PD-FDS: Purchase Density based Online Credit Card Fraud Detection System

Youngjoon Ki HACKER@KOREA.AC.KR
and **Ji Won Yoon** JIWON_YOON@KOREA.AC.KR
Korea University

Abstract

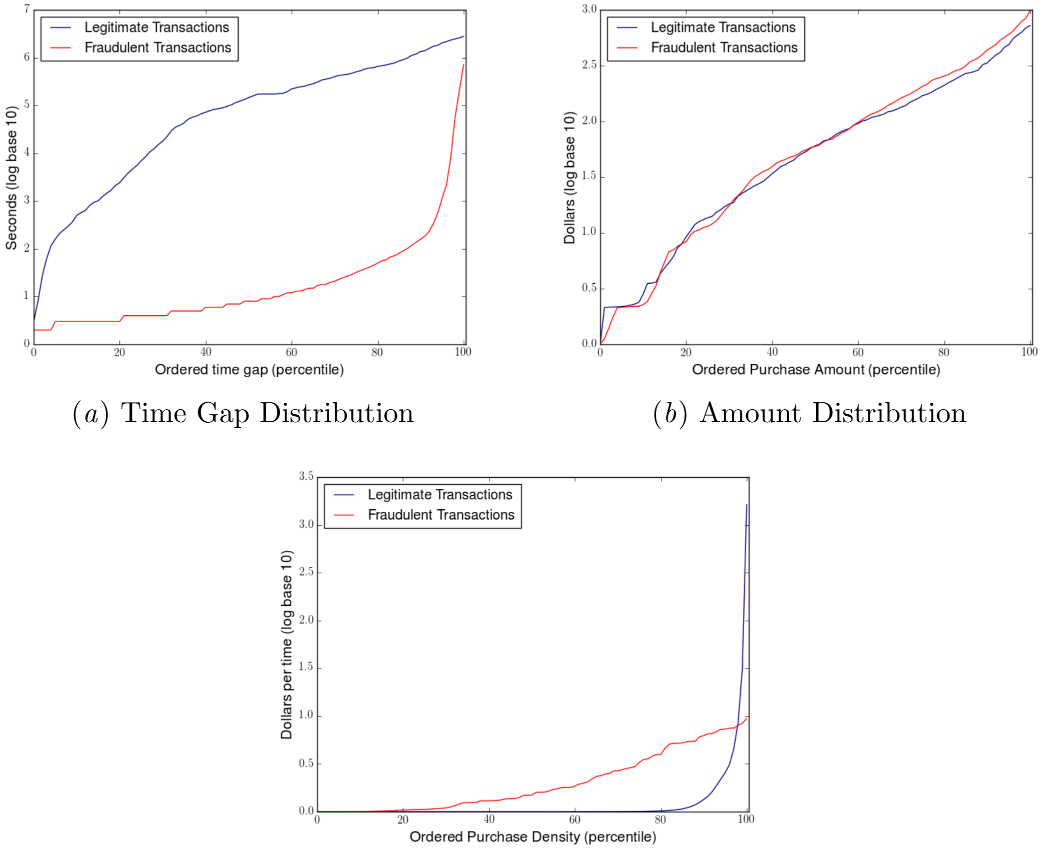
Credit card fraud detection is an endless war between fraudsters and payment service providers. Indeed, annual global financial loss by credit card frauds has increased. Fraudsters have been organized and systematized, attempting to find weak points of existing fraud detection system (FDS). State-of-the-art FDS approaches utilize already existing fraud cases, which can result in different FDS by payment service providers. Therefore, a new payment service provider may not have room for installing a FDS due to the lack of fraudulent cases. Moreover, credit card transactions contain the legitimate owner's personal information, which can be exposed to an honest but curious fraud analyst. In this paper, we propose a purchase density based FDS (PD-FDS) that uses three features which are not related to personal information. PD-FDS does not require already existing fraudulent transactions and also shows low false positive rate (<0.01).

Keywords: Credit Card Fraud Detection, Unsupervised Learning, Poisson Process

1. Introduction

The credit card is gradually replacing the use of cash in most places through its convenience. With the increase of popularity, the global loss to credit card fraud is also increasing. According to a survey (Nilson, 2015), $21.84 billion dollars are misused by worldwide credit card frauds in 2015. Moreover, the global financial loss of credit card fraud has increased already, and the fraudsters have become systematized and organized (Forster, 2015). Likewise, fraudsters will target the weak point of monitoring (Forster, 2015) disguising their purchase patterns to be seen as legitimate transactions. Indeed, fraudulent transactions show similar patterns with legitimate transactions (Kim and Kim, 2002; Maes et al., 2002; Seeja and Zareapoor, 2014). This implies that FDS can cause high false negative or high false positive rates. False positives occur when a payment service provider fails to catch positive (fraudulent) transactions. Accordingly, the false negative rates are related to the payment service provider's financial loss by frauds. On the other hand, the high false positive rates are related with both administrative cost (Bahnsen et al., 2013) and customer inconvenience (Panigrahi et al., 2009) which might lead the customer to leave the card company. These cost of customer inconvenience is difficult to evaluate but still important to payment service providers. In this study, we propose three versions of FDS by choosing when the FDS blocks the fraudulent transaction. The result shows that false positives range from 0.01 to 0.00005, and it can be chosen by a payment service provider's policy.

Contribution We suggest a purchase density based fraud detection system (PD-FDS) which uses an unsupervised learning method Moreover, PD-FDS does not require personal information such as location, age or income. Instead, it only utilizes three features: time, amount, and merchant type, which are not enough to identify the legitimate owners. Lastly, PD-FDS shows low false positive rate (< 0.01) in the worst case .



(a) Time Gap Distribution

(b) Amount Distribution

(c) Purchase Density Distribution

Figure 1: Exploratory data analysis results

2. Related Work

Various credit card fraud detection approaches are based on supervised learning algorithms such as artificial neural network (ANN), logistic regression, support vector machines (SVMs) or random forests. Among various approaches, random forests have shown the highest detection accuracy (Whitrow et al., 2009; Bahnsen et al., 2016; Bhattacharyya et al., 2011; Bahnsen et al., 2015; Dal Pozzolo et al., 2014). However, supervised learning approach is rather data-dependent since its classifier is built based on the existing fraudulent cases. This approach may not be suitable to a new payment service provider who does not have enough fraudulent transactions. Moreover, different dataset would induce different types of

FDS. This indicates that each company would have different FDS because fraudulent cases are difficult to be shared due to the users' privacy issues.

On the other hand, approaches based on unsupervised learning focus on user behaviors. It is possible to detect frauds with the greatest accuracy by using user behavior patterns (Edge and Sampaio, 2009). Moreover, unsupervised learning approaches assume that the legitimate users' pattern has a boundary of normal behavior, and the transaction is regarded as abnormal if a transaction exceeds the boundary. Zaslavsky and Strizhak (2006), Quah and Sriganesh (2008) and Olszewski (2014) introduced approaches to cluster users' pattern using self-organization map (SOM). In SOM based approaches, each user's transaction pattern can be described in 2-dimensional space, and the abnormal transactions locate far from normal transactions.

PD-FDS is an unsupervised learning based approach which uses each user's purchase history. We expect that our approach can be utilized as a prior knowledge for detecting fraudulent transactions by a new payment service providers who do not have enough fraudulent cases.

3. Background

In this section, we briefly explain the types of credit card frauds. In addition, we introduce the concept of Poisson process and how to define risk probability.

3.1. Type of Credit Card Frauds

There are three major types in credit card frauds which have different aspects as follows:

- **Lost Card** : Fraudsters acquire a credit card by chance.
- **Stolen Card** : Fraudsters steal a credit card on purpose. This type of fraud includes pickpocketing, skimming and account takeover.
- **Forged Card** : Fraudsters counterfeit an application to issue a credit card with a legitimate owner's identification.

The three types of frauds occupy more than 97% of financial loss by frauds in France, UK and Canada (Forster, 2015). There are more types of frauds (Jha and Westland, 2013) but we do not consider in this study.

3.2. Poisson Process

The Poisson process is a well-known probabilistic modeling method to measure the probability of the number of events $N(t)$ in time t. In the process, the probability that event happens n times follows Poisson distribution of parameter λt, where λ is the average number of events when $t = 1$. That is, $P\{N(t) = n\} = \frac{(\lambda t)^n e^{-\lambda t}}{n!}$. In this study, we regard the event as the amount of purchase $A(t)$, and t indicates the time interval between transactions. Accordingly, the average amount λ can be obtained from the before transactions.

4. Methodology

In this section, we introduce three major features to distinguish fraudulent transactions. Moreover, we propose three objectives we aim at to design FDS. Lastly, the measure of risk is explained using Poisson process.

4.1. Key Features to Detect Fraud

Comparing with legitimate transactions, fraudulent transactions have three different features. We explain the features based on a real data set from a Korean payment service provider. The dataset contains 6.8 millions of legitimate online credit card transactions and 3,399 fraudulent transactions for three months. The fraudulent cases in the dataset were labeled by customer report or the payment service provider's investigation. In addition, online purchase is also known as Card Not Present (CNP) such as 'key in' method.

4.1.1. Time Gap

Fraudsters would try to exploit profit as many as possible while the legitimate owner does not notice. Since the fraudsters do not know the credit limit of the card owner, they would attempt to purchase a lot of items during short period before the card is blocked. Figure $1(a)$ shows that fraudulent transactions have shorter time gap on average than legitimate transactions. This implies that fraudsters tend to hurry to gain illegal profit.

4.1.2. Amount

Amount of money can be another important feature since the fraudsters would have a tendency to buy more expensive things than legitimate users. However, Figure $1(b)$ shows that fraudulent transactions have similar patterns with legitimate patterns. This implies that the amount itself cannot be a good feature to distinguish fraudulent transactions. As we can see in Figure $1(c)$, purchase density can distinguish fraudulent transactions and legitimate transactions. In the figure, fraudulent transactions show higher purchase density averagely than legitimate transactions. Thus, amount has to be combined with the time gap to become a meaningful feature.

4.1.3. Merchant Category

Merchant category is also an important feature to differentiate fraudulent transactions since the level of user identification at the merchant is different. For instance, when we purchase a flight ticket, we have to provide passport information to identify ourselves. However, we do not always have to hand over identification card in a convenience store. We list merchant categories which require additional identification as below.

- Educational Services
- Airlines
- Tax, Government Services

The merchants have a common feature that the average of paid amount is high, which can occur high purchase density. In this study, we regard the listed merchant categories are legitimate transactions despite of the high purchase density since it always requires additional identification methods. Actually, fraudulent transactions were found in almost every merchant in our dataset. This indicates that frauds can occur in every kind of merchant which do not strictly check the users' identification.

4.2. Objective

In this section, we explain four important objectives to design FDS. The objectives are as follows:

4.2.1. User Specific Approach

FDS can earn the highest accuracy by examining each user's purchase event in detail. There are three approaches to detecting fraudsters in the view point of user management: rule-set based, cluster based and user behavior based. Rule-set based approach applies the same fraud detection rules to all users, which is simple but has a risk to occur high false positives. For a better detection accuracy, cluster based approach categorizes users in several groups by their characteristics such as income, job or purchase pattern. On the other hand, user behavior based approach investigates each user's purchase pattern, which is less broad than applying the same rules to everyone but possible to acquire the most accurate result. We focus on the user specific approaches by utilizing each user's purchase history.

4.2.2. High Precision and Recall

Determining an appropriate accuracy measure is another important issue in FDS. Since FDS dataset is highly unbalanced, some accuracy measures may not be proper to be adopted. In this study, we use precision and recall to verify the accuracy of FDS. The recall indicates how many frauds are detected by the FDS from the total frauds, and the precision shows how precisely the FDS works while not detecting the legitimate transactions as frauds. That is, high precision is related with less customer inconvenience, and high recall is connected with less loss to card service provider. High precision is also closely related with real-time blocking since FDS has to determine whether transaction is fraudulent or legitimate within only a few seconds.

Meanwhile, Area Under Curve of Receiver Operating Characteristic (ROC-AUC) is often utilized to measure the accuracy of fraud detection. However, ROC-AUC may not be a meaningful accuracy measure in credit card frauds since it does not reflect a false positive rate when dataset is highly unbalanced (Davis and Goadrich, 2006). Thus, we do not consider ROC-AUC in this study and would rather consider precision, recall and false positive rates.

4.2.3. Privacy Preservation

Credit card transactions often contain various personal information such as the owner's age, gender or residence, which may be used to re-identify the owner. Re-identification can happen from either 3rd party FDS analyzer or a curious insider in company. For this reason, FDS should deal with only a few features that are not related with users' identification. In this study, we only use user id, time-gap, amount and merchant category code. User-ID is based on a credit card number which it is necessarily modified with a hash function such as SHA256 and the other features are not enough to identify a specific user.

4.2.4. Unsupervised Learning

A new payment service provider would require various fraud cases in order to run a fraud detection system. However, fraud cases are closely related to personal information that the fraud cases are difficult to be shared among payment service providers. In this situation, supervised learning based approach is not appropriate since it utilizes already existing fraud cases. From the point of view, we consider unsupervised learning based approach using anomaly of purchase density.

4.3. Risk Measurement

Before predicting fraudulent transactions, we have to define parameters to estimate the risk probability of the next transaction. As we discussed in section 4, the purchase density can be a good feature to measure the risk probability. To measure the risk probability, we first calculate each individual's purchase density by using the purchase history. Next we estimate the risk probability using a cumulative density function (CDF) of Poisson distribution which has a parameter as the purchase density β.

If X represents amount and A_n represents the amount of n th transaction, the risk probability of $n+1$ th transaction is as follows:

$$P\{Trans_{n+1} = Fraud\} = P\{X < A_{n+1}\} = e^{-\beta_n t_{n+1}} \sum_{i=0}^{\lfloor A_{n+1} \rfloor} \frac{(\beta_n t_{n+1})^i}{i!}. \tag{1}$$

and β_n is calculated by

$$\beta_n = \frac{\sum_{i=1}^{n} A_i}{\sum_{j=2}^{n} t_j}, (n = 2, 3, 4, \cdots) \tag{2}$$

where β_n is the average purchase amount per time from the first transaction to the n th transaction, and t_n is the time gap between n th transaction and $n-1$ th transaction. The risk probability of a transaction will show a value if a high volume of purchases happens in a short period. Also, we utilized the average of β to measure the risk probability of the first transaction. In the empirical result, the average purchase density β_1 was 20.0.

Figure 2 shows the changes of one hundred legitimate users' β as the transaction increases. The time-varying purchase density implies that the same amount can have different risk probability by each person's purchase history. Moreover, we realized that the purchase density changes over time and it tends to converge as the number of transaction increases.

5. Experiment Results

In the experiment, we regarded that a transaction is suspicious when the risk probability exceeds 90%. Moreover, we set a blocking parameter k that blocks the k th consecutive

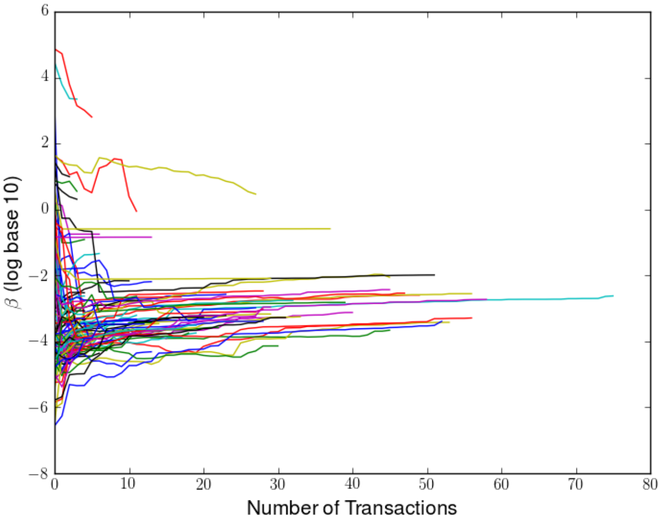


Figure 2: Changes of β from 100 legitimate users

suspicious transactions. For instance, if $k = 1$, PD-FDS detects the very transaction as a fraud. On the other hand, if $k = 3$, PD-FDS does not block the first and second suspicious transactions and block the third transaction.

The PD-FDS results when $k = 1, 2, 3$ are shown in Table 1. The result shows that false positives decrease according to the increase of k, but the financial loss of payment service provider also increases. Likewise, blocking the kth suspicious transaction is related with a trade-off between detection accuracy (recall) and customer convenience (precision). If FDS blocks those first suspicious transactions ($k = 1$), it can occur high false positives which can cause higher monitoring cost and customer inconvenience. Since customer inconvenience is difficult to evaluate, the choice of k will be different by card company's policies.

Table 1: Accuracy metrics: Here **FPR** represent false positive rates.

Model		**Precision**	**Recall**	**F-measure**	**FPR**
PD-FDS	($k = 1$)	0.040	0.833	0.076	0.01
PD-FDS	($k = 2$)	0.336	0.729	0.460	0.0007
PD-FDS	($k = 3$)	0.870	0.671	0.757	0.00005

6. Discussion and Future Work

In an additional experiment, we found that specific merchants had high probabilities of fraud. The risk probabilities of merchants can be utilized as a meaningful feature to detect frauds by using supervised learning approaches. However, a new payment service provider does not have the information of risky merchants. This implies that the new payment service provider has to afford financial loss until it gathers enough fraudulent cases to build up their own FDS. From this perspective, our approach can be utilized as a prior knowledge to detect risky transactions before the payment service provider gathers enough information of risky merchants.

Moreover, the accuracy of PD-FDS may be affected by the season or time of year. For instance, a user might make a lot of purchases in a short period of time during holidays or during family vacations. PD-FDS might detect the legitimate transactions as frauds since the seasonal events were not considered. We will consider the annual events such as Black Friday to increase the accuracy in the future work.

7. Conclusion

We proposed PD-FDS that utilizes three features not related to personal information: time gap, amount and merchant category code. Since the fraudsters have a goal to make unfair profit as much as and as soon as possible, we focused on the features to define risk probability using Poisson process. Likewise, PD-FDS is unsupervised learning based approach which can be utilized by a new payment service provider. Lastly, PD-FDS has 0.01 of false positive rate in the worst case, and shows 0.757 of F-measure in the best case.

References

Alejandro Correa Bahnsen, Aleksandar Stojanovic, Djamila Aouada, and Bjorn Ottersten. Cost sensitive credit card fraud detection using bayes minimum risk. In *Machine Learning and Applications (ICMLA), 2013 12th International Conference on*, volume 1, pages 333–338. IEEE, 2013.

Alejandro Correa Bahnsen, Djamila Aouada, Aleksandar Stojanovic, and Björn Ottersten. Detecting credit card fraud using periodic features. In *Machine Learning and Applications (ICMLA), 2015 IEEE 14th International Conference on*, pages 208–213. IEEE, 2015.

Alejandro Correa Bahnsen, Djamila Aouada, Aleksandar Stojanovic, and Björn Ottersten. Feature engineering strategies for credit card fraud detection. *Expert Systems With Applications*, 51:134–142, 2016.

Siddhartha Bhattacharyya, Sanjeev Jha, Kurian Tharakunnel, and J Christopher Westland. Data mining for credit card fraud: A comparative study. *Decision Support Systems*, 50 (3):602–613, 2011.

Andrea Dal Pozzolo, Olivier Caelen, Yann-Ael Le Borgne, Serge Waterschoot, and Gianluca Bontempi. Learned lessons in credit card fraud detection from a practitioner perspective. *Expert systems with applications*, 41(10):4915–4928, 2014.

Jesse Davis and Mark Goadrich. The relationship between precision-recall and roc curves. In *Proceedings of the 23rd international conference on Machine learning*, pages 233–240. ACM, 2006.

Michael Edward Edge and Pedro R Falcone Sampaio. A survey of signature based methods for financial fraud detection. *computers & security*, 28(6):381–394, 2009.

Horst Forster. Card fraud report 2015. http://www.paymentscardsandmobile.com/wp-content/uploads/2015/03/PCM_Alaric_Fraud-Report_2015.pdf, 2015.

Sanjeev Jha and J Christopher Westland. A descriptive study of credit card fraud pattern. *Global Business Review*, 14(3):373–384, 2013.

Min-Jung Kim and Taek-Soo Kim. A neural classifier with fraud density map for effective credit card fraud detection. In *International Conference on Intelligent Data Engineering and Automated Learning*, pages 378–383. Springer, 2002.

Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, and Bernard Manderick. Credit card fraud detection using bayesian and neural networks. In *Proceedings of the 1st international naiso congress on neuro fuzzy technologies*, pages 261–270, 2002.

Nilson. Nilson report 2016. https://www.nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf, 2015.

Dominik Olszewski. Fraud detection using self-organizing map visualizing the user profiles. *Knowledge-Based Systems*, 70:324–334, 2014.

Suvasini Panigrahi, Amlan Kundu, Shamik Sural, and Arun K Majumdar. Credit card fraud detection: A fusion approach using dempster–shafer theory and bayesian learning. *Information Fusion*, 10(4):354–363, 2009.

Jon TS Quah and M Sriganesh. Real-time credit card fraud detection using computational intelligence. *Expert systems with applications*, 35(4):1721–1732, 2008.

KR Seeja and Masoumeh Zareapoor. Fraudminer: a novel credit card fraud detection model based on frequent itemset mining. *The Scientific World Journal*, 2014, 2014.

Christopher Whitrow, David J Hand, Piotr Juszczak, D Weston, and Niall M Adams. Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, 18(1):30–55, 2009.

Vladimir Zaslavsky and Anna Strizhak. Credit card fraud detection using self-organizing maps. *Information and Security*, 18:48, 2006.