique is the so-called temporal point process[25]. A variety of temporal point process models has been witnessed, ranging from classic parametric models[14] to nonparametric models[26] and to deep network based approaches[27-29]. What's more, combining two-way exploration[30], GAN[31] with the proposed method is one of the future directions. Last but not least, how to learn an interpretable behavioral model[32,33] over time is also the immediate interest.

References

[1] Sánchez D, Vila M A, Cerda L, et al. Association rules applied to credit card fraud detection[J]. *Expert Systems with Applications*, 2009, 36(2): 3630-3640

[2] Bahnsen A C, Stojanovic A, Aouada D, et al. Improving credit card fraud detection with calibrated probabilities [C]// Proceedings of the 2014 SIAM International Conference on Data Mining, Philadelphia, USA, 2014: 677-685

[3] Šubelj L, Furlan Š, Bajec M. An expert system for detecting automobile insurance fraud using social network analysis[J]. *Expert Systems with Applications*, 2011, 38(1): 1039-1052

[4] Weng H, Li Z, Ji S, et al. Online e-commerce fraud: a large-scale detection and analysis[C]//2018 IEEE 34th International Conference on Data Engineering (ICDE), Paris, France, 2018: 1435-1440

[5] Hu N, Liu L, Sambamurthy V. Fraud detection in online consumer reviews[J]. *Decision Support Systems*, 2011, 50(3): 614-626

[6] Zheng Y J, Zhou X H, Sheng W G, et al. Generative adversarial network based telecom fraud detection at the receiving bank[J]. *Neural Networks*, 2018, 102: 78-86

[7] Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets[C]// Advances in Neural Information Processing Systems, Montréal, Canada, 2014: 2672-2680

[8] Xie C, Cai H, Yang Y, et al. User profiling in elderly healthcare services in China: scalper detection[J]. *IEEE Journal of Biomedical and Health Informatics*, 2018, 22(6): 1796-1806

[9] Bekirev A S, Klimov V V, Kuzin M V, et al. Payment card fraud detection using neural network committee and clustering[J]. *Optical Memory and Neural Networks*, 2015, 24(3): 193-200

[10] Hilas C S, Mastorocostas P A, Rekanos I T. Clustering of telecommunications user profiles for fraud detection and security enhancement in large corporate networks: a case study[J]. *Applied Mathematics & Information Sciences*, 2015, 9(4): 1709

[11] Xu H, Li Z, Chu C, et al. Detecting and characterizing web ot traffic in a large E-commerce marketplace[C]// European Symposium on Research in Computer Security, Barcelona, Spain, 2018: 10. 1007/978-3-319-98989-1_8

[12] Yan J C, Tian C H, Huang J, et al. Incremental dictionary learning for fault detection with applications to oil pipeline leakage detection[J]. *Electronics Letters*, 2011, 47(21): 1198-1199

[13] Xiao S, Yan J, Farajtabar M, et al. Learning time series associated event sequences with recurrent point process networks[J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2019, 30(10): 3124-3136

[14] Yan J, Wang Y, Zhou K, et al. Towards effective prioritizing water pipe replacement and rehabilitation[C]// 23rd International Joint Conference on Artificial Intelligence, Beijing, China, 2013: 2931-2937

[15] Yan J C, Xiao S, Li C S, et al. Modeling contagious merger and acquisition via point processes with a profile rgression prior[C]// International Joint Conference on Artificial Intelligence, New York, USA, 2016: 2690-2696

[16] Liu X, Yan J, Xiao S, et al. On predictive patent valuation: forecasting patent citations and their types[C]// 31st AAAI Conference on Artificial Intelligence, San Francisco, USA, 2017: 1438-1444

[17] Yan J, Liu X, Shi L, et al. Improving maximum likelihood estimation of temporal point process via discriminative and adversarial learning[C]// Proceedings of the 27th International Joint Conference on Artificial Intelligence, Stockholm, Sweden, 2018: 2948-2954

[18] Blondel V D, Guillaume J L, Lambiotte R, et al. Fast unfolding of communities in large networks[J]. *Journal of Statistical Mechanics: Theory and Experiment*, 2008(10): P10008

[19] Grover A, Leskovec J. node2vec: scalable feature learning for networks[C]// Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, USA, 2016: 855-864

[20] Perozzi B, Al-Rfou R, Skiena S. Deepwalk: online learning of social representations[C]//Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, New York, USA, 2014: 701-710

[21] Tang J, Qu M, Wang M, et al. Line: large-scale information network embedding[C]//Proceedings of the 24th International Conference on World Wide Web, Florence, Italy, 2015: 1067-1077

[22] Yan J, Wang J, Zha H, et al. Consistency-driven alternating optimization for multigraph matching: a unified approach[J]. *IEEE Transactions on Image Processing*, 2015, 24(3): 994-1009

[23] Yan J, Cho M, Zha H, et al. Multi-graph matching via affinity optimization with graduated consistency regularization[J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2015, 38(6): 1228-1242

[24] Yu T, Yan J, Liu W, et al. Incremental multi-graph matching via diversity and randomness based graph clustering[C]//Proceedings of the European Conference on Computer Vision (ECCV), Munich, Germany, 2018: 139-154

[25] Daley D J, Vere-Jones D. An Introduction to the Theory of Point Processes: Volume II: General theory and Structure[M]. Berlin: Springer Science & Business Media, 2007

[26] Lewis E, Mohler G. A nonparametric EM algorithm for multiscale Hawkes processes[J]. *Journal of Nonparametric Statistics*, 2011, 1(1): 1-20

[27] Du N, Dai H, Trivedi R, et al. Recurrent marked temporal point processes: embedding event history to vector[C]//Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, USA, 2016: 1555-1564

[28] Xiao S, Yan J, Yang X, et al. Modeling the intensity function of point process via recurrent neural networks [C]//31st AAAI Conference on Artificial Intelligence, San Francisco, USA, 2017: arXiv: 1705.08982v1

[29] Xiao S, Farajtabar M, Ye X, et al. Wasserstein learning of deep generative point process models[C]//Advances in Neural Information Processing Systems, Long Beach, USA, 2017: 3247-3257

[30] Zhang X Y, Wang S P, Yun X C. Bidirectional active learning: a two-way exploration into unlabeled and labeled data set[J]. *IEEE transactions on Neural Networks and Learning Systems*, 2015: 10. 1109/TNNLS. 2015. 2401595

[31] Zhang X Y, et al. Active semi-supervised learning based on self-expressive correlation with generative adversarial networks[J]. *Neurocomputing*, 2019(345): 103-113

[32] Li L, Yan J, Yang X. Learning interpretable deep state space model for probabilistic time series forecasting[C]//Proceedings of the 28th International Joint Conference on Artificial Intelligence, Macao, China, 2019: 2901-2908

[33] Zhang X Y, Shi H, Li C, et al. Learning transferable self-attentive representations for action recognition in untrimmed videos with weak supervision[C]//Proceedings of the 33rd AAAI Conference on Artificial Intelligence, Hawaii, USA, 2019: 9227-9234

Sun Quan, born in 1978. He received the B. S. degree from National University of Defense Technology, Hunan, China in 1996 and the M. S. degree from Fudan University, Shanghai, China in 2004. His research interests include risk prevention and control, cloud computing, electronic payment and e-commerce.