Latin American Journal of Central Banking 3 (2022) 100050

Contents lists available at ScienceDirect

Latin American Journal of Central Banking

journal homepage: www.elsevier.com/locate/latcb

Identifying clusters of anomalous payments in the salvadorian payment system

Franklim Arévalo[a], Paolo Barucca[b], Isela-Elizabeth Téllez-León[c,*], William Rodríguez[d], Gerardo Gage[e], Raúl Morales[f]

[a] *Specialist of the Oversight of Payment Systems Department, Central Reserve Bank of El Salvador, Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88, Edificio Oca Chang, Segundo Nivel, San Salvador, El Salvador*
[b] *Professor at University College London. University College London, Gower Street, London WC1E 6BT, UK*
[c] *Director of Financial Markets Infrastructures at CEMLA. Durango 54, Colonia Roma Norte, Alcaldía Cuauhtémoc, Ciudad de México 06700, Mexico*
[d] *Senior of Information Systems. Central Reserve Bank of El Salvador, Prolongación Avenida Alberto Masferrer y calle al Volcán No. 88, Edificio Oca Chang, Segundo Nivel, San Salvador, El Salvador*
[e] *Former Analyst at CEMLA. Durango 54, Colonia Roma Norte, Cuauhtémoc City Hall, Mexico City 06700, Mexico*
[f] *Former Manager at CEMLA. Durango 54, Colonia Roma Norte, Alcaldía Cuauhtémoc, Ciudad de México 06700, Mexico*

ARTICLE INFO

Keywords:
Automated detection
Anomalous patterns
Payment systems
Supervisory analysis

ABSTRACT

We develop an unsupervised methodology to group payments and identify possible anomalies. With our methodology, we identify clusters based on a set of network features, using transactional (unlabeled) information from a systemically important payment system of El Salvador. We first preprocess network features, such as degree and strength, through a principal components analysis we reduce the dimensionality of the newly defined data, then we place the main variables into clustering algorithms (*k-means* and *DBSCAN*) to analyze anomalous payments. We then analyze, these clusters using random forest to obtain the main network feature. Our results suggest that the proposed methodology works very well to detect anomalous payments, and it is very important to study the case of El Salvador, because of the recent restructuring of the Massive Payment System in El Salvador (promoted by the *Transfer365* project), because the authorities want to increase financial inclusion. This change will make the SPM available to the public, to diversify services and incorporate more participants because, historically, it has operated with only three active participants. We expected that *Transfer365* will interconnect the LBTR participants' systems with their banking core, the systems of the Ministry of Finance, and other authorized participants to channel large payment flows. Then, identifying possible anomalies through methodology will enhance risk monitoring and management by payment systems overseers.

1. Introduction

Payment systems or Financial Market Infrastructures (FMIs) are the backbone of the economy because they provide the platform(s) where financial system's participants are able to perform the majority of their transactions, whose supervision is one of the main objectives of central banks and analytical tools are essential to improve the ability to monitor the proper functioning of FMIs.

We study the Massive Payment System (SPM, in Spanish, Sistema de Pagos Masivos), because it will become one of the engines of financial inclusion for El Salvador. At the beginning of 2021, the BCR presented important modifications in the SPM, mainly driven

[*] Corresponding author.
E-mail address: itellez@cemla.org (I.-E. Téllez-León).

https://doi.org/10.1016/j.latcb.2022.100050
Received 6 August 2021; Received in revised form 19 November 2021; Accepted 10 January 2022

by the introduction of the *Transfer365* project. This change will make the SPM available to the public through system's participants to diversify services and incorporate more participants, as historically it has operated with only 3 active participants. As a result, the SPM could enhance its functioning to enable that transfers between different banks, government payrolls, card payments and loan operations will take place under a 24/7 operating mode. The BCR expects to improve the financial inclusion with the SPM, by enabling that all entities of the financial system may participate, including banks, cooperative banks, savings and credit companies, ministry of finance, pension fund manager (AFP), Development Bank of El Salvador, institute of guarantees and deposits (IGD), among others. In other words, the SPM will serve as a real-time platform for the clearing and settlement of retail payments, besides the current arrangements provided by the ACH and other retail payment systems. In special, it is foreseen that the *Transfer365* will interconnect the systems of RTGS participants with their banking core, and the systems of the Ministry of Finance and other authorized participants, to channelize large streams of payments.

From the above, it is expected that the transactions of the payment systems with this new service will grow exponentially, as they will be available to the entire population. In this scenario, oversight functions could become complex for the BCR and as such, the application of machine learning techniques could be purposeful to understand the behavior of the connections of the different participants and identify possible anomalies in an automated way. To better guide the operation of the SPM, and on the other, to improve the capacity to identify anomalies or possible threats.

The automated detection of anomalous patterns in payment systems could allow central banks and supervisory authorities to identify potentially fraudulent transactions, cyber-attacks and unexpected behavioral changes from system's participants, which could lead to systemic events. However, only a limited number of studies applies machine learning methods to detect anomalous behavior in payment systems.

The analysis of risks (including legal, financial, operational, among others) in the payment systems helps to identify and mitigate stressful events (as operational problems, macroeconomic stress, crash of stock markets after start of COVID, among others). How a central bank must supervise the proper functioning of the payment system as it is the backbone of the economy through which economic transactions are possible. This oversight role is not relatively new area in central banking, since the first PFMIs were published in 2001 and a more extensive set of Principles in 2012 (CPMI, IOSCO). The operators are responsible for the system, which is in many cases not the central bank (CCPs, settlement organizations, ACHs, CLS). Then, there is only the oversight role which is often with the central bank. By doing so, they could contribute to avoid or minimize significant losses for the system operator and the participants. Given the fact that payment systems are the bedrock of financial systems and the economy, its safe and efficient performance is paramount.

We develop a machine learning methodology for clustering the transactions of the *Sistema de Pagos Masivos* from El Salvador (SPM), which is a relevant RTGS subsystem and classified as a systemically important payment system (SIPS), and with that identify groups of unusual payments in order to assist overseers in delving timely interventions. We define an unsupervised methodology, which does not require pre-labeled data, to single out anomalous behavior in a large set of transactions taking place in the SPM, from 2013 to the first quarter of 2021. Two main sets of features are investigated in the first part of our study. In the first set, qualitative features are transformed into a binary vector by one-hot encoding. For the second set, new features are created to account for the network characteristics inherent to the SPM. A third approach combines and tests the above-mentioned sets of features. Then, we implement Principal Components Analysis and two clustering algorithms, *k-means* and *DBSCAN*, to the different sets of features (as degree and strength), divide transactions into clusters, and provide a statistical description of their features.

The methodology used in this paper begins with data preprocessing, to employ anomaly detection methods, through the creation of two sets of functions: one-hot encoding functions and network-based functions. The trainers are created with the purpose of capturing the average behavior of the participants during the period studied. Care is taken to standardize and eliminate the noise to correctly feed the PCA, once this has been worked, through selected techniques for clustering, such as *k-means* and *DBSCAN*, different experiments were carried out, to know the characteristic that governs the clusters the random forest was applied.

Finally, we analyze the results obtained by the clustering analysis observing its distribution over the network features and point out the most relevant groups of operations according to its anomalous nature. This analysis serves to better define why these operations may represent a risk for the well-functioning of the payment system and therefore, determine if they should be further reviewed by overseers. Our work contributes to the development of oversight tools based on Machine Learning techniques that enhance central banks' oversight capacities over financial market infrastructures. In our knowledge, this is the first time that clustering and denoising methods are applied to the detection of anomalies in a transactional level dataset and the results obtained show that our methodology can serve to support central banks' monitoring task.

This work analyzes through machine learning techniques, the anomalous payments in the SPM of El Salvador. We consider an anomalous payment a transaction with patterns that do not conform to a normal payment flow as defined by Chandola et al. (2009). The following section presents the literature review, then Section 2 describes the payment systems of El Salvador, particularly the importance of analyzing the SPM Section 3. presents the methodology used in this paper starting with preprocessing, PCA denoising, clustering algorithms, *k-means* algorithm, *DBSCAN* and Random Forest. In Section 4 the results are showed and summarized, at the end we present the conclusions.

2. Literature review

Network theory can help the oversight goal. Even though, Leon and Pérez (2014) evaluated the systemic importance of financial market infrastructures, the anomaly detection techniques used for network intrusion detection have been analyzed by Chan et al. (2003), Yeung and Chow (2002), Siaterlis and Maglaris (2004), Chandola et al., (2006), Sun et al., (2007). Meanwhile, studies on classification-based anomaly detection techniques using neural networks were studied in Hawkins et al. (2002), Thompson et al. (2002), Dasgupta and Nino (2000), among others. Thus, we contribute with the literature analyzing anomalous payments through clusterization and random forest, as innovative and powerful techniques to study the El Salvador case.

Payment systems can be represented as time-varying directed networks, where each participant is a node and transactions in a given time interval are edges between participants. This representation can prove to be useful for multiple kinds of analysis, for example, identifying operations related to money laundering and terrorism financing. This helps to make the financial systems more secure, as analyzed by Collin et al. (2016). In Bech and Atalay (2010), the authors investigated the overnight federal funds market from the US from the perspective of the network topology that it formed. The network was observed to be sparse and disassortative and showed small world property, that is to say, each financial institution is just a few transactions away from each other. In Soramäki and Cook (2013) a tailored metric was developed to measure systemic risk in payment systems, the SinkRank. This methodology predicts the level of disruption in the network that the failure of a bank can cause in the whole payment system and which banks would be the most affected, the approach taken is based on network theory and absorbing Markov chains. However, we are interested in anomaly detection techniques as approach to monitor and oversee payment systems and other FMIs relate to see financial systems as networks. They have been shown to exhibit a regular set of features and patterns at a network level.

An important task related to the oversight of FMIs is the detection of anomalies or outliers that can arise from different sources as money laundering, financing of terrorism, behavioral changes from one or many FMIs' participants, among others. Clustering techniques have proven to be prolific for anomaly detection in different fields. In Baek et al. (2021) was developed a cluster-based methodology to detect anomalies in a computer network, which under this context have the form of network intrusions, under a semi-supervised approach they implemented *k-means* clustering to create labels of normal and anomalous and then they trained the model by using the labels to predict future anomalies. Another example of the use of clustering techniques for anomalies detection is observed in Sutapatt and Vasarhelyi, (2011), where *k-means* was used in order to find clusters of group-life insurance claims that were needed to further investigate because of its abnormal nature. Within the context of finance, Khac and Kechadi (2010) utilized an approach based on clustering combined with neural networks and decision trees to identify suspicious cases of transactions for money laundering activities within an investment bank. For the above, we can see the effectiveness of studying with the clustering approach and decision trees, then in this line, we analyze anomalies in the payment systems for the El Salvador case through clustering algorithms (*k-means* and *DBSCAN*) and random forest.

As shown in Chandola et al. (2009), it is essential to detect anomalies in the payment system, as we analyze concluded, they survey existing techniques for anomaly detection, point out the key assumptions, the methods, and the advantages and disadvantages of such techniques. Among recent applied studies there is the one by Triepels et al. (2018), they developed a method that reconstructs distinctive characteristics of the payment network, accounting for anomalies if changes appear in the liquidity vectors between banks. This analysis was carried out in a real-time gross settlement system. Similarly, Sabetti and Heijmans (2021) use (deep) neural networks (autoencoder) to detect anomalous flows of payments in an automated clearing house of Canada. They suggest that their automatic encoder detects anomalous payment flows and could provide atypical signals that are important for financial stability analysis carried out by central banks. While, for the Ecuadorian system Rubio et al. (2020) studied anomalous payments through autoencoder methodology.

Other related studies on risk indicators for oversight, operational risk, intraday patterns and timing are: Berndsen and Heijmans (2020), Glowka et al. (2017) and Massarenti et al. (2012). While, in Barucca and Lillo (2018) a methodology is developed based on Stochastic Block Models (SBM), structured simulated networks, to investigate all the possible two-blocks organizations that interbank networks could present. They found that under normal conditions, the networks of overnight loans in the Eurozone from 2010 to 2014, displayed a bipartite structure, where banks are either acting as lenders or borrowers. While, under distressed conditions, the structure tends to lose this bipartite structure due to individual banks' modifying their strategies, in connection with monetary measures.

In sum, our study is in line with anomalous payments analysis. Recently, Triepels et al. (2018) introduced novel unsupervised methodologies to classify transactions in payment systems and recognize when the financial network as a whole cease to follow its usual patterns of behavior. This is accomplished by learning a complex representation of vector of transactions based on a set of hidden variables obtained as the output of a feedforward neural network, an encoder, which is then followed by a reverse transformation, a decoder, which tries to approximate the initial set of variables, that is to say, the vector of transactions. Other studies that analyze anomaly detection techniques are León (2020) and Rubio et al. (2020). While, other that used for host-based intrusion detection are: Esponda et al. (2004), Eskin (2000), Ghosh et al. (1998), Hu et al. (2003), Heller et al. (2003), Lee et al. (2000), among other. Clustering studies are found for the study of anomaly detection techniques used for credit card fraud detection, as in Bolton and Hand (2001). As part of our methodology, we follow a simpler yet similar logic, *k-means* clustering identifies sets of transactions which can consistently fall into large clusters of similar transactions, sharing similar properties in terms of transaction volume and simple network features, while other transactions remain isolated or fall into smaller clusters which can be individually analyzed. In this line, we analyze the El Salvador case through clustering algorithms (*k-means* and *DBSCAN*) to analyze anomalous payments and we use random forest to obtain the main network feature.

3. The payment system of El Salvador

The Central Reserve Bank of El Salvador (Banco Central de la Reserva: BCR) provides a variety of critical payment and settlement services to banks and other financial system's participants through the real time gross settlement (RTGS) system. The RTGS allows numerous interconnections with other FMIs and payment systems.

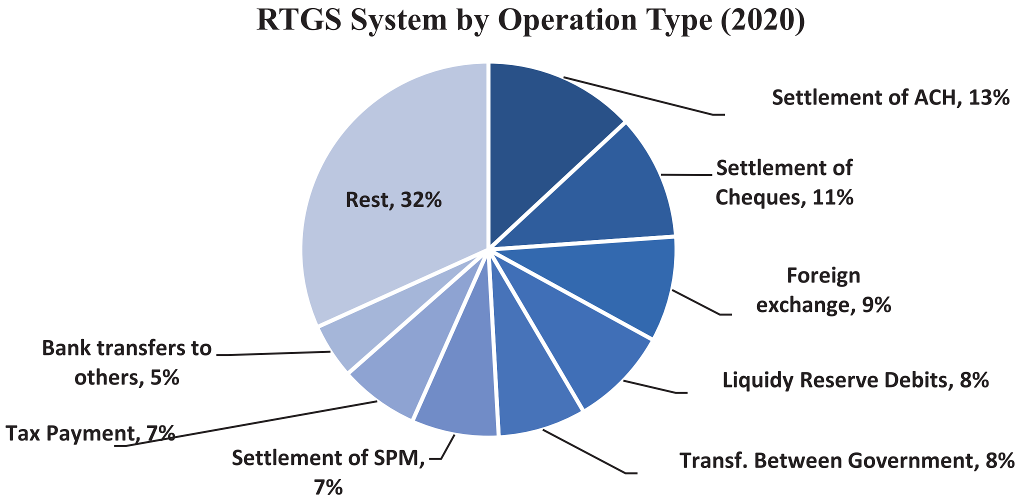


Fig. 1. Salvadorian RTGS system by operation type in 2020 source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.

3.1. The real time gross settlement system

The main payment system in El Salvador is the real time gross settlement system (RTGS), which is the axis and central support of the entire national payment infrastructure, as this is where the monetary settlement of transactions takes place in the various markets considered critical. In this system, transfers are processed related to transactions that RTGS participants make on their own behalf, the funds are debited and credited in real time between deposit accounts, said accounts are only held by RTGS participants, including financial system participants and the public sector. The BCR's accountholders (banks and other financial system's participants) can make transfers of funds between them, and in turn allows the settlement of other payment systems, providing irrevocability and finality. Each participant can initiate a transaction on an automated (straight-through-processing, STP) basis, and they define the level of services that is offered to their clients.

The total value settled in the RTGS increased at a rate of approximately 9.5% per year for the 2015–2020, and the total value settled in 2020 was USD 69.5 billion, almost 2.8 times the country's GDP for that same year.

On the other hand, the total number of payment orders settled (volume) in the RTGS increased at a rate of approximately 10.4% per year from 2015 to 2020. The pandemic constituted an important push for the use of the RTGS, this could be largely explained because of the special operations that the government initiated and the RTGS participants movements to respond to liquidity shocks in the interbank market.

RTGS participants can exchange various kinds of payments, such as international or domestic transactions, direct or indirect payments, and so on. Each transaction corresponds to a single operation type. One can underline that each type of payment could be associated with specific patterns and characteristics. In fact, the RTGS provides more than 100 ”operation types”, yet over 70% of the total amount settled corresponds to only 8 of them, including: settlement of SPM operations, settlement of Check Clearing House (CCH) orders, settlement of Automated Clearing House (ACH) positions, transfers between government institutions, foreign exchange transactions, tax payments and liquidity reserve debits, as shown in Fig. 1.

In this context, the SPM stands as one of the key retail payment systems managed by the BCR for making transfers nationwide, only behind the ACH and the CCH platforms.

3.2. Sistema de Pagos Masivo (SPM)

The *Sistema de Pagos Masivos* (SPM) is a platform managed by the BCR and began operations in 2013. The SPM is a deferred settlement system that enables payment orders from an origin participant, for the payment of obligations to third parties (suppliers, payrolls, pension funds). Payments ordered in the SPM are automatically credited into the beneficiaries' account. The workflow of the SPM is depicted in Fig. 2 and it can be described as follows Fig. 3.

- Customer/User perform payment transaction through a participant A.
- Participant A and participant B both have accounts with a central bank.
- A payment in dollars is to be made from participant A to participant B.
- Participant A submits the payment instructions to SPM.
- Participant A's account is debited, and participant B's account is credited – the payment is settled.
- The SPM through the RTGS transfers the payment information to Bank B.
- Final customer/user receive payment transaction in their personal account through a participant B.

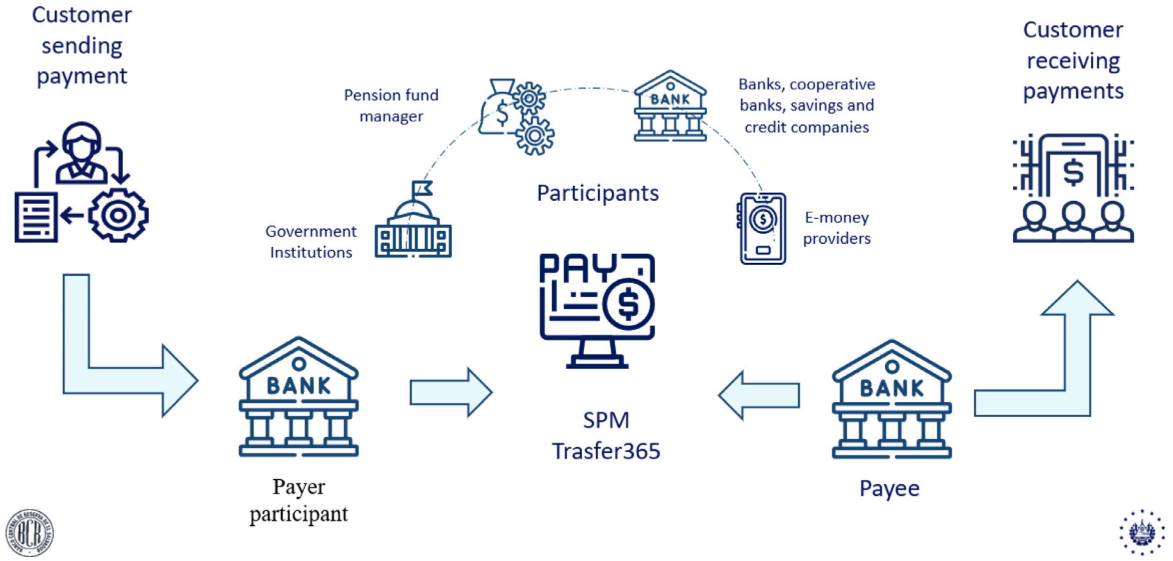


Fig. 2. SPM Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.

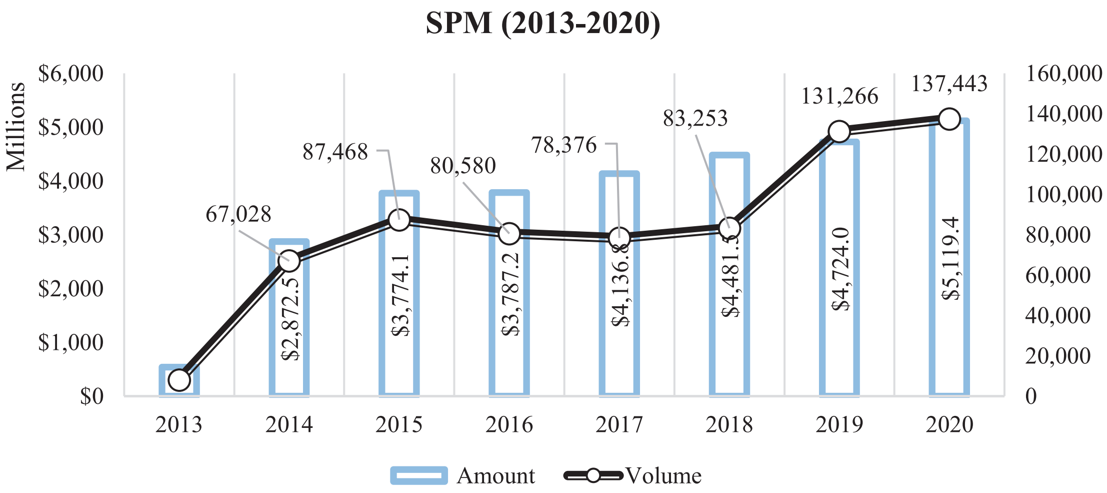


Fig. 3. Salvadorian SPM growth between 2013 and 2020 source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.

Table 1
Percentage behavior of each participant.

Origin Participant	2013	2014	2015	2016	2017	2018	2019	2020
Ministry of Finance	100.0%	100.0%	100.0%	100.0%	100.0%	99.9%	99.9%	99.6%
The Development Bank of El Salvador						0.0%	0.0%	0.3%
E-Money Provider						0.1%	0.1%	0.1%

Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.

In December 2016, the Board of Directors of the Central Bank indicated that the SPM should be treated as a SIPS considering the criticality of the payments made through it. This change made that oversight of the system became relevant to avoid that the SPM is not sufficiently protected against risks. It was also acknowledged that an alteration in the system could trigger or transmit negative effects on a larger scale among the participants or create systemic alterations in the financial sector as a whole. The initial shock could, for example, be caused by the insolvency of a participant.

In 2020, the total value of transactions processed in the SPM increased at a rate of approximately 10.5% per year. You can observe the behavior for each participant in Table 1. The value settled in the SPM reached USD 5.2 billion, this amount represents almost 0.46 times the country's GDP.

The SPM began operations with Ministry of Finance in 2013, and in 2018 The Development Bank of El Salvador and E-Money Provider were incorporated, both with low participation compared to Ministry of Finance.

Currently there are 13 institutions that receive transactions made through the SPM, 99% issued by the Ministry of Finance. From 2013 to 2016, more than 80% of the funds were allocated to a single participant, but as of 2017 the proportion has changed somewhat due to the interaction of new participants in the SPM. In particular, Bank 2 received the largest number of payments, but in the last four years, other bank Bank 9 more than doubled the number of payments received in a year. We can identify a structure of payments featuring in the SPM. The system is extremely concentrated, one bank had over 90% of the transactions in 2013 and that decreased to about 77.3% in 2020. One bank increased from roughly 2 to 11%. The top 5 banks have 95.9% in 2020 regarding 99.6% the transactions on average over the whole data sample.

The SPM has historically been structured in 5 different types of operations; however, its occupation is concentrated in 2 more important ones. In particular it can be noted that between 2013 and 2015 the SPM was used close to 100% in operations destined to the payment of service providers provided to government institutions. Between 2016 and 2020 the structure changed with the incorporation of new operations, being allocated in average on those dates 48.1% to payroll payments and 51.73% to payment of suppliers. This means that the system has been used more frequently in order to facilitate payment transactions to different service providers that are provided to different government institutions.

It can be concluded that the SPM has presented a growing trend in terms of the number and type of transactions as well as in the number of participants. The *Transfer365* project would possibly accelerate these trends to make that the SPM acquires an even more considerable role in the national financial infrastructure.

3.3. Data description

We use unlabeled financial transactions from SPM from 2013 to the first quarter of 2021. The analysis was made on an anonymized daily dataset, that contains information from 2013 to 2020. For each transaction the data provided is:

- √ Origin participant or payer participant: Identification of the bank, institution or any other participant who orders to make the transaction.
- √ Beneficiary participant or payee participant: Identification of the bank, institution or any other participant who is the recipient of the transaction.
- √ Settlement date: Date when the transaction triggers a charge to the origin participant and a debit to the beneficiary participant.
- √ Operation type: Identification of the operation type related to the transaction. It is set by the origin participant and must be enabled to their account for use as a security measure.

Instruction amount: Value in USD of the transaction. Instruction means the order to perform the charge and debit to the accounts of participants.

There are more data elements characterizing payment transactions, yet for the exploration of anomalies, we focus on the ones above.

I. Our methodology creates clusters based on a set of one-hot-encoding and network features according to their relative distance in a reduced feature space, created by implementing PCA. We specifically look for a cluster, or set of clusters, which, based on a posteriori analysis, can be identified as anomalous.

4. Methodology

The methodology can be divided into three main steps: data preprocessing, PCA denoising and clustering analysis. The first step has the purpose of transforming the original data into features that are meaningful for the anomaly detection task performed by the clustering algorithm. In our case, it involves the creation of two new sets of features: one-hot encoding features and network-based features. The formers are created from the interactions that occur between the participants of the payment system. They are created with the purpose to capture the average behavior of the participants during the period studied. Then, as part of the preprocessing step, the features are standardized to correctly feed the PCA. In this regard, once the one-hot encoding features are created we end up with a large number of components, which can have repercussions on the performance of the models. Hence, we decided to introduce a denoising step and apply PCA, which maintains the most relevant information contained in the data. The last step we perform is the clustering analysis, the techniques selected were *k-means* and *DBSCAN*; we run different experiments where we change the set of features and their normalization. In the following subsections we deepen on each of the techniques implemented, PCA, *k-means, DBSCAN* and random forest.

Three main steps were made: data preprocessing, PCA denoising and the implementation of clustering algorithms. In all the cases the features were transformed with PCA preserving 85% of variance and varying the set of features which were standardized. We can summarize the performance of each model as follows:

- Model 1: The model was trained with the *k-means* algorithm. It was fed with network and amount features standardized and one-hot-encoded features.
- Model 2: The model was trained again with the *k-means* algorithm, but for this case, the complete set of features were standardized.
- Model 3: The model was trained with the *DBSCAN* algorithm. It was fed with network and amount features standardized and one-hot-encoded features.

- Model 4: The model was trained with the *DBSCAN* algorithm. It was fed with the complete set of features standardized.

In the case of the *k-means* implementation, the Elbow method was selected to identify the optimal number of clusters. For the *DBSCAN* algorithm, we computed a set of values for both of its parameters and selected the configuration that yielded the lowest number of observations that couldn't be classified, that is to say, the ones that were assigned to the cluster -1.

4.1. Preprocessing

We define for any given time, transactions are grouped into a *NxN* transaction matrix, $w_{ij}^{(t)}$, representing the volume of the transaction from institution *i* to institution *j* in time interval *t*. For convenience we also define the matrix $a_{ij}^{(t)}$ defined as,

$$a_{ij}^{(t)} = 1 \ if \ w_{ij}^{(t)} > 0$$

and zero otherwise.

Transaction data present a temporal weighted network structure as each transaction in any given time window has a weight, a paying institution and a receiving institution. Because of this temporal weighted network, we can define a set of network quantities that measure both the activity of an institution on the given time window and also in the recent past. Let us define in detail the network quantities that we look at: the total out-degree (number of out-counterparties at time t) of the financial institution that is giving the money,

$$Degree^{out}(t, \ \ i) = \sum_j a_{ij}^{(t)}$$

the total out-volume or out-strength of the financial institution that is giving the money,

$$Strength^{out}(t, \ \ i) = \sum_j w_{ij}^{(t)}$$

the total in-degree (number of in-counterparties at time t) of the financial institution that is receiving the money,

$$Degree^{in}(t, \ \ i) = \sum_j a_{ji}^{(t)}$$

and the total in-volume or in-strength of the financial institution that is giving the money,

$$Strength^{in}(t, \ \ i) = \sum_j w_{ji}^{(t)}$$

For each of these quantities we can compute moving averages in time windows of different sizes namely,

$$MA_{STR}(t, \ \tau, \ i) = \frac{1}{\tau} \sum_{k(\tau)} Strength^{in/out}(i, t-k)$$

which in our case provides at each time step the average in-going and out-going volume (strength) transacted by institution in the last 7 days,

$$MA_{VOL}(t, \ \tau, \ i) = \frac{1}{\tau} \sum_{k(\tau)} Volume^{in/out}(i, t-k)$$

which in our case provides at each time step the average in-going and out-going volume transacted by institution in the last 7 days,

$$MA_{VOL}(t, \ \tau, \ i) \ = \ \frac{1}{\tau} \sum_{k(\tau)} Degree^{in/out}(i, t-k)$$

which conversely provides at each time step the average in-going and out-going degree for each institution in the last 7 days. These features aim to evaluate a given transaction based on the historical pattern of the given institution.

Once we define these node features, we can then associate them as features of the corresponding transactions, for example, each transaction inherits the network features of its sending and receiving institution.

Each transaction is then associated with a set of features

$$f = \left(f_1, \ f_2, \ldots, \ f_p\right)$$

where *p* is the number of transaction features.

If we want to characterize transactions at an institution-level, then we need to represent the information related to the institution. This is accomplished using one-hot encoding in which each institution label is associated to a binary digit and the full set of institutions is associated to an ordered binary vector. Consequently, each transaction between a given pair of institutions, can be associated to two binary vectors, one for the sender institution, in which only the digit corresponding to the sender institution label is non-zero and equal to one, and one for the receiver institution, according to the same criterion.

One-hot encoding has the advantage of defining an unambiguous vectorial representation for each institution, but inconveniently increases the number of features by the number of different possible labels. When considering both the features that are coming from one-hot encoding and from network analysis we end up with a significantly larger set of features for each transaction,

$$f' = \left(f'_1, \ f'_2, \ldots, \ f'_q\right)$$

where q is the number of transaction features when one-hot encoding is in place.

Due to the different range of values where features lie, it was decided to conduct a re-scaling or standardization of the features. Let $X_f = (x_1, x_2, \ldots, x_n)^T$ be the vector of values of feature *f*, then the standardization of a given instance of X_f is computed as,

$$x_i^{standardized} = \frac{x_i - \mu_f}{\sigma_f}$$

Where x_i is the *i*th instance of X_f, and μ_f and σ_f corresponds to the mean and standard deviation of X_f, respectively.

4.2. PCA denoising

After creating the two sets of new features, the dimensionality of the studied dataset increased. Also, due to the nature of the one-hot-encoding features, where many values are zero, noise was introduced. Training models in machine learning with high-dimensionality and noisy data could pauperize the final performance.

We implement PCA, which is a dimensionality-reduction technique that generates a linear transformation of the original data into a new lower-dimensional space with the objective to capture most of the data variance into the first's vectors, called Principal Components. PCA is also applied as a visualization tool, besides reducing the complexity of the data by creating a projection.

Let PC = $\{\overline{PC}_1, \ldots, \overline{PC}_r\}$ be the set of principal components where $\overline{PC}_i = \sum_{j=1}^{p} \theta_{j,i} X_j$ and $\sum_{j=1}^{p} \theta^2{}_{j,i} = 1$, with *p* the number of features and $X_j$the vector of values of the *j*th feature from the matrix *X*. PCA objective is to find the values of $\theta' s$ that determines the lineal transformation where most of the variance is captured in the principal components in a decreasing manner (the first component will capture most variance than the second component, and so successively) and these are orthogonal to each other.

Given a principal component PCA seeks to solve a sequence of optimization problems, starting by the first principal component, defined as

$$\max_{\theta_{1,i,\ldots,}\ \theta_{p,i,}} \left\{ Var\left(\overline{PC}_1\right) \right\} = \left\{ \frac{1}{n} \sum_{j=1}^{n} pc^2{}_{ij} \right\}$$

Subject to $\sum_{j=1}^{p} \theta^2{}_{j,i} = 1$ and to the ortogonality condition. The solution can be obtained applying Singular Value Decomposition on the matrix *X*, which in our case corresponds to the dataset obtained after creating the network and one-hot-encoding features.

4.3. Clustering algorithms

Clustering methods group individual data instances into different clusters; where the members within a same cluster present similar characteristic, that is, are close in its defined space, and the different clusters' members are dissimilar between them, that is, are far. In this context, the closeness is defined by a distance metric that in our case was the Euclidean distance.

We utilized two different clustering algorithms, *k-means* and *DBSCAN*. The first is defined under a centroid-based procedure, where the number of clusters to be created have to be set a priori, i.e., it is the algorithm's hyperparameter. The second algorithm is defined under a density-based procedure, where one has to set two parameters, one regarding to the level of closeness between two instances to be considered neighbors and the number of members that a neighborhood should have to be considered a cluster.

4.3.1. K-means *algorithm*

K-means algorithm falls within the group of centroid-based methods, that is, it defines the center of each cluster (centroid) and this is utilized as reference to decide to if an observation is close enough to belong to a cluster. In the case of *k-means*, the centroid of a cluster corresponds the vector that contains the mean of each feature in the dataset.

Following, the *k-means* algorithm generates a partition of the data into *k* groups, where each observation should be assigned to one group and the groups should not present overlapping, that is, for a set of groups $G = \{g_1, \ldots, g_K\}$; $g_i \cap g_j = \emptyset$ for every $i \neq j$. Before the training process, the number of clusters *k* is defined, meanwhile in the *DBSCAN* algorithm does not need to be specified the number of clusters to be generated a priori and lead a clusterization, where possibly a subset of observations were not able to be assigned to any of the clusters that creates.

K-means objective is to generate clusters where the variation of its members is the minimal, i.e., to found a partition where there exists the minimum distance between clusters' members. In our work, the Euclidean distance was used to define the variation (closeness) metric, defined for each cluster as

$$V\left(g_k\right) = \frac{1}{\left|g_k\right|} \sum_{i,\ \ddot{\imath}\in g_k} \sum_{j=1}^{p} (x_{i,j} - x_{\ddot{\imath},j})^2$$

Where $|g_k|$ is the cardinality of the *kth* cluster, *p* the number of features, and the $x' s$ represents the transactions. Thus, the objective function is:

$$C = \min_{\left\{g_{1,\ldots,}g_K\right\}} \left\{ \sum_{k=1}^{K} g_k \right\}$$

Varying the number of clusters, the objective function attains different values and we use the Elbow method Thorndike (1953) to select the number of clusters.

4.3.2. DBSCAN

An issue that presents the *k-means* algorithm relates to the selection of the number clusters to create, which is the only hyper-parameter to be tuned during the learning process. The *DBSCAN* algorithm is an alternative methodology that automatically generates the different clusters, based on the density of the data that is fed to the model. Instead of specifying the number of clusters that the algorithm should create, in the *DBSCAN* algorithm two hyperparameters should be specified, which are eps and minPoints. The first hyper-parameter, eps, specifies how close points should be, that is the distance between two points, to be considered neighbors. The second hyper-parameter, minPoints, specifies the minimum number of points that should exist within a group to consider it a cluster. Also, *DBSCAN* by definition creates a group of points that, given its conditions, cannot be considered to be members of any of the clusters created, that is to say, it creates a group of outliers.

As clustering algorithms are unsupervised methodologies, there is no response variable on which the performance of the models can be evaluated using metrics such as accuracy. An alternative to assess the performance of these types of models is to measure the consistency of the clusters created after training. In this sense, in our paper we use four different indexes: Silhouette index, Calinski-Harabasz index, Davies-Bouldin index and the adjusted Rand index. The first three are indexes that individually evaluates the *goodness* of clusterizations, where goodness is defined in a different form for each index, while the last index compares in a pairwise fashion how similar or dissimilar are two clusterizations.

The Silhouette index proposed by, is intended to evaluate how much an observation is similar to the rest of observation that were assigned to the same cluster, and how dissimilar this observation is with the rest of observations in other clusters. It is computed as,

$$S(i) = \frac{a(i) - b(i)}{max\ \{a(i),\ b(i)\}}$$

Then, we have $a(i)$, which is the average distance from observation i to the rest of its cluster observations and $b(i)$ is the minimum mean distance of i to all points of which i is not a cluster member. Its values ranges from $(-1,\ 1)$ where high values indicates that the observation belongs to the correct cluster and vice versa. The overall Silhouette index is computed as the mean individual observations Silhouette index. This index is often used to decide the correct number of clusters that should be use.

The Calinski-Harabasz Calinski and Harabasz (1974) index has the purpose to evaluate the goodness of a clusterization by identifying the observations in a multidimensional Euclidean space. This index considers the ratio of the sum of between-clusters dispersion and intra-cluster dispersion. For a set of data D of size n_D, which has been clustered into k groups, the Calinski-Harabasz index is computed as,

$$s = \frac{tr\left(B_k\right)}{tr\left(W_k\right)} \times \frac{n - k}{k - 1}$$

Where $tr(B_k)$ is the trace of the between group dispersion matrix, and $tr(W_k)$ is the trace of the inter-cluster dispersion matrix, defined as:

$$B_k = \sum_{q=1}^{k} n_q \left(c_q - c_D\right)(c_q - c_D)^T$$

$$W_k = \sum_{q=1}^{k} \sum_{x \in C_q} \left(x - c_q\right)(x - c_q)^T$$

Where C_q is the set of observations in cluster q, c_q is the center of cluster q, and c_D is the center of the complete set of data D. This index is higher when clusters are dense and well separated.

The Davies-Bouldin index Davies & Bouldin (1979) measures the similarity between clusters, where the similarity is a measure that compares the distance between clusters with the size of the clusters themselves. It can be utilized to determine how well the data is splitted up into different clusters, and as consequence can be used to compare different partitions (clusterizations). It is computed as:

$$DB = \frac{1}{k} \sum_{q=1}^{k} \max_{i \neq j} \left\{R_{ij}\right\}$$

where k is the total number of clusters, and R_{ij} is the similarity measure defined as:

$$Rij = \frac{s(i) + s(j)}{d(i, j)}$$

Where $s(i)$ is the average distance between each point of cluster i and the centroid of that cluster, and $d(i, j)$ is the distance between cluster centroids i and j.

Finally, Rand index measures the similarity between two clusterizations comparing them directly. The index computing takes into consideration the three assumptions, which will conform the basis for the comparison:

(i) Each data point or observation is assigned to only one of the clusters created.
(ii) Clusters are defined for both the observations that belong to it and the observations that does not belong to it.
(iii) All the observations have the same importance for the clustering process.

Given the above assumptions, Rand index observes on how pairs of observations are clustered, having that if for a pair both observations are in the same cluster for both clusterizations or if them are assigned into different clusters for the two clusterizations, then it represents a similarity in the clusterings. In the opposite case a dissimilarity is present when a pair of observations are assigned to one cluster for one clustering and in a different cluster for the second clustering.

More precisely, let x be the number of pairs of observations that are in the same cluster for both clusterizations compared, let y be the number of pair of observations that are in different clusters for both clusterizations, and let $\binom{n}{2}$ the total number of possible combinations of pair of observations with n the total observations within the dataset. The Rand index is computed as:

$$ri = \frac{x+y}{\binom{n}{2}}$$

Rand index could arise issues when having random clusterization assignments. To overcome this issue it is needed to define an adjusted index version, which utilize the expected value of the index, $E(ri)$. It is computed as:

$$Adjustedri = \frac{ri - E(ri)}{\max(ri) - E(ri)}$$

4.4. Random forest

Random forests fall within the supervised algorithms category, but they are also a useful tool to get insights of which features are of importance for the learning process. In this sense, we implement a random forest in order to know which of the features that we built to create the clusters for the payment's operations were the one that influenced more during the training of the models, that is, the features that contains important information.

Random forests are an ensemble of individual uncorrelated decision trees. Decision trees are machine learning tools used both in regression and classification tasks; them work by creating a partition of the data space, using as criteria of partition the predictive variables. In this work we want to classify the belonging of each operation to one of the clusters created, thus we look to find a set of k regions $R_1,\ R_2, \ldots,\ R_k$ that minimizes the error classification rate

$$E = 1 - \max_{n} \widetilde{p_{rn}}$$

Where $\widetilde{p_{kn}}$ represents the proportion of observations of observations that belongs to the rth region that belongs to the nth cluster, it is also common to instead of the error classification rate use the Gini index and the Entropy as objective functions. Decision trees alone, although pose an intuitive interpretation, have a poor precision level in terms of prediction, thus techniques as bagging and random forest make use of a set of them to improve on this regard.

Random forest consists in the creation of a set of decision trees by following the next steps:

i Set the number, A, of trees that will be created and p the number of variables that will be considered during the partition process ($p < P$ where P is the total number of predictive variables).
ii Create A subsamples with replacement of the same size of the original dataset.
iii Generate a tree for each subsample created, only considering p predictive variables. It is important to note that although the number of predictive variables considered will be the same, these will vary for each tree.
iv The predictions for a new observation will be given by the class with a majority in the correspondent region that the observation belongs to.

Take only a subsample of size p from the set of predictive variables has the purpose to reduce create uncorrelated trees and thus reduce the variance of the model.

Once the model is trained the variable importance is obtained by measuring the improvement that the use of that variable had on the creation of the tree, this is done for all the trees considered in the random forest and finally accumulated for each predictive variable Tibshirani et al. (2001).

5. Results

In the following, we provide some insight on how the clusters created for each model are distributed over the most relevant network features. The features analyzed were amount, beneficiary counterparty degree, origin participant degree and beneficiary participant strength.[1] In this section, we show the results for four models trained. We use *k-means, DBSCAN* and Random Forest.

After training the 4 models, we analyze the distribution of the clusters focusing on the most relevant network variables. We first see the distribution of the variables individually, represented by density graphs (Section 4.1) and following the distribution over two variables, represented by scatterplots (Section 4.2).

5.1. Clusters' distribution plots for feature

Now, from 4.1.1 to 4.1.5 we provide the results per features through density graphs by amount, degree, strength and interaction.

5.1.1. Amount feature

For the *DBSCAN* models (model 3 and 4) the algorithm assigned to *cluster -1 to* those operations whose amount was very low or very high, that is, it found difficulties to assign those operations to any of the clusters generated. Model 1 assigned a specific cluster for those operations with high amounts. For model 2, we observe that there is no clear separation between the clusters generated as model 4. In the four models, it is observed that, in terms of quantity, the densities in the first model have similar distributions with the exception of one. This tells us that anomalous operations can be slightly identified if the amount is analyzed. The models that can be used to that are 2 and 3.

From the oversight perspective, the results have been deepened and it has been identified that model 3 closely matches the transactional reality of the SPM. Cluster 0 performs operations between 1 originator (Ministry of Finance) and 1 single beneficiary participant (Bank 2) with transactions of large amounts of money, cluster 1 performs operations between 1 originator and all beneficiary participants (private banks) and cluster 2 show the interaction of 2 new participants of origin (The Development Bank of El Salvador and E-Money Provider) this element clearly indicates a new interaction in the system that has been precisely identified by the algorithm. Likewise, for cluster 2 of model 2 the algorithm yielded results that indicate closely similar conclusions presented previously. See Appendix D1.

5.1.2. Beneficiary participant degree feature

The distribution of the beneficiary participant degree. It can be seen that for Models 2 and 4 there is a group that distances itself from the rest and corresponds to operations where the beneficiary participant presents a higher degree. For Models 1 and 3 we also observe the existence of this group, although in this case there is another cluster that overlaps.

From an oversight point of view, we can see that the degree of beneficiary participant would show the anomalous operations of at least one or two clusters in all the models. This indicates that it is important to analyze the counterpart of the operations to identify if the transactions are atypical. Similarly, this indicates that the patterns (historical records) are important because if a counterparty is different, it could indicate an atypical activity in the payment system, this only implies that it would be useful to review operations that are atypical when they change from the traditional beneficiary counterparty. See Appendix D2.

5.1.3. Origin participant degree feature

We have the distribution of the degree of the payers. Although in each model the overlapping between clusters changes, in each of them there is a group where the degree of the participant of origin is low, this is mostly noticeable for models 2 and 4. The figures in the Appendix D3, they together indicate that a different beneficiary and origin counterparty, respectively, could indicate clusters that are far from the group of operations. Then our models would identify which cluster should be reviewed by overseers given that an atypical behavior could be taking place. See the Appendix D3.

5.1.4. Beneficiary participant strength feature

Figures in the Appendix D4, which presents the distribution for beneficiary counterparty strength, show where clusters group a set of operations for which the beneficiary participant strength is high. Additionally, it is possible to observe that for all the models, there is also a cluster where most of its members correspond to operations where the beneficiary participant has a low strength. These panels clearly show how the distributions for the strength of the target participant indicate in the 4 models which cluster should be analyzed, because it is concentrated on one side and they show a leptokurtic distribution, while the other groups have a mesokurtic distribution.

In fact, the algorithm shows cluster 0, which explains common behaviors among a source participant (Ministry of Finance) that sends transactions to other beneficiary participants, whose "beneficiary participant straight" values are high compared to cluster 1. See the Appendix D4.

On the other hand, cluster 2 generated by the algorithm correspond to operations that do not have the same "Beneficiary participant Strength" as clusters 0 and 1, deepening the analysis it was found that all cluster 2 is related to the operations of two new entities of origin from the beginning of the intervention in the system, it is consistent that they do not have the same behavior as the other participants over time. The start of operations of 2 new participants of origin in the system, the first in August 2018, at which time The Development Bank of El Salvador begins operations, and the second in November 2018, at which time E-Money Provider begins operations (see graph below).

[1] In our work the amount refers to the money settled for the operations studied. The beneficiary degree of a participant A refers to the number of participants that sends money to A, and its computation is defined in the methodology as in-degree. The origin degree of a participant B refers to the number of institutions that receives money from B, and its computation is defined in the methodology as out-degree. Finally, the beneficiary strength of an institution C refers to the sum of the amounts that C receives from the rest of the institutions, and it's defined as in-strength in the methodology section.

5.1.5. Interaction feature

We obtained the distribution for the number of interactions between the institutions, see the Appendix D5. For all the models an overlap is observed for the cases where the number of interactions is low. There is also a group where the number of interactions is high, having that this group is separated from the rest for Models 2 and 4. The number of interactions between the participants provides a similar intuition as in Figures in Appendix D, in terms of the degree of beneficiary and origin participant, respectively. This indicates that there is an anomalous behavior between the direction of the transaction and the number of interactions. It is a clear indication that the operations identified by cluster should be carefully analyzed by the overseers, before they can become a risk for the payment system. See the Appendix D5.

We identified that model 2, cluster 0, identifies the strong interactions between the same participant of origin (Ministry of Finance), towards the participant with the highest transactionality in the SPM (entity 2). In cluster 1, it identifies the interaction of the same originating participant (Ministry of Finance) with the rest of beneficiary participants that have a lower volume of operations in the system. Likewise, cluster 2 identifies the transactions of two new participants as originators of payment to the rest of the beneficiary participants.

On the other hand, model 4 identifies groups of interactions from cluster 0 to cluster 7 that have the same source participant (Ministry of Finance) and one beneficiary participant per cluster. Furthermore, it identifies cluster -1 that indicates interactions of new participants as payment originators and includes a group of operations with interactions in a lower range than the rest of the clusters.

Of the two previous models (2 and 4), the *k-means* model (model 2) stands out, which shows a clustering based on two groups disaggregating the new participants in the same cluster (The Development Bank of El Salvador and E-Money Provider), which could be considered anomalous, without including the lowest interactions, unlike model 4.

5.2. Main scatterplots

From 4.2.1 to 4.2.3, we show the distribution over two variables, represented by the main scatterplots.

5.2.1. Amount vs origin participant degree

Models 1, 3 and 4 have a greater influence on the creation of clusters, this is explained since after a certain threshold the operations belong to a single group. For Models 1 and 2, which were trained with *k-means*, there is a small group of operations where the participant degree of origin is low, as well as, the amount that is settled. In Model 1, there are two overlapping groups where the degree of the participant of origin is high and the amount is low. This analysis gives a clear intuition about the characteristics of the payment system that can be overseen to identify anomalous payments. See the Appendix D6.

The origin participant and amount tell us how the clusters behave by segment of operations; when operations in a cluster are separated from the usual quantity, it would be convenient to review their operations to avoid a problem in the payment system.

The origin participant and quantity tell us how the clusters behave by segment of operations. In particular, when operations in a cluster are separated from the usual amount, it would be convenient to identify if it relates to an anomaly.

5.2.2. Amount vs interactions

In Models 1, 3 and 4 the amount has a greater influence on the creation of clusters, this is explained since after a certain threshold the operations belong to a single group regardless of the degree of the participant origin. For Models 1 and 2, which were trained with *k-means*, there is a small group of operations, cluster 3 and 2, respectively; where the degree of origin is low, as well as, the amount that is settled. These small group identifies the transactions of two new participants as originators of payment to the rest of the beneficiary participants. This cluster classification gives a clear intuition about the patterns established in the payment system and that could be subject of monitor to identify anomalous payments, such as the particular case of the low operations of the new participants as we previously showed. See the Appendix D7.

In the case of the *DBSCAN* algorithm (models 3 and 4), cluster -1 that normally gathers the anomalies shows a fairly high density of operations almost in the entire range of amounts and for the entire x-axis. This could be interpreted that for the algorithm, the clusters with a lower density have a strong relationship unlike the cluster of anomalies that is dispersed throughout the distribution plane.

For this analysis, models based on network variables turn out to be more descriptive by providing a better distribution of operations, isolating anomalies with greater precision; while models based on all hot-encoding variables, the results become more confusing.

5.2.3. Beneficiary participant and origin participant degree

We show that in every model exists a cluster where the operations are related to origin and beneficiary participants with a high degree. In each of the models it is observed how the origin and beneficiary participant distinguish the clusters. Overseers therefore could analyze the operations that move away from their cluster, because these could relate to anomalous operations. See the Appendix D8.

We see this interpretation since through the random forest technique, we obtained that the variables that influence the clustering are the beneficiary participant and interactions characteristics, in almost all the models. Although, origin participant is not a clear characteristic of distinction of clusters in Models 2 and 3. For the variables of degree and strength that correspond to beneficiary, the four models, indicate results in the same line.

Table 2
Summary of the models.

Model	Description	Number of clusters	Most interesting findings
Model 1	*K-means* + network and amount feature standardized and one-hot-encoding features.	5	We identify cluster 0 that performs operations between 1 originator (Ministry of Finance) and 1 single beneficiary participant (Bank 2). The identification of an anomalous cluster is not clear.
Model 2	*K-means* + the complete set of features were standardized.	3	We identify cluster 0 that performs operations between 1 originator (Ministry of Finance) and 1 single beneficiary participant (Bank 2). We identify cluster 1 that performs operations between 1 originator (Ministry of Finance) and all beneficiary participants (private banks). We identify cluster 2 that show the interaction of 2 new participants of origin (The Development Bank of El Salvador and E-Money Provider), which requires attention from the authorities, since it is a different behavior.
Model 3	*DBSCAN* + network and amount feature standardized and one-hot-encoding features.	4	We identify cluster 0 that performs operations between 1 originator (Ministry of Finance) and 1 single beneficiary participant (Bank 2). We identify cluster 2, which carries out operations for a new participant, although not with great accuracy because it leaves out important operations. The identification of an anomalous cluster is not clear.
Model 4	*DBSCAN* + the complete set of features standardized.	9	We identify 8 different clusters that indicate operations between the same source participant (Ministry of Finance) and 1 beneficiary participant per cluster (8 different banks). We identify the cluster 1, which could determine an anomalous behavior.

5.3. Features obtained from a random forest trained for each of models' clusters

In Appendix E can be observed firstly that the random forests trained are consistent with features importance, that is, the most relevant features for the prediction of the clusters in all models were beneficiary participant degree, beneficiary participant strength degree and number of interactions. Similarly, the less relevant features are consistent for all the models too, whose are the amount and the origin participant strength (for two models).

It is worth noting that the origin participant degree turned out to be a relevant feature for Model 1 and Model 4, having that for Model 1 its importance was greater than the beneficiary participant degree and strength.

5.4. Summary of the models' results

In this section, we conclude that models 2 and 4 are the ones that best fit the needs of the Payment Systems Surveillance of the Central Reserve Bank of El Salvador". This conclusion has been reached because with the tests that were carried out, it was determined that the algorithm was able to identify structural changes in the participants, an example of this is that in model 2, cluster 2, the algorithm captures the participation of 2 new actors, mainly the entry into force of "electronic money" in El Salvador operations that are transacted by the SPM, an event that was graphed in the "Appendix B", marked in red, a fact that was verified by knowledge of the business and the results match the dates. This event was key to selecting model 2. On the other hand, model 4 generates 9 different clusters, 8 of them determine the participation between 1 participant of origin versus 1 of destination, and a ninth cluster that could be considered suspicious. The relevant thing about these 8 clusters is that none of the other models separated the transactions one by one (origin vs destination) and a ninth cluster that makes a mix of transactions that must be checked but for this we need to get more in the operations, something which is extended for other studies. In sum, we present the summary of the 4 models in the next Table 2, we found very interesting results, listed below:

Based on the findings, we conclude that models 2 and 4 are the ones that best fit the needs of the Payment Systems Surveillance of the Central Reserve Bank of El Salvador. Appendix A–C show more evidence in this regard. This analysis helps us to explain how these features influenced the different models for the cluster's creation, where the extreme values are related to the grouping of operations with these characteristics.

5.5. How good each cluster separates the data

The Table 3 shows the results of three metrics that are individually computed for each model and is intended to compare through different criteria (described on detail in the methodology section) the partition quality for the clusterings created. It can be observed that model 1 yielded the best performance in two of the three metrics. However, the model 2 shows a better result and the model 1 is the next best performer, under the Davies-Bouldin index. Therefore, we observed that model 1 generates best separation clusters in terms of intra-cluster homogeneity and more heterogeneity between clusters' members.

Table 4 shows a pairwise comparison of the clusterings to see how similar are the partitions created. Model 3 has the highest index scores, being more similar to the Model 1 and Model 2 than with Model 4. Also, the cluster assignation between models 1 and

Table 3
Clusters' assessment metrics. Comparison between the trained models using assessment metrics that evaluate how well the clusters are separating the data, this using different criteria such as the distance between the members of a cluster to its centroid and to the other centroids, the dispersion within of a cluster and with respect to the rest, among others.

Model	Silhouette Index	Calinski-Harabasz Index	Davies-Bouldin Index
Model 1	0.072201	10,307.607	3.886
Model 2	-0.29455	6320.188	2.049
Model 3	-0.13381	2357.366	6.049
Model 4	-0.37454	124.206	4.166

Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.

Table 4
Adjusted Rand index for all the models. Pairwise comparison between the four models through the Rand index, where value close to zero represent a random cluster labeling, and values close to one represent very similar cluster labeling.

	Model 1	Model 2	Model 3	Model 4
Model 1	1			
Model 2	0.79191527	1		
Model 3	0.78580545	0.94591571	1	
Model 4	0.50335022	0.5083992	0.52593604	1

Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.

2 is similar according to the adjusted rand index. Model 4 created the most dissimilar clusters compared with the rest of the models. Finally, the most similar clusters are those that corresponds to Model 2 and Model 3.

6. Conclusions

We investigated the optimal procedure of feature selection and denoising for clustering financial transactions with the aim of detecting clusters of anomalous payments in the SPM, which is SIPS operated by the BCR under its RTGS infrastructure. Our analysis could be relevant for oversight purposes as it allows to have an insightful, granular, and advanced examination on the possible atypical payments that could constitute a risk for the payment system, financial system, and overall economy of El Salvador. It could become a powerful tool to monitor the activity of the SPM, once the *Transfer365* made it possible to open access for more participants and enable new types of retail payments, to be done- for instance faster payments such as in Brazil, Mexico or Dominican Republic.

We decided to use standard clustering methodologies- that is to say, *k-means, DBSCAN* and random forest and analyzed the impact of feature selection on the clusters that can be obtained. We also found that network features provide consistent clusters - whether PCA denoising is applied or not - and that one-hot encoding is a promising method to include information at the institutional-level, as they can significantly change the clusters identified by network features.

We obtained four different models, of which we analyzed the statistical distribution of the network features of transactions belonging to different clusters. We performed this to identify clusters with transactions with significantly different distributions of features, such as, displaying very large out-volumes. For this analysis, we focused on the most relevant variables: Amount, Beneficiary participant Degree, Origin counterparty Degree, Beneficiary participant Strength and Interaction.

Our analysis concludes that the number of interactions between the participants indicates the same intuition as the degree of beneficiary and origin counterparty. This means that to identify and identify anomalous behavior, authorities should check the direction (origin-beneficiary participant) of a transaction and the number of interactions between SPM participants.

When analyzing the characteristics of all the models separately, in some cases, we found that *k-means* cluster results that are more useful than DBScan and vice versa, therefore, it becomes important to explore the clustering offered by each of these two techniques before issuing precise conclusions.

In sum, the ability to single out consistent clusters with robust feature distributions, including some containing transactions following unusual patterns, with a simple and interpretable methodology could be a "jump" for the automation of in-depth monitoring tools underpinning the oversight of payment systems. However, the knowledge of payment overseers is irreplaceable and should always be at the fore of the use of these novel techniques and approaches.

Future research in the area can lead to enhanced and adaptable methodologies for oversight purposes given the increasing complexity and relevance of systems like the SPM. This could possibly involve the use of other complex unsupervised techniques in machine learning. In our best knowledge, our approach contributes to the literature by suggesting a novel tool using Machine Learning techniques to improve risk-detection activities by central banks' overseers.

Disclaimer

Any errors in this paper are the sole responsibility of the authors. This paper reflects the authors' views and does not reflect those of Central Reserve Bank of El Salvador, CEMLA or UCL. We appreciate the valuable comments of Serafín Martínez.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A

We can underline that 2020 was the year of higher amounts settled mainly due to the increase in operations of Ministry of Finance, which increased 8.1%, especially operations related to payment to suppliers, amid the pandemic.

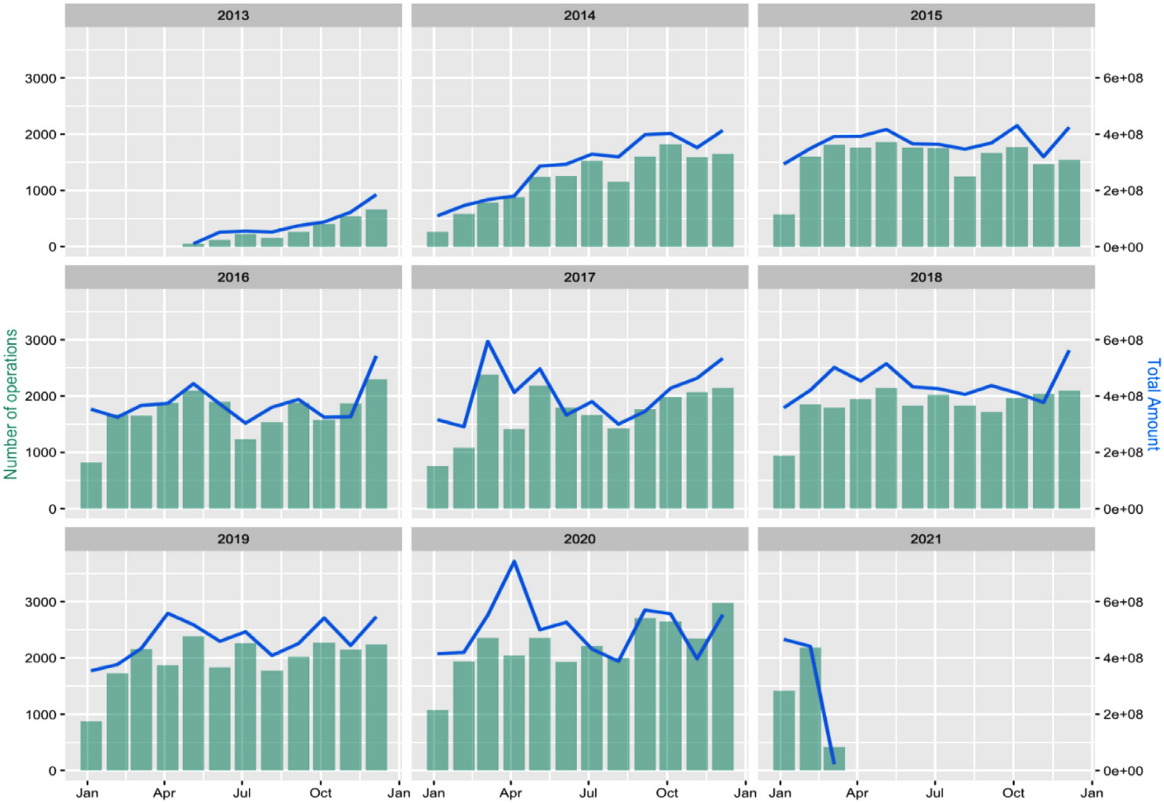


Fig. A. Bar plot of number of operations (left y-axis) and line plot number of participants (right y-axis), since 2015 to September 2020 Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.

Appendix B

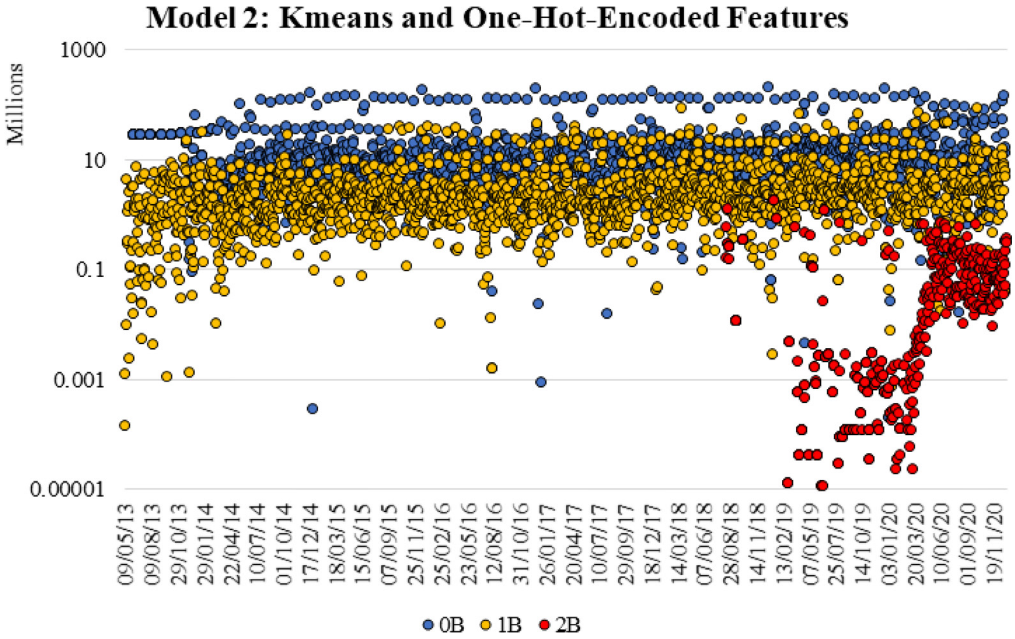


Fig. B. *K-means* and One-hot-encoded features. Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.

Appendix C

This Figure shows the origin (blue) and the beneficiary (red) participants, and the center value represents the number of interactions with all participants. Ministry of Finance as a participant of origin has the highest number of interactions and entity 2 has the highest number of interactions as a beneficiary participant.

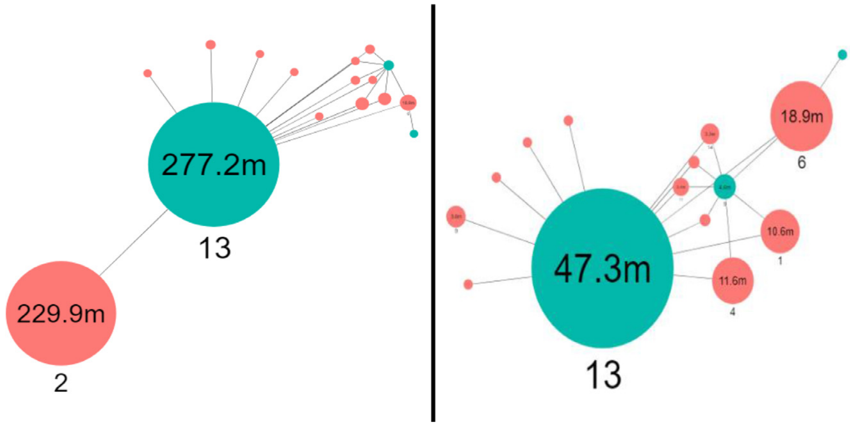
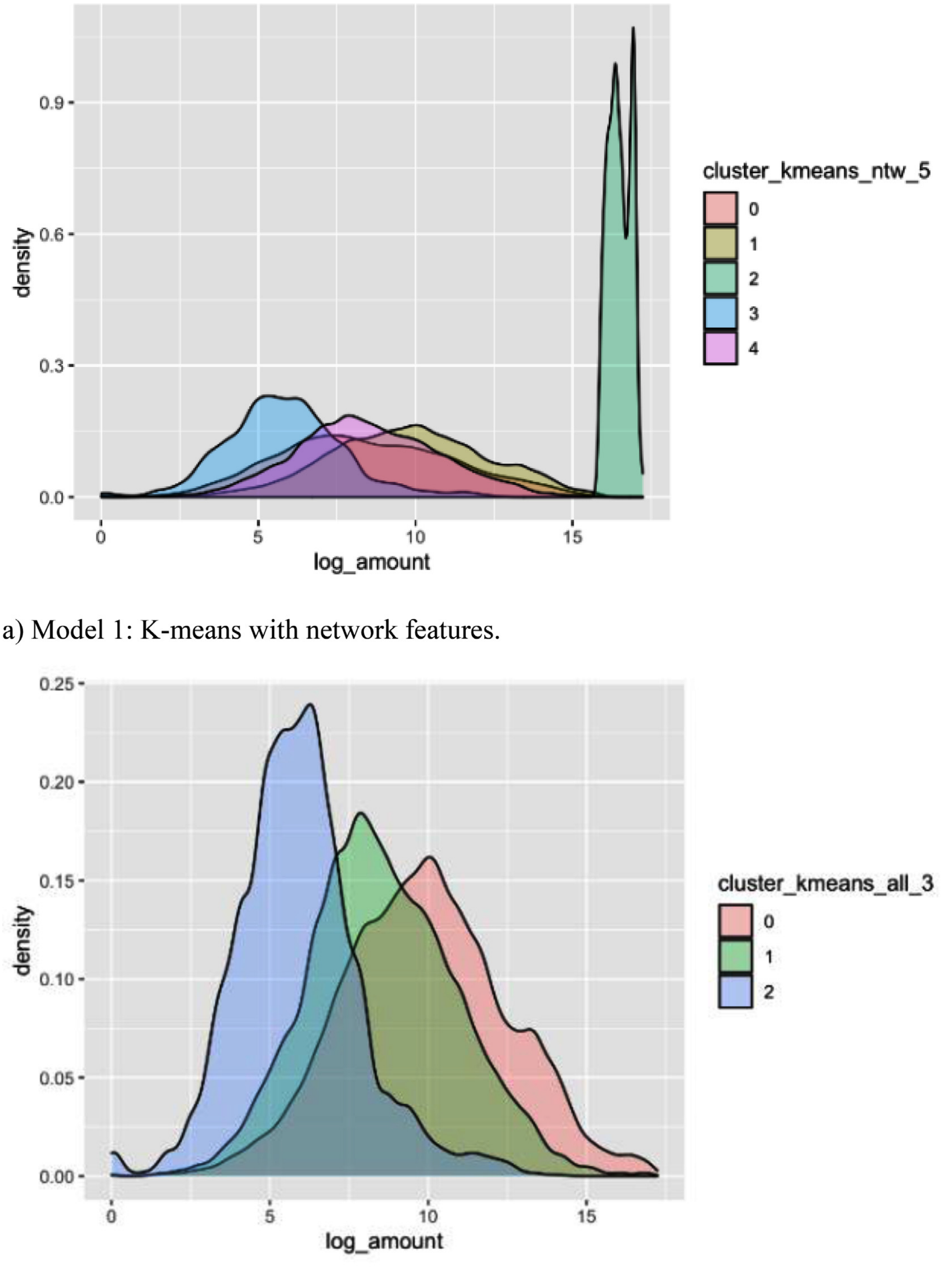


Fig. C. Representation of interaction between origin participant and beneficiary participants. In the left side can be see all the beneficiary participant and in the right side the Bank 2 has been removed.
Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.

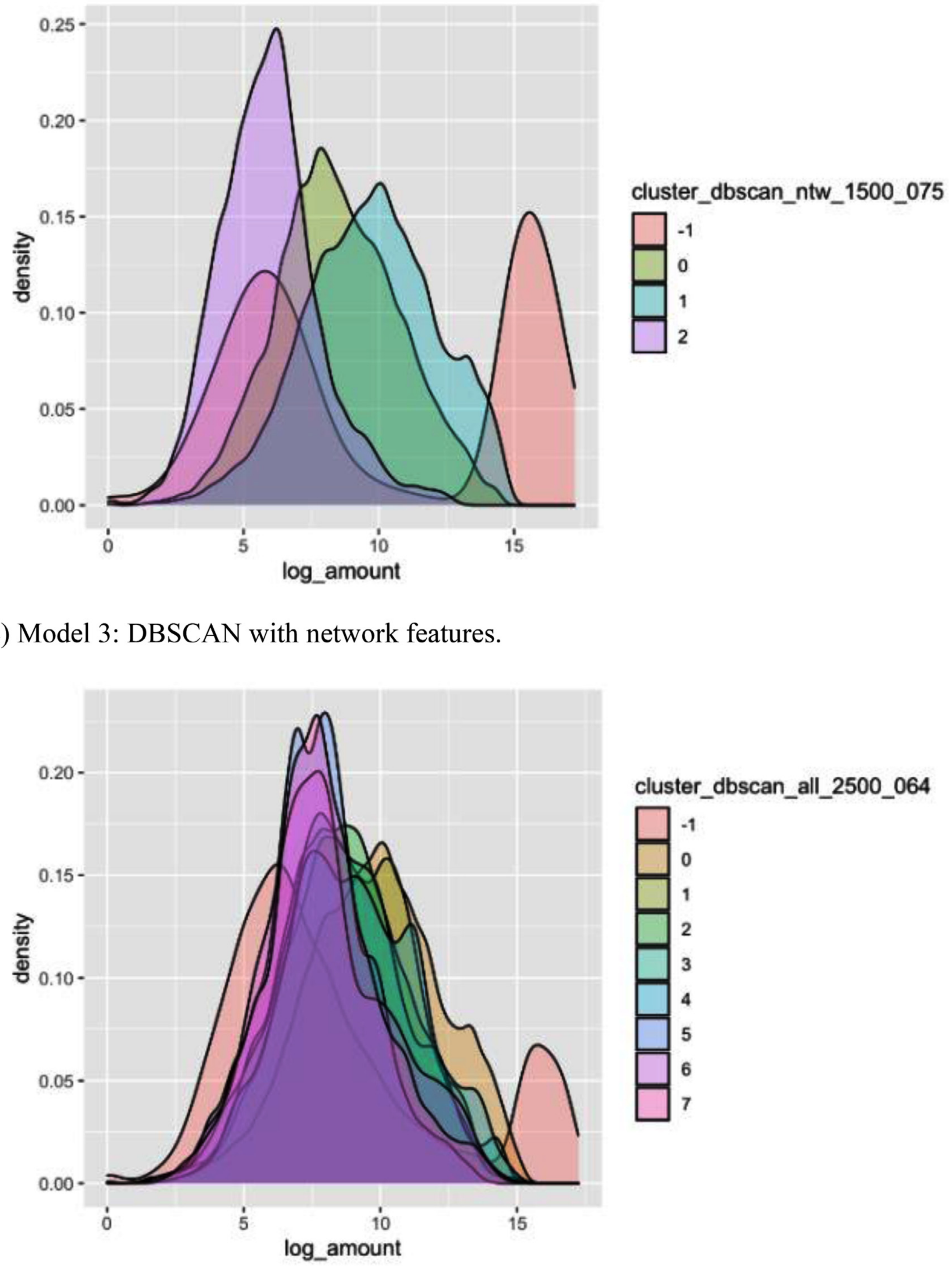
Appendix D. Results of the models



a) Model 1: K-means with network features.

b) Model 2: K-means all features standardized.

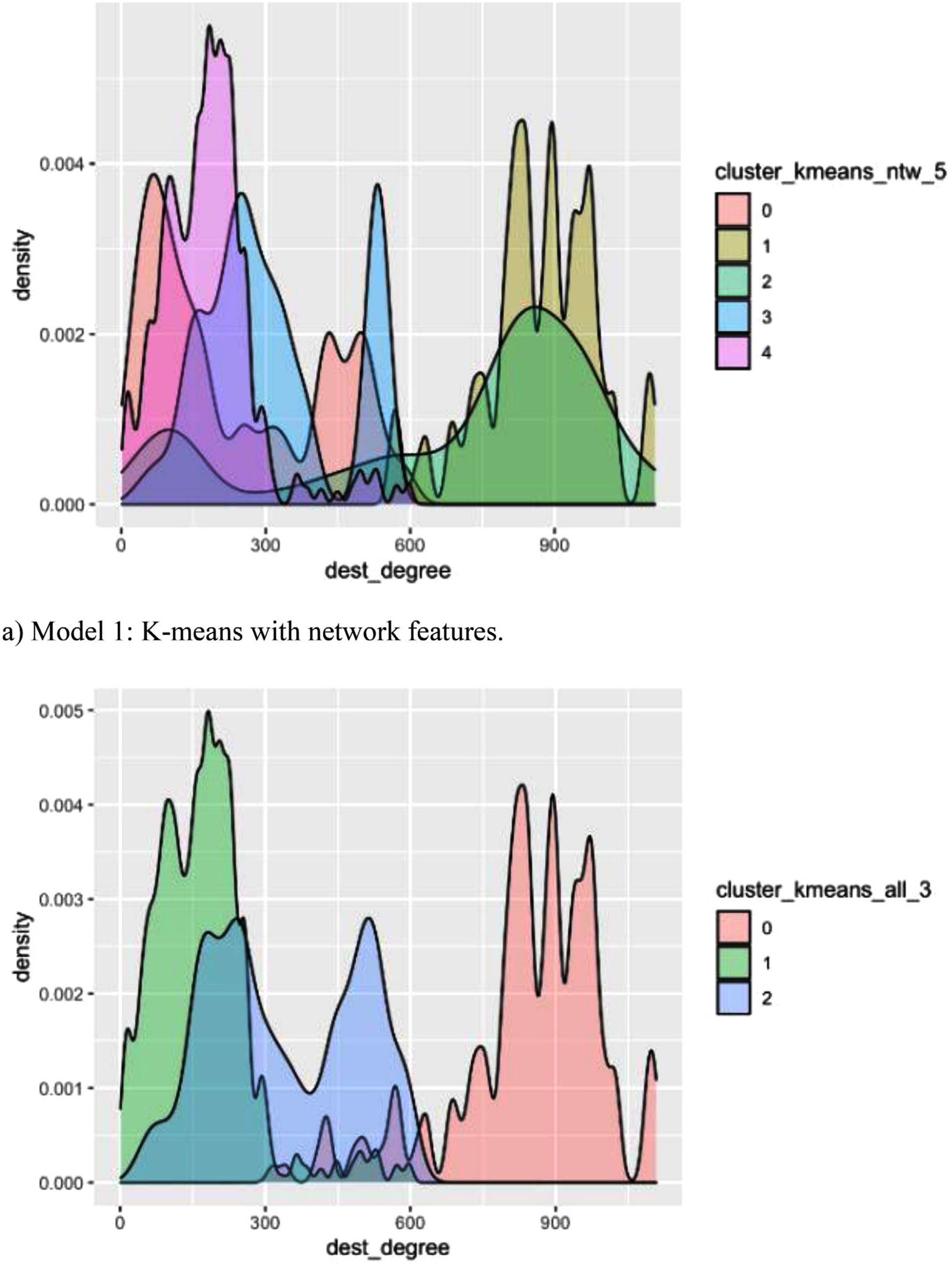
Fig. D1. Figures for amount feature. Four models clusters' distribution plots for the logarithmic amount. Each panel represent how clusters distributes for each model. The x-axis represents the logarithmic amount and y-axis represents the density that each cluster has over the range of values for the logarithmic amount. Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador. (a) Model 1: *K-means* with network features. (b) Model 2: *K-means* all features standardized. (c) Model 3: *DBSCAN* with network features. (d) Model 4: *DBSCAN* all features standardized.



c) Model 3: DBSCAN with network features.

d) Model 4: DBSCAN all features standardized.

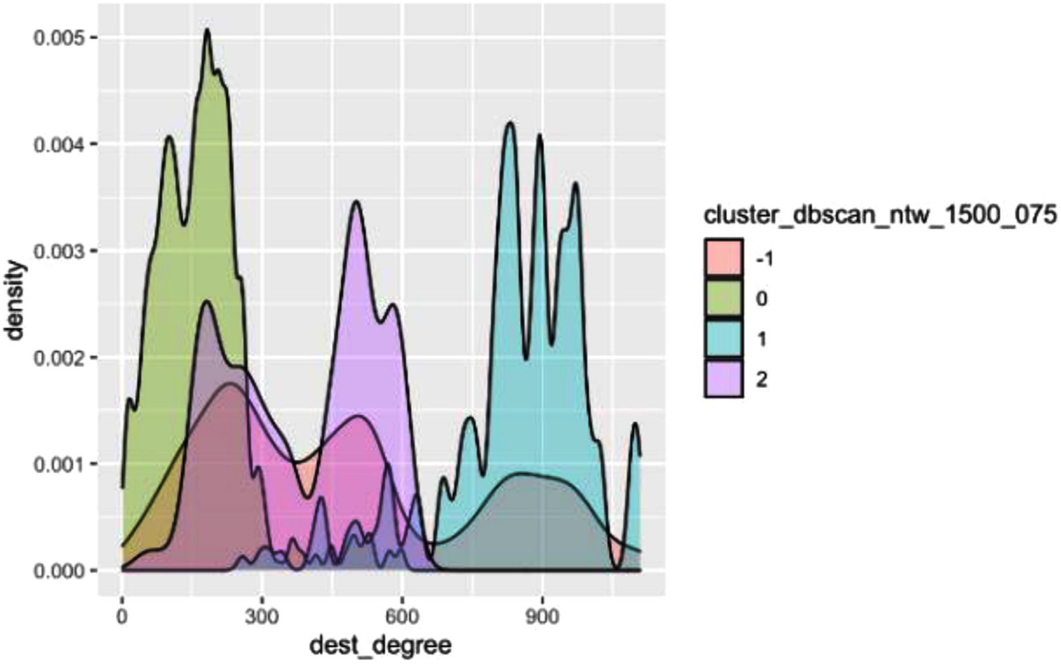
Fig. D1. Continued



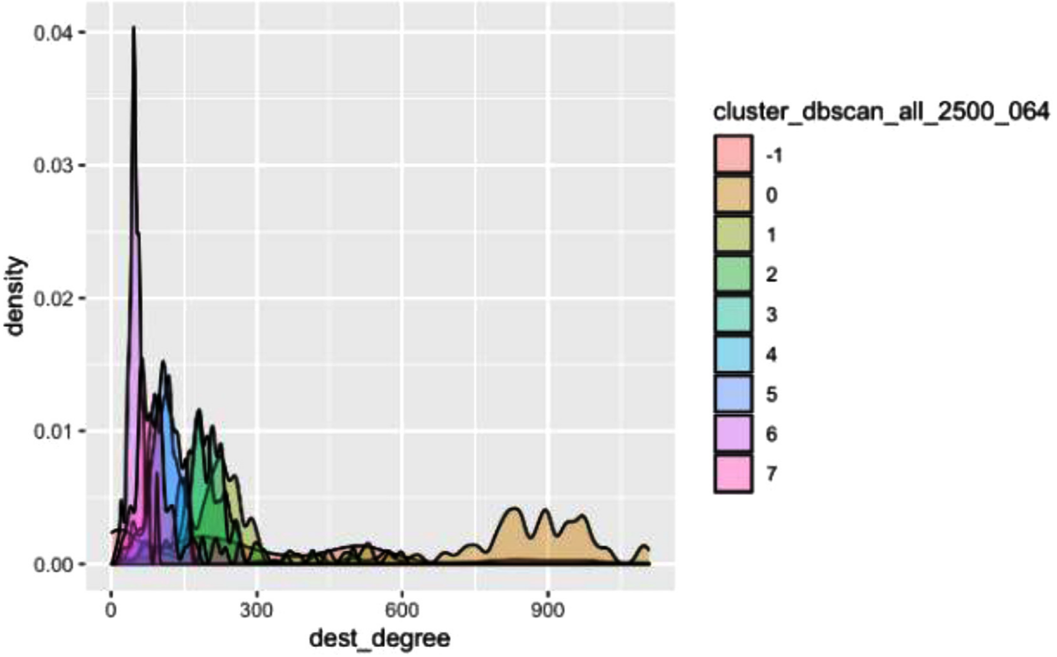
a) Model 1: K-means with network features.

b) Model 2: K-means all features standardized.

Fig. D2. Figures for destination degree feature. Four models clusters' distribution plots for the beneficiary counterparty degree. Each panel represent how clusters distributes for each model. The x-axis represents the beneficiary participant degree and y-axis represents the density that each cluster has over the range of values for the beneficiary counterparty degree. Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador (a) Model 1: *K-means* with network features. (b) Model 2: *K-means* all features standardized. (c) Model 3: *DBSCAN* with network features. (d) Model 4: *DBSCAN* all features standardized.

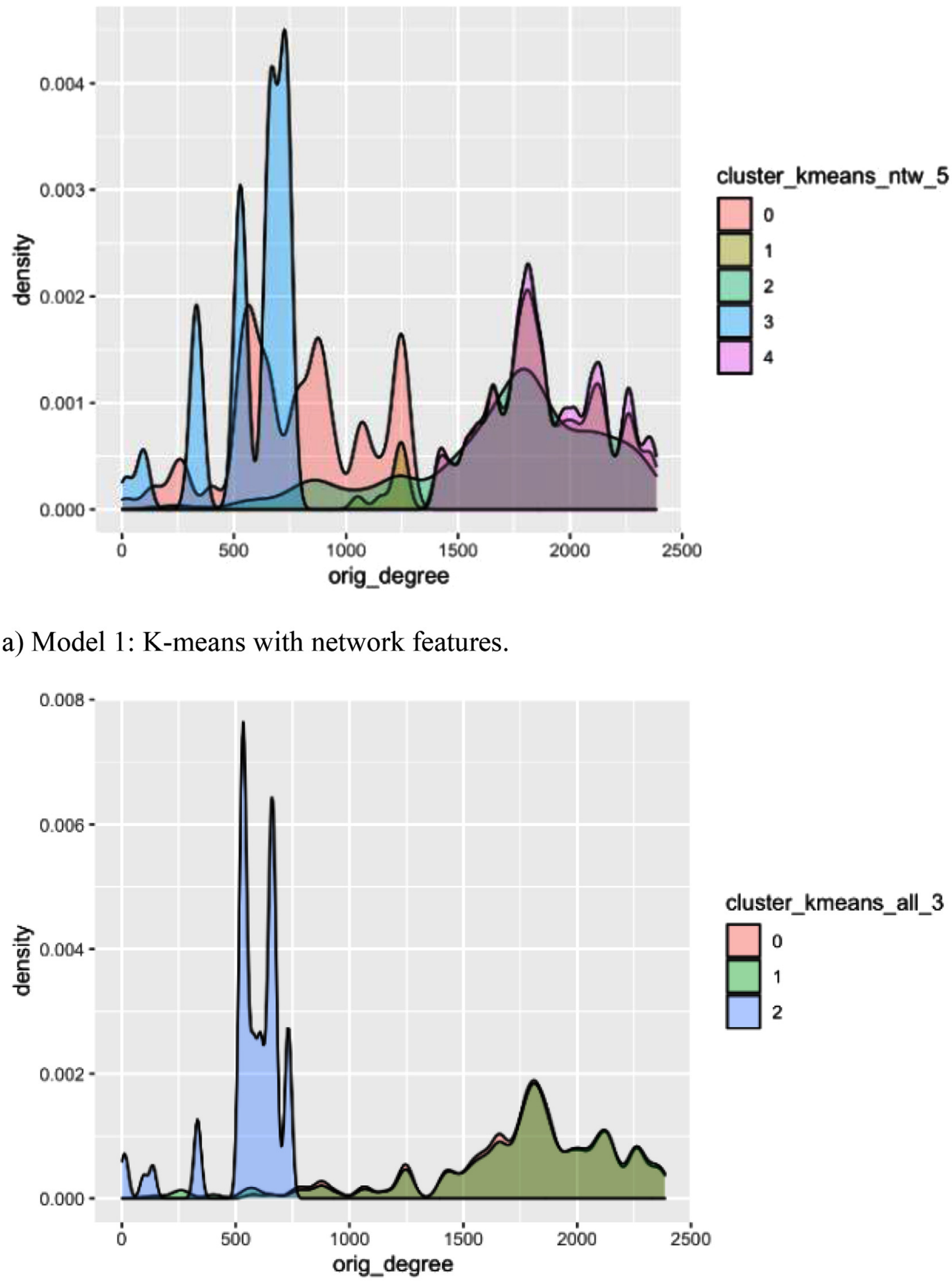


c) Model 3: DBSCAN with network features.



d) Model 4: DBSCAN all features standardized.

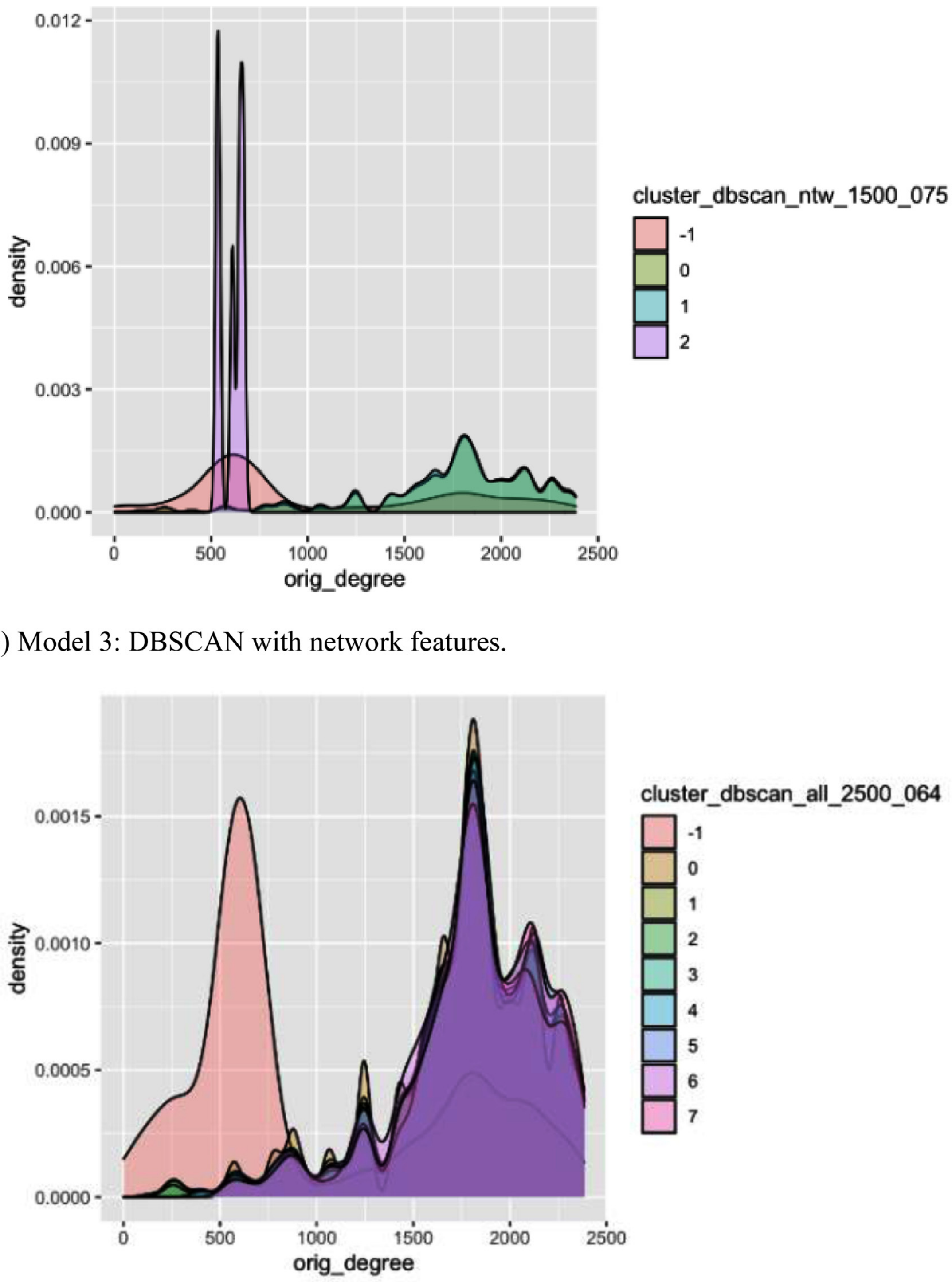
Fig. D2. Continued



a) Model 1: K-means with network features.

b) Model 2: K-means all features standardized.

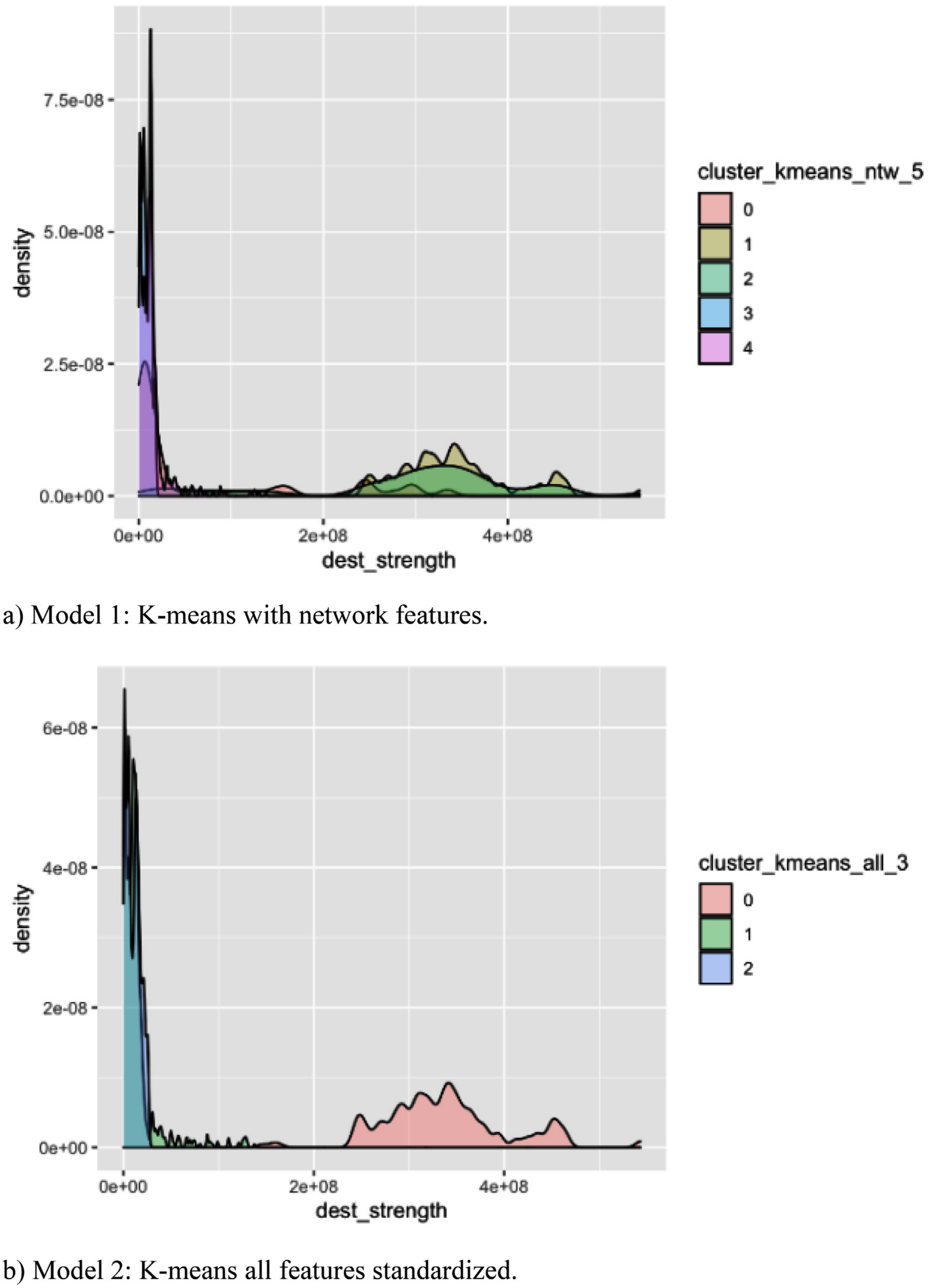
Fig. D3. Figures for Origin degree feature. Four models clusters' distribution plots for the origin counterparty degree. Each panel represent how clusters distributes for each model. The x-axis represents the origin participant degree and y-axis represents the density that each cluster has over the range of values for the origin participant degree. Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador a) Model 1: *K-means* with network features. (b) Model 2: *K-means* all features standardized. (c) Model 3: *DBSCAN* with network features. d) Model 4: *DBSCAN* all features standardized.



c) Model 3: DBSCAN with network features.

d) Model 4: DBSCAN all features standardized.

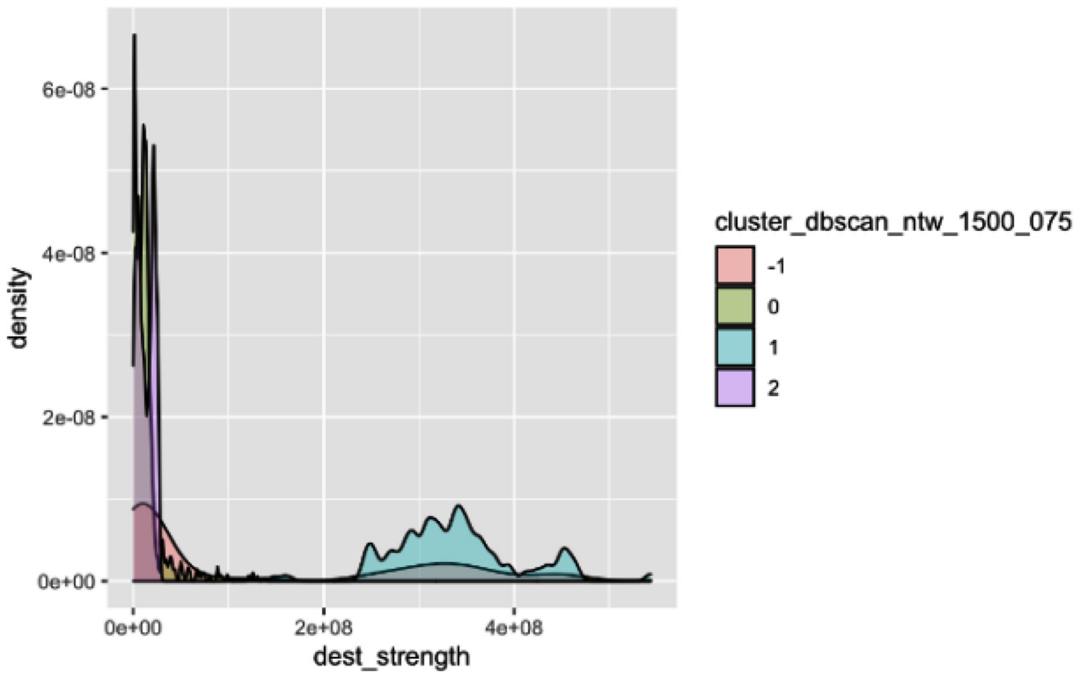
Fig. D3. Continued



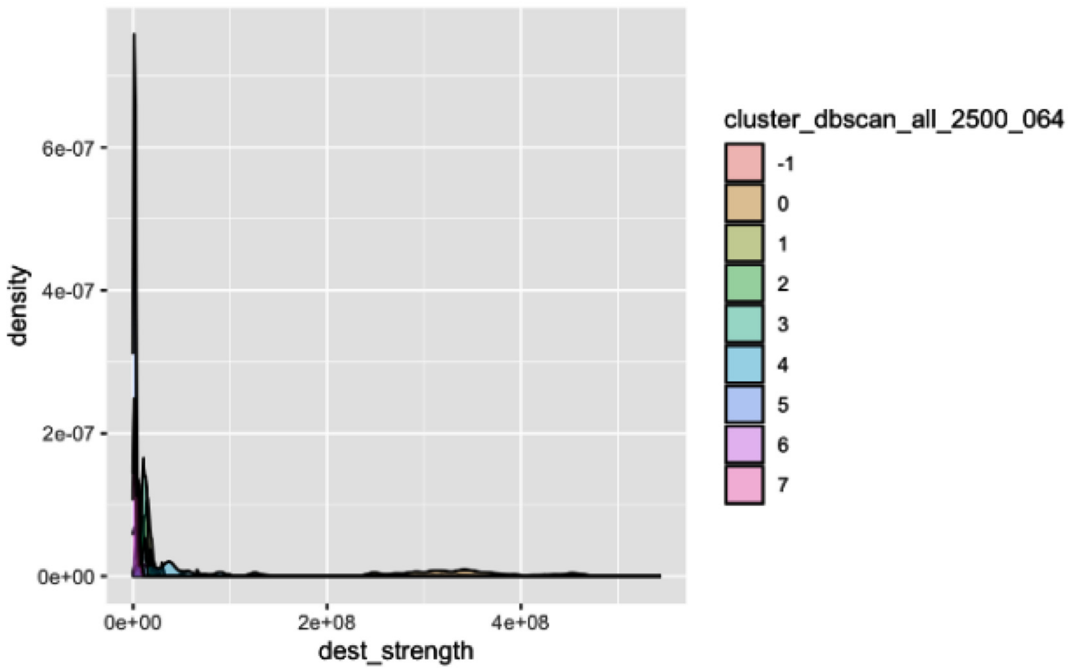
a) Model 1: K-means with network features.

b) Model 2: K-means all features standardized.

Fig. D4. Beneficiary participant strength feature. Four models clusters' distribution plots for the beneficiary participant strength. Each panel represent how clusters distributes for each model. The x-axis represents the beneficiary participant strength and y-axis represents the density that each cluster has over the range of values for the beneficiary participant strength. Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador (a) Model 1: *K-means* with network features. (b) Model 2: *K-means* all features standardized. (c) Model 3: *DBSCAN* with network features. (d) Model 4: *DBSCAN* all features standardized.

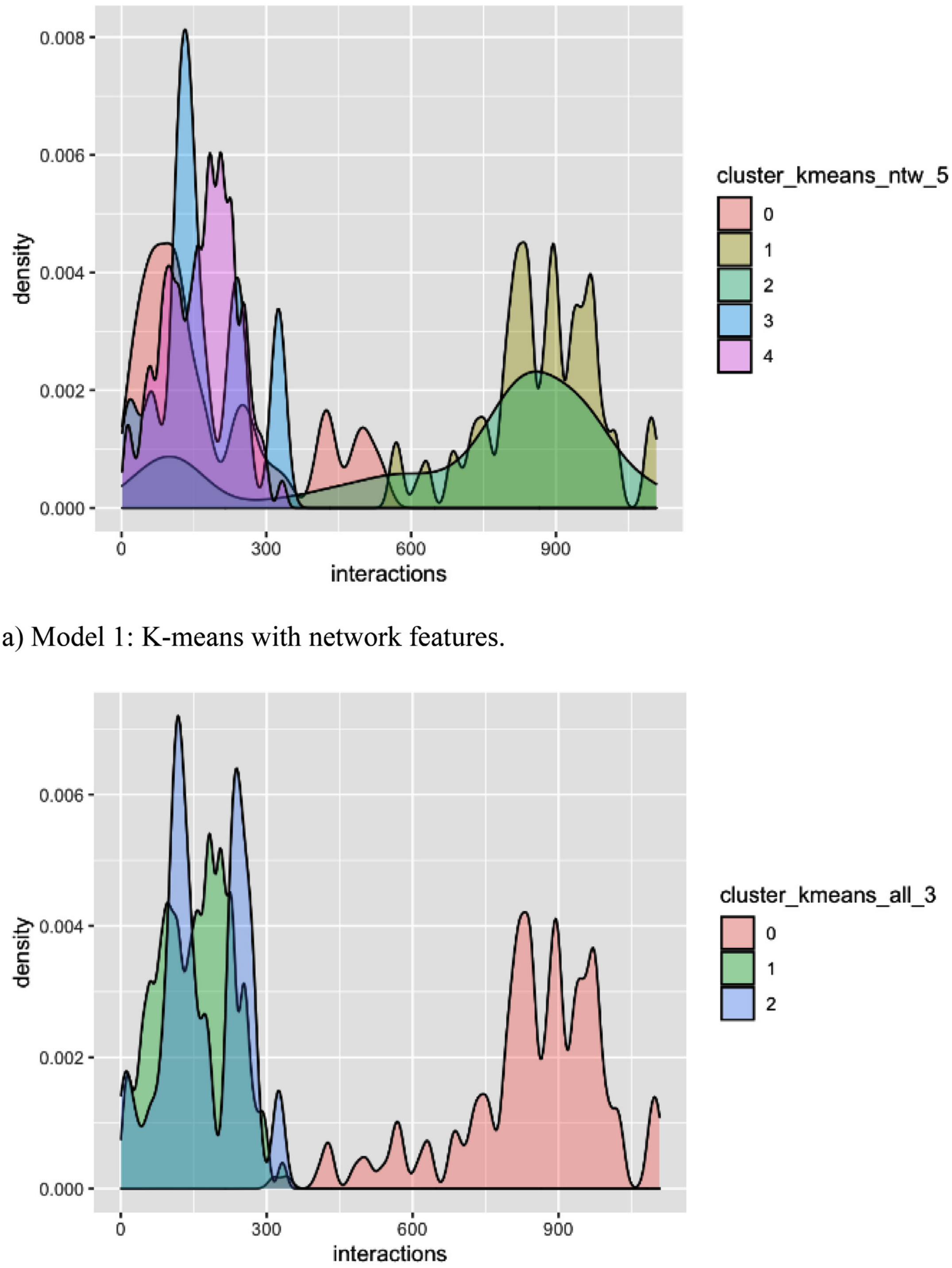


c) Model 3: DBSCAN with network features.



d) Model 4: DBSCAN all features standardized.

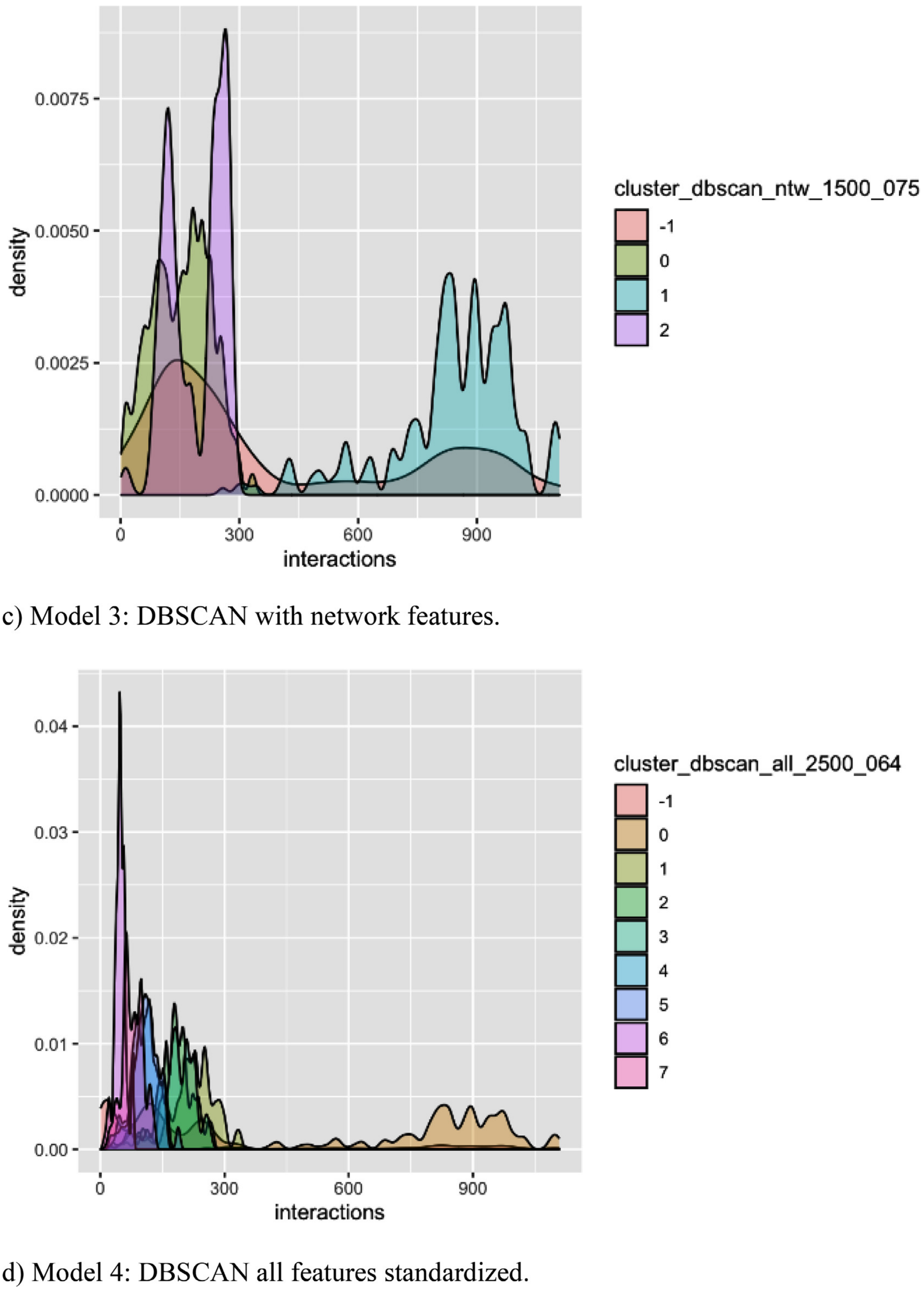
Fig. D4. Continued



a) Model 1: K-means with network features.

b) Model 2: K-means all features standardized.

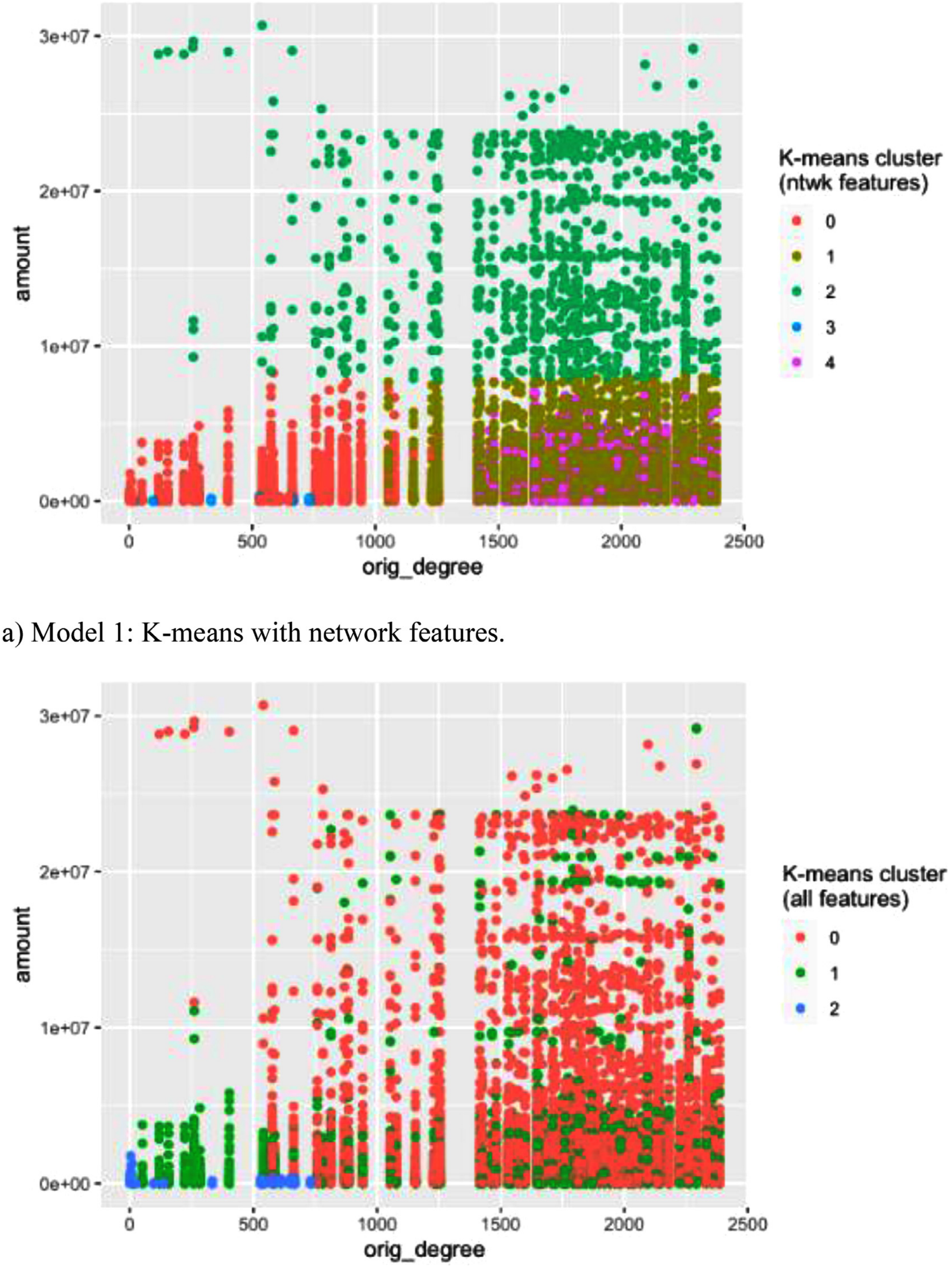
Fig. D5. Figures for interaction feature. Four models clusters' distribution plots for the number of interactions between the participants that are settling an operation. Each panel represent how clusters distributes for each model. The x-axis represents the number of interactions between participants settling an operation and y-axis represents the density that each cluster has over the range of values for the interactions. Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador (a) Model 1: *K-means* with network features. (b) Model 2: *K-means* all features standardized. (c) Model 3: *DBSCAN* with network features. (d) Model 4: *DBSCAN* all features standardized.



c) Model 3: DBSCAN with network features.

d) Model 4: DBSCAN all features standardized.

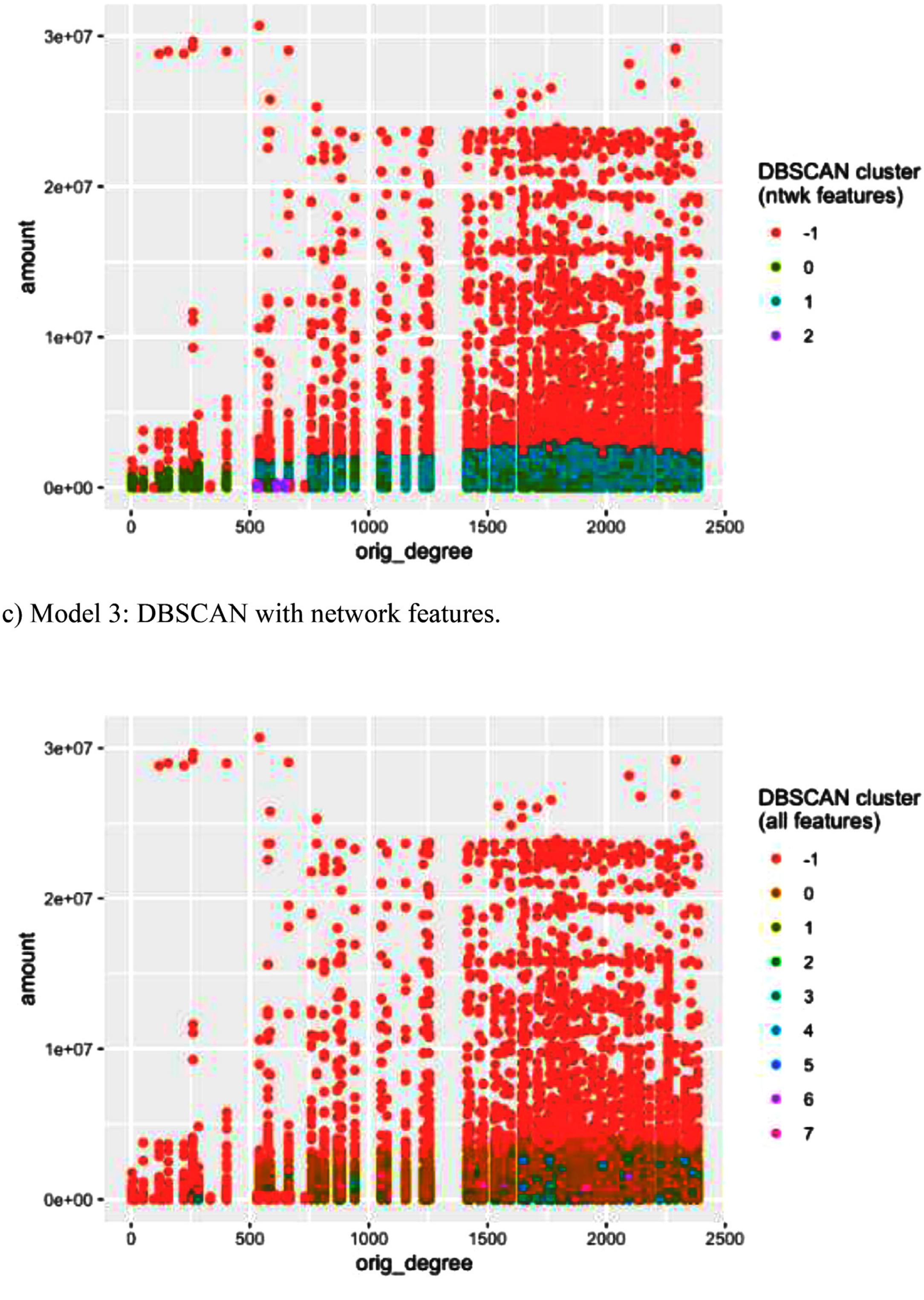
Fig. D5. Continued



a) Model 1: K-means with network features.

b) Model 2: K-means all features standardized.

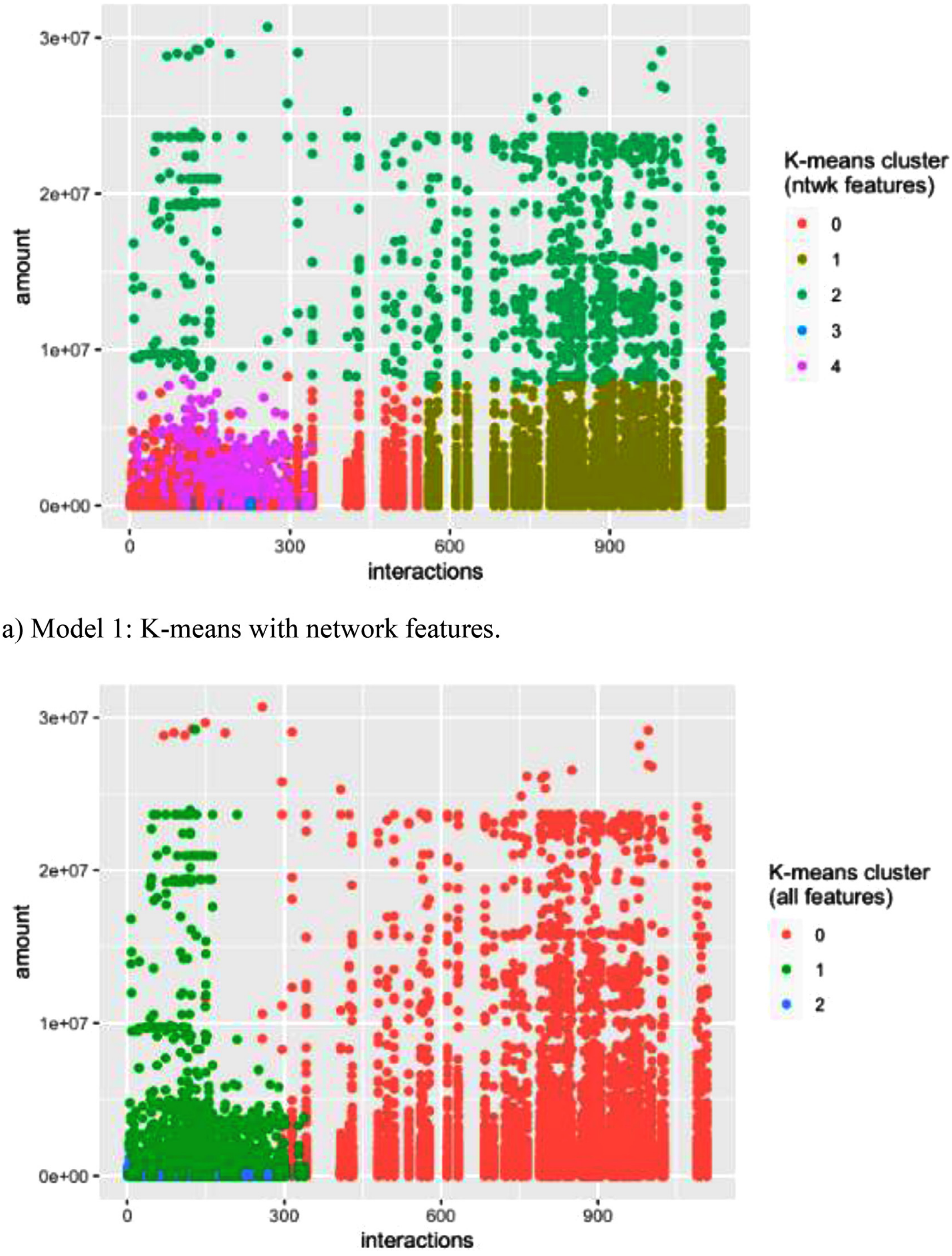
Fig. D6. Figures for amount vs origin participant degree. Scatterplot between amount and origin participant degree. The four panels correspond to one of the four models. The dots are colored depending on each operation belongs. The x-axis is representing the origin participant degree and y-axis represent the amount of every operation. Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.(a) Model 1: *K-means* with network features. (b) Model 2: *K-means* all features standardized. (c) Model 3: *DBSCAN* with network features. (d) Model 4: *DBSCAN* all features standardized.



c) Model 3: DBSCAN with network features.

d) Model 4: DBSCAN all features standardized.

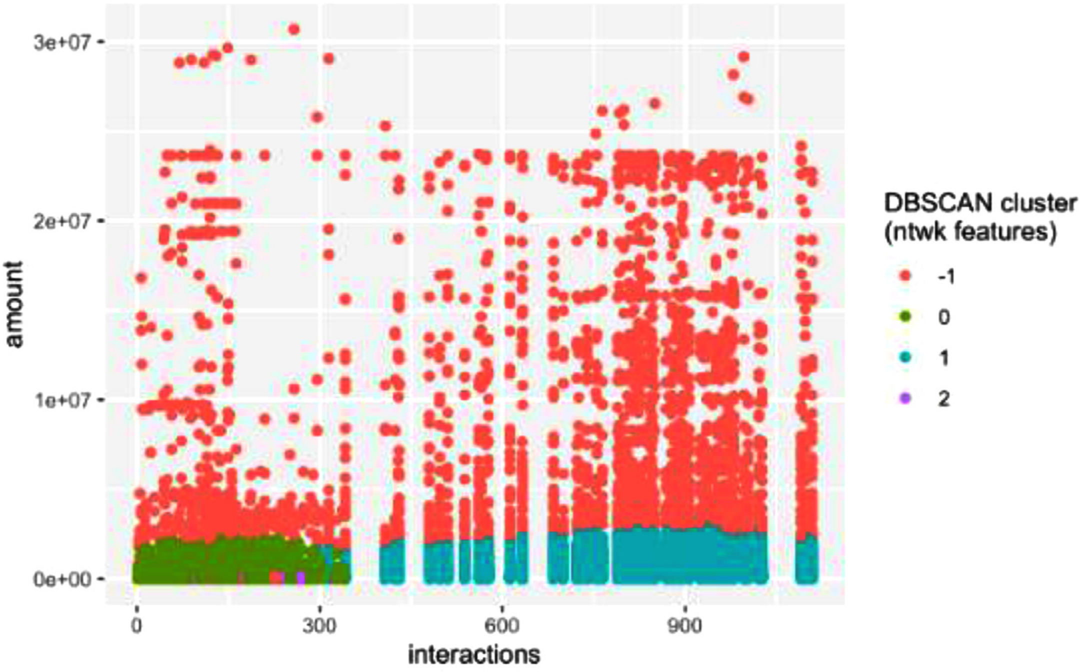
Fig. D6. Continued



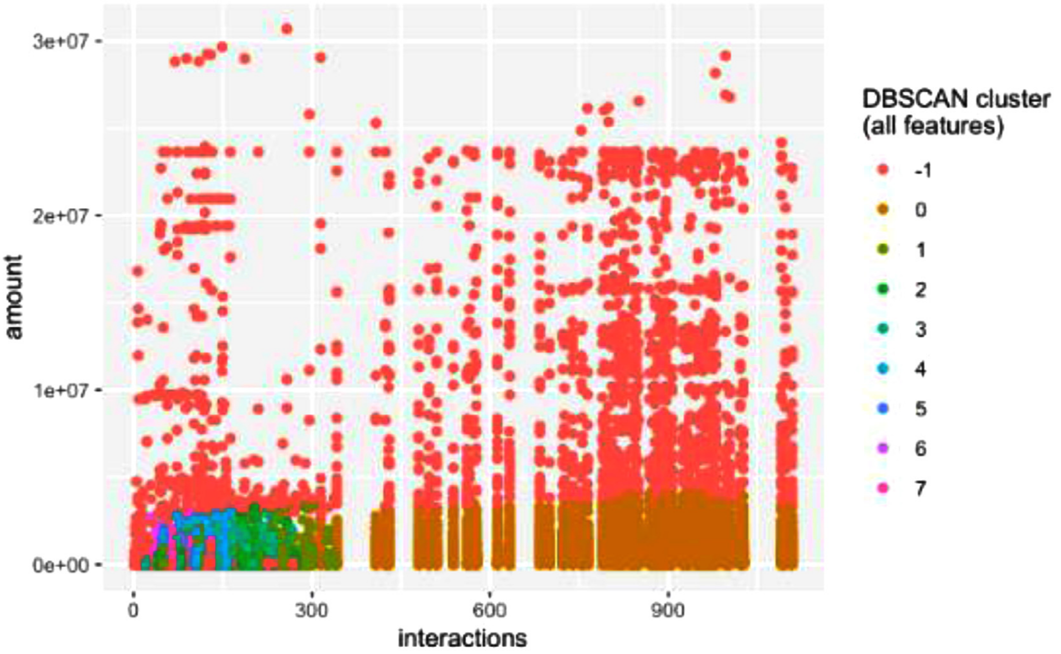
a) Model 1: K-means with network features.

b) Model 2: K-means all features standardized.

Fig. D7. Figures for Amount vs participants' interactions. Scatterplot between participants' interactions and the amount. The four panels correspond to one of the four models. The x-axis is representing the number of interactions between the participants settling the operation and y-axis represent the amount of every operation, the dots are colored depending on each operation belongs. Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador. (a) Model 1: *K-means* with network features. (b) Model 2: *K-means* all features standardized. (c) Model 3: *DBSCAN* with network features. (d) Model 4: *DBSCAN* all features standardized.

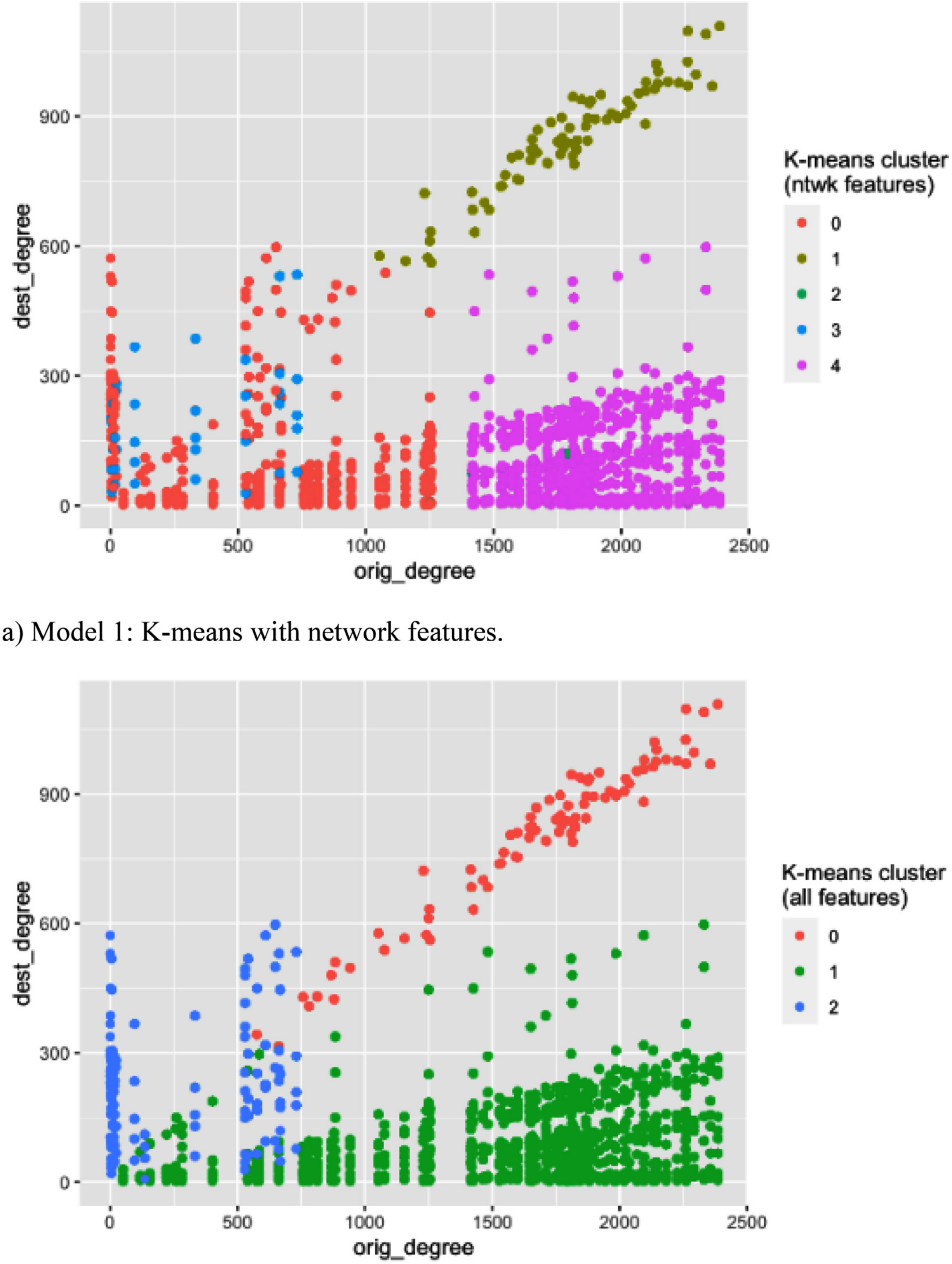


c) Model 3: DBSCAN with network features.



d) Model 4: DBSCAN all features standardized.

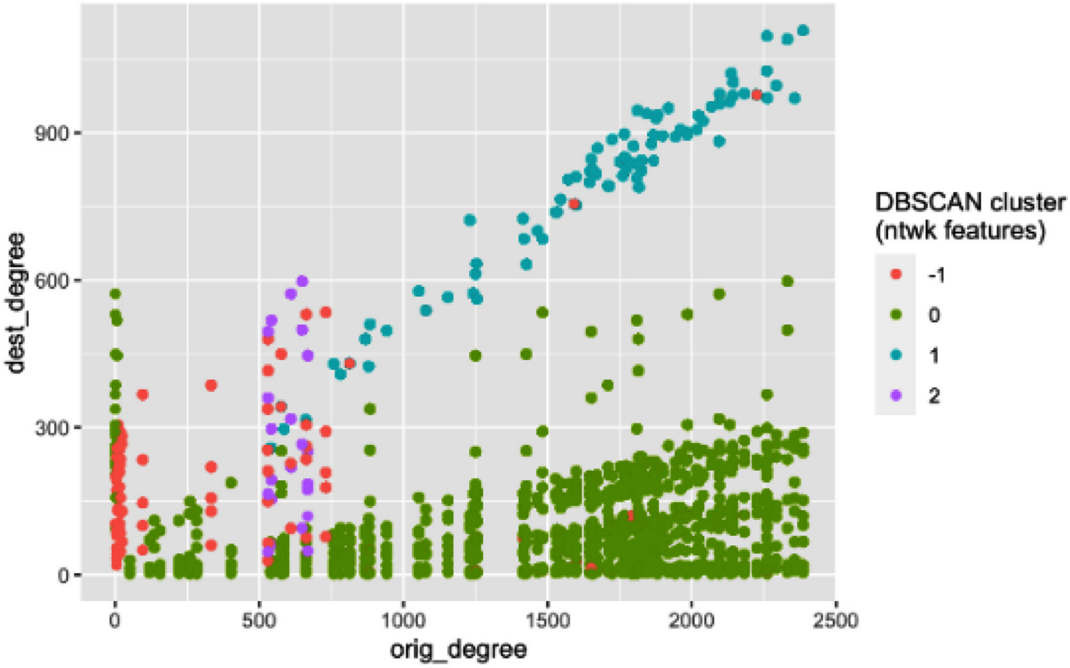
Fig. D7. Continued



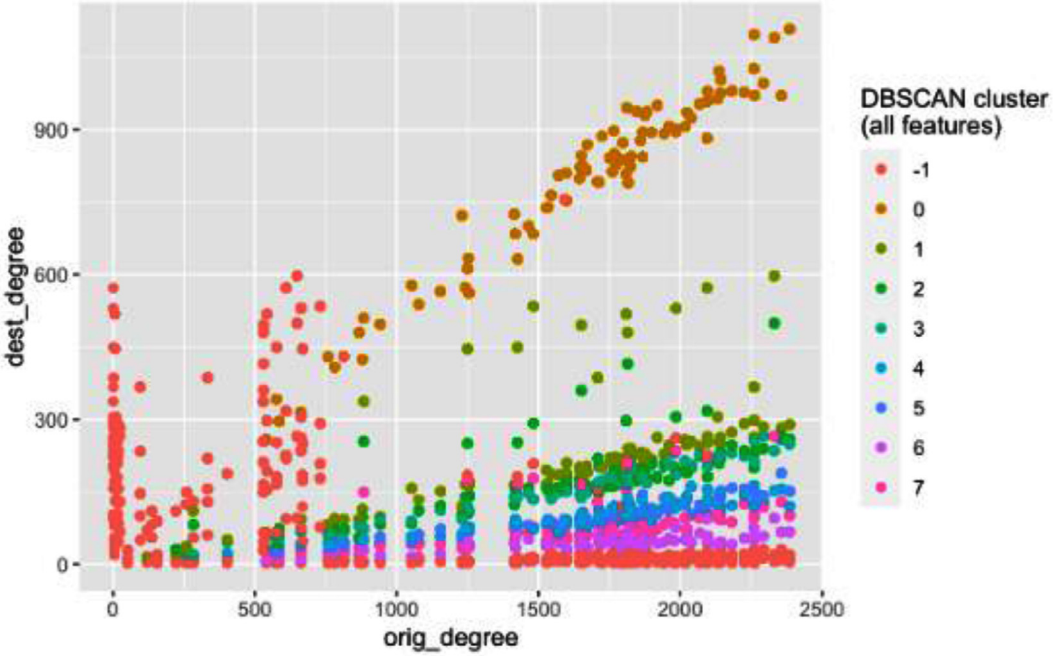
a) Model 1: K-means with network features.

b) Model 2: K-means all features standardized.

Fig. D8. Figures for Beneficiary participant and origin participant degree. Scatterplot between beneficiary participant and origin participant degree. The four panels correspond to one of the four models. The x-axis is representing the origin participant degree and y-axis represent the beneficiary participant degree, the dots are colored depending on each cluster belongs. Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador (a) Model 1: *K-means* with network features. (b) Model 2: *K-means* all features standardized. (c) Model 3: *DBSCAN* with network features. (d) Model 4: *DBSCAN* all features standardized.



c) Model 3: DBSCAN with network features.



d) Model 4: DBSCAN all features standardized.

Fig. D8. Continued

Appendix E

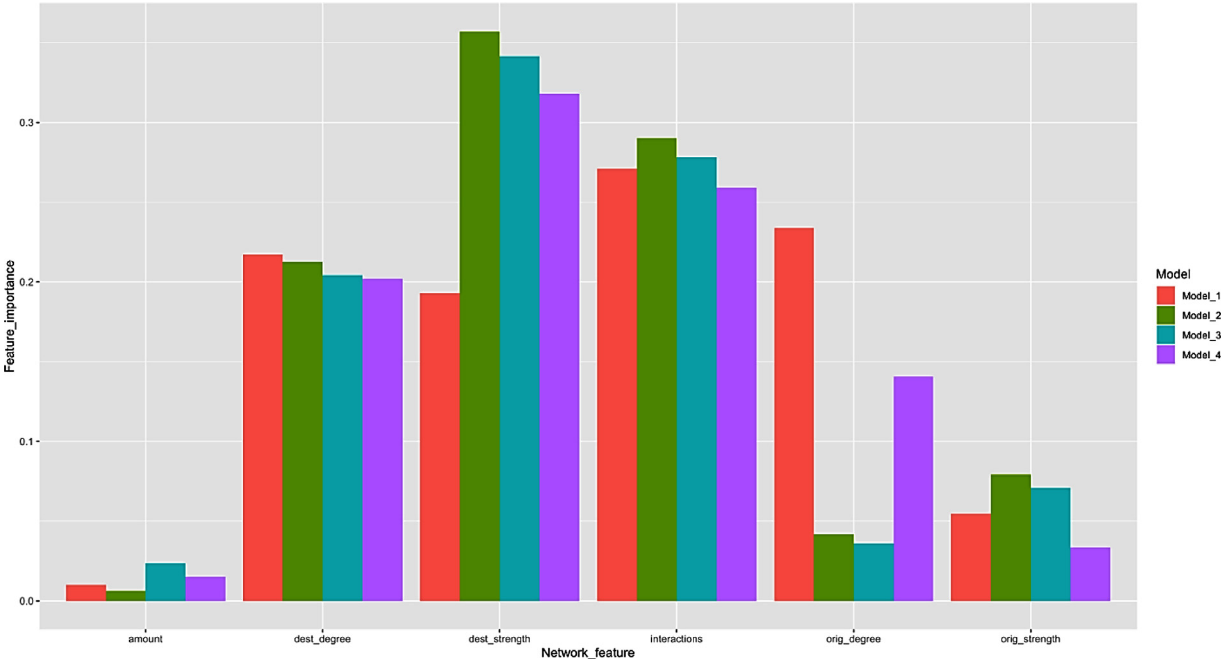


Fig. E. Feature importance bar-plot for the most relevant features obtained from a Random Forest trained for each of models' clusters. The x-axis represents the most relevant the network features used for the random forest training. Y-axis represents the feature importance of each variable, where the Gini index was the measure used. The bars colors are related to each of the clusterizations obtained for the four models. Source: Authors' elaboration based on information from the Central Reserve Bank of El Salvador.

References

Baek, S., Kwon, D., Suh, S.C., Kim, H., Kim, I., Kim, J., 2021. Clustering-based label estimation for network anomaly detection. Digit. Commun. Netw. 7 (1), 37–44.

Barucca, P., Lillo, F., 2018. The organization of the interbank network and how ECB unconventional measures affected the e-MID overnight market. Comput. Manag. Sci. 15 (1), 33–53.

Bech, M.L., Atalay, E., 2010. The topology of the federal funds market. Phys. A 389 (22), 5223–5246.

Berndsen, R., Heijmans, R., 2020. Risk indicators for financial market infrastructures: from high frequency transaction data to a traffic light signal. J. Risk 2 (3), 39–64.

Bolton, R.J., Hand, D.J., 2001. Unsupervised profiling methods for fraud detection. Credit scoring and credit control VII 235–255.

Caliński, T., Harabasz, J., 1974. A dendrite method for cluster analysis. Communications in Statistics-theory and Methods 3 (1), 1–27.

Chan, P.K., Mahoney, M.V., Arshad, M.H., 2003. A machine learning approach to anomaly detection (CS-2003-06). Florida Institute of Technology, Melbourne, FL.

Chandola, V., Eilertson, E., Ertoz, L., Simon, G., Kumar, V., 2006. Data Mining for Cyber Security, Data Warehousing and Data Mining Techniques for Computer Security. Springer Verlag.

Chandola, V., Banerjee, A., Kumar, V., 2009. Anomaly detection: a survey. ACM Comput. Surv. (CSUR) 41 (3), 1–58.

Collin, M., Cook, S., & Soramaki, K. (2016). The impact of anti-money laundering regulation on payment flows: Evidence from SWIFT Data. Center for Global Development Working Paper, (445).

Dasgupta, D., Nino, F., 2000. A comparison of negative and positive selection algorithms in novel pattern detection. In: Proceedings of the IEEE International Conference on Systems, Man and Cybernetics.'Cybernetics Evolving to Systems, Humans, Organizations, and Their Complex Interactions', 1. IEEE, pp. 125–130 Cat. no. 0.

Davies, D.L., Bouldin, D.W., 1979. A cluster separation measure. IEEE transactions on pattern analysis and machine intelligence 2, 224–227.

Eskin, E., 2000. Anomaly detection over noisy data using learned probability distributions. In: Proceedings of the 17th International Conference on Machine Learning. Morgan Kauf-mann Publishers Inc., pp. 255–262.

Esponda, F., Forrest, S., Helman, P., 2004. A formal framework for positive and negative detection schemes. In: Proceedings of the IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 34, pp. 357–373.

Ghosh, A.K., Wanken, J., Charron, F., 1998. Detecting anomalous and unknown intrusions against programs. In: Proceedings of the 14th Annual Computer Security Applications Conference. IEEE, pp. 259–267 (Cat. No. 98Ex217).

Glowka, M., Paulick, J., Schultze, I., 2017. The absence of evidence and the evidence of absence: an algorithmic approach for identifying operational outages in target2. J. Financ. Mark. Infrastruct. 6 (2–3), 63–91.

Hawkins, S., He, H., Williams, G., Baxter, R., 2002. Outlier detection using replicator neural networks. In: Proceedings of the International Conference on Data Warehousing and Knowledge Discovery. Springer, Berlin, Heidelberg, pp. 170–180.

Heller, K.A., Svore, K.M., Keromytis, A.D., Stolfo, S.J, 2003. One class support vector machines for detecting anomalous windows registry accesses. In: Proceedings of the Workshop on Data Mining for Computer Security.

Hu, W., Liao, Y., Vemuri, V.R., 2003. Robust anomaly detection using support vector machines. In: Proceedings of the International Conference on Machine Learning, pp. 282–289.

Le Khac, N.A., Kechadi, M.T, 2010. Application of data mining for anti-money laundering detection: a case study. In: Proceedings of the IEEE International Conference on Data Mining Workshops. IEEE, pp. 577–584.

León, C., Pérez, J., 2014. Assessing financial market infrastructures' systemic importance with authority and hub centrality. J. Financ. Mark. Infrastruct. 2 (3), 67–87.

León, C., 2020. Detecting anomalous payments networks: a dimensionality-reduction approach. Latin Am. J. Cent. Bank. 1 (1–4), 100001.

Lee, W., Stolfo, S.J., Mok, K.W., 2000. Adaptive intrusion detection: a data mining approach. Artif. Intell. Rev. 14 (6), 533–567.

Massarenti, M., Petriconi, S., Lindner, J., 2012. Intraday patterns and timing of TARGET2 interbank payments. J. Financ. Mark. Infrastruct. 1 (2), 3–24.

Rubio, J., Barucca, P., Gage, G., Arroyo, J., Morales-Resendiz, R., 2020. Classifying payment patterns with artificial neural networks: an autoencoder approach. Latin Am. J. Cent. Bank. 1 (1–4), 100013.

Sabetti, L., Heijmans, R., 2021. Shallow or deep? Training an autoencoder to detect anomalous flows in a retail payment system. Latin Am. J. Cent. Bank. 2 (2), 100031.

Siaterlis, C., Maglaris, B., 2004. Towards multisensor data fusion for DoS detection. In: Proceedings of the ACM symposium on Applied Computing, pp. 439–446.

Soramäki, K., Cook, S., 2013. SinkRank: an algorithm for identifying systemically important banks in payment systems. Econ. Open-Access Open-Assess. E J. 7 (2013–28), 1–27.

Sun, J., Xie, Y., Zhang, H., Faloutsos, C., 2007. Less is more: compact matrix decomposition for large sparse graphs. In: Proceedings of the SIAM International Conference on Data Mining, pp. 366–377 Society for Industrial and Applied Mathematics.

Thompson, B.B., Marks, R.J., Choi, J.J., El-Sharkawi, M.A., Huang, M.Y., Bunje, C., 2002. Implicit learning in autoencoder novelty assessment. In: Proceedings of the International Joint Conference on Neural Networks. IJCNN'02, 3. IEEE, pp. 2878–2883 (Cat. No. 02CH37290).

Thorndike, R.L., 1953. Who belongs in the family? Psychometrika 18 (4), 267–276.

Tibshirani, R., Walther, G., Hastie, T., 2001. Estimating the number of clusters in a data set via the gap statistic. J. R. Stat. Soc.: Series B (Stat. Methodol.) 63 (2), 411–423.

Triepels, R., Daniels, H., Heijmans, R., 2018. Detection and explanation of anomalies in real-time gross settlement systems by lossy data compression. In: Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017). Springer Verlag, pp. 145–161.

Yeung, D.Y., Chow, C., 2002. Parzen-window network intrusion detectors. In: Proceedings of the Object Recognition Supported By User Interaction For Service Robots, 4. IEEE, pp. 385–388.