Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services

Evgenia Novikova, Igor Kotenko

Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services

Evgenia Novikova[1] and Igor Kotenko[1,2]

[1] Laboratory of Computer Security Problems
St. Petersburg Institute for Informatics and Automation (SPIIRAS)
39, 14 Liniya, St. Petersburg, Russia
{novikova, ivkote}@comsec.spb.ru

[2] St. Petersburg National Research University of Information Technologies, Mechanics and Optics, 49, Kronverkskiy prospekt, Saint-Petersburg, Russia

Abstract. Mobile money transfer services (MMTS) are currently being deployed in many markets across the world and are widely used for domestic and international remittances. However, they can be used for money laundering and other illegal financial operations. The paper considers an interactive multi-view approach that allows describing metaphorically the behavior of MMTS subscribers according to their transaction activities. The suggested visual representation of the MMTS users' behavior based on the RadViz visualization technique helps to identify groups with similar behavior and outliers. We describe several case studies corresponding to the money laundering and behavioral fraud. They are used to assess the efficiency of the proposed approach as well as present and discuss the results of experiments.

Keywords: mobile money transfer services, fraud detection, visual analytics, RadViz visualization

1 Introduction

The field of Mobile Money Transfer service (MMTS) is a growing market segment, particularly in developing countries, where banking systems may not be as dense or available as in developed countries. For example, M-Pesa, which was launched in 2007 in Kenya, displayed in December 2011 about 19 million subscribers, namely 70% of all mobile subscribers in Kenya [29]. Orange Money is deployed in 10 countries and gathers around 14% of the mobile subscribers of these countries [23]. In such services, transactions are made with electronic money, called mMoney. The users can convert cash to mMoney through distributors and use it to purchase goods at merchants, pay bills or transfer it to other users [16].

The risks inherent to all payment systems are present in the mobile environment. However, the usage of mobile technologies introduces additional risks caused by the large number of non-bank participants, rapidity of transactions and higher level of anonymity compared to traditional banking systems [16, 18]. Therefore, it is required to determine new approaches to detect frauds in mobile money transfer services.

The aim of this paper is to show how visual analytics can provide better insight in the large data sets describing MMTS activity and can assist in fraud detection. Visual data exploration can be considered as a hypothesis generation and verification process which is intuitively clear and does not require explicit application of complex mathematical and statistical methods [11, 13, 21]. We suggest an interactive multi-view approach allowing the analyst to get a global overview of the MMTS subscribers' activity and then focus on users of the particular interest drilling down into their transactions. It is based on RadViz-based [3] visualization of the MMTS users that helps to determine similarity groups and outliers among them and is supported by graph-based and table views assisting in analyzing structural links of the user.

Specifically, our main contribution is the interactive RadViz-based visual representation of MMTS subscribers allowing detection of groups of users with similar behavior. To the best of our knowledge, our work is the first to exploit RadViz visualization technique to visualize MMTS subscribers. To demonstrate and evaluate the usefulness of the proposed approach we investigated several case studies corresponding to the money laundering and behavioral fraud, which take place when the mobile device is used to carry out illegitimate transactions without its owner's consent.

The rest of the paper is structured as follows: *Section 2* overviews mobile money transfer service and its structure, and discusses related work in the field of fraud detection techniques in mobile payments as well as visualization techniques used to detect financial frauds. *Section 3* describes the approach suggested, including visual models and interactions with them. *Section 4* presents the case studies used to demonstrate the proposed approach for financial fraud detection in mobile payments using visual analytics techniques, discusses the results and presents ideas about further developments of the approach. *Section 5* sums up our contributions.

2 Background

2.1 Mobile Money Transfer Service

The paper is based on the MMTS use case detailed in [1, 25]. This section outlines the major points to understand the use case. MMTS are systems where electronic money, called *mMoney* or *m*, is issued to different roles such as regular users, retailers, merchants, in order to perform various types of transactions which range from merchant payments to transfers between individuals.

Fig. 1, which is adapted from [10], shows the economic principle of mMoney and the roles of various actors. As depicted, the Mobile Network Operator (MNO) emits mMoney in partnership with a private bank. The MNO regularly produces compliancy reports, including suspicious activity reports, to the Central Bank, responsible for the country's monetary policy. The emitted mMoney can only be used among the MNO's clients subscribing to the MMT service. The subscribers are end-users, service providers or retailers. They hold a prepaid account stored on a platform and accessible via the MNO's network and an application on their mobile device. Some users, such as retailers or service providers, can use computers to access their account. This account contains mMoney which can be acquired from the retailers. End-users can either transfer money to other end-users or purchase goods.

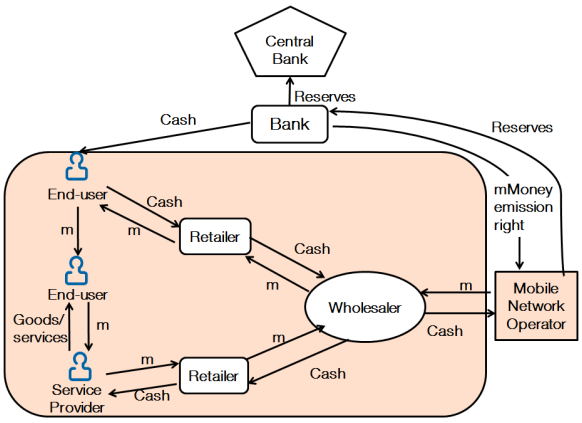


Fig. 1. Economic environment of Mobile Money Transfer services [10]

2.2 Fraud Detection Techniques in Mobile Payments

In the Kenyan MMT service M-Pesa, fraud detection is carried out by the Minotaur tool which uses neural networks [19, 22]. Apart from this system, there is not much publicly available information about fraud detection in MMT services. However, to our knowledge, the most widely deployed tools are based on rules, linear regression and neural networks.

If we consider other payment systems, several fraud detection techniques have been applied. For example, in the field of credit card fraud detection, Al-Khatib [2] identifies several studies which use neural networks, expert systems, case-based reasoning, genetic algorithms, inductive logic programming and regression. Another illustration is the use of graphs proposed by Ron and Shamir [26] to explore the data related to the transactions in the Bitcoin payment system in order to highlight awkward transactions schemes.

3 Related Work

Due to the complexity of financial data (often with multidimensional attributes), many sophisticated visualization and interaction techniques have been proposed (to analyze the financial market as a whole, or single assets in particular), which support visually decision making [15]. Parallel coordinates, scatter-plot matrices, survey plots, special glyphs [28], treemaps [31], stacked and iconic displays, dense pixel-displays [33], dendrograms, fish-eye views [14] are applied to explore financial data.

However, the visualization techniques applied in fraud detection systems are rather limited. The most of commercial software products [8, 20, 27] extensively use trends, pie charts and histograms and gauge-based glyphs to display characteristics of financial flows, number of registered alerts, their type and criticality, etc. The choice of these visual models is explained by their simplicity and ability to communicate the most important information at glance. They can be easily included in the reports of any level and purpose. Apart from the standard visual models, geographical maps are

often present in fraud detection systems as they allow detecting regions with high financial risk level as well as determining the limits of organization responsibility. Such kind of metrics is usually encoded by color or specific icon [8, 20].

In [8] the visual representation of statistically calculated behavior of a peer group and deviations from it is used as an advanced technique to reduce alert generation. The behavior of the group is displayed as a set of line charts in which *x*-axis corresponds to the time and *y*-axis – to the values of the most important characteristics of the transaction flow such as average transaction amount, number of transactions, etc. The vertical axis is divided into three zones determining deviation level in users' behavior. The normal (average) behavior lies in yellow zone, location of the charts in the red colored zone indicates that behavior deviates significantly from the average one and orange shows the presence of deviation. These deviation levels could be adjusted according to the average characteristics of the peer group thus decreasing alert triggering level.

In order to support alert investigation the most of the fraud detection systems implement flexible querying mechanism that allows the analyst to extract all data associated with a given key value, i.e. account or credit card number [8, 27]. However, identifying hidden relationships, based on data from multiple sources, and tracking the movement of money made between a variety of entities is difficult using tabular methods. For this reason the graph-based representation of users' financial contacts are applied in fraud detection systems [20, 27] and adopted by different forensic companies [6, 32]. Usually graph vertexes represent different entities such as accounts, user IDs, phones, credit cards, addresses, organizations, etc. The edges between them indicate the usage or participation of the corresponding entity in financial operations, and the line thickness displays the frequency of the transactions between entities. The graph-based representation of transaction activity helps to discover connections between customers, to identify suspicious communication patterns, revealing thus organized group of fraudsters.

Korczak et al. [12] address the problem of graphical representation of sequential financial operations in readable manner. Exploration of transaction chains assists the analyst to detect money laundering operations. However, the major concern when designing a visualization algorithm of sequential operations is the complexity of the resulting graph. In order to solve this problem the authors propose the evolutionary algorithm that minimizes the number of edge intersections.

Chang et al. [4] present the WireVis tool for the analysis of financial wire transactions for fraud protection. It is based on transaction keyword analysis and built in collaboration with the Bank of America. All the textual elements contained in transaction data records are seen as keywords. WireVis uses a multi-view approach including a keyword heatmap and a keyword network graph to visualize the relationships among accounts, time and keywords within wire transactions. The keyword heatmap characterizes the usage frequency of the keyword in the users' groups. Authors suggest an interesting modification of the clustering algorithm applied to form groups of similarities. They treat each account as a point in the *k*-dimensional space (where *k* is the number of keywords), and group the accounts based on their distances to the average point of all accounts. This approach significantly decreases the complexity of clustering procedure having complexity $O(3n)$. In order to support the visualization of transaction activity over time, authors propose the Strings and Beads view in which

the strings refer to the accounts or cluster of accounts over time, and the beads refer to specific transactions on a given day. The *x*-axis of the view corresponds to the progression of time, and the y-axis shows a transaction attribute selected form the predefined list.

4 Data, Models, and Techniques

4.1 Data

The data from existing MMTS are not publicly available and in the most cases confidential. A possible solution of this problem can be usage of artificially generated data. This approach is widely used to train automatic fraud detection techniques based on pattern recognition and machine learning [9]. In our work we use MMTS log synthetic simulator [9] to generate test data containing different fraudulent scenarios. The MMTS log synthetic simulator was developed within the FP7 project MASSIF to assess efficiency of the proposed intrusion detection techniques for the mobile money transfer scenario [25]. It models the mobile money transfer platform and the behavior of its legitimate or fraudulent users.

These data describe only transaction logs and contain such information as the phone number of the customer (sender/receiver), their account ID and role (customer, retailer, merchant, operator, etc.), transaction ID, its timestamp, type (money transfer between individuals, cash in or cash out of the mobile wallet, etc.), transaction amount, status as well as sender's and receiver's balance before and after transaction.

In order to assess the suggested approach we generated various case studies, including money laundering activities and mobile botnets, using this simulator. In generated scenarios each MMTS subscriber has only one account and role associated with him (her).

4.2 Visual Models and Interaction Techniques

When designing main form of the MMTViewer, a tool demonstrating the approach, we followed Shneiderman's information seeking mantra [30] that consists in having the overview first and then focusing on particular areas of interests.

Thus, the main window is divided into three subviews: (A) RadViz-based view, (B) graph-based view and (C) table view, designed to inspire the analyst to dive into data, generate hypotheses and verify them (Fig. 2).

The goal of the RadViz-based view (A) is to provide the general overview of the transaction activity in the MMTS. It allows identification of the existence of patterns in subscribers' behavior, while the graph-based view (B) helps to focus on the links of a particular user or a group of users. The table view (C) gives detailed information on the selected MMTS entity (subscriber or transaction). These three views are coordinated together, so selecting a user in view A results in highlighting corresponding user and his/her transactions in view B and refreshing detailed information in view C.

With these three tightly linked views the analyst can interact with users and transactions in order to understand how the data correlate. We suppose such approach is significantly more powerful that using the views separately.

The tool described in the paper is written in Java. All visual models are implemented using Prefuse Toolkit [24], which allows development of highly interactive visualizations. It can be easily integrated into Swing applications or Java applets.

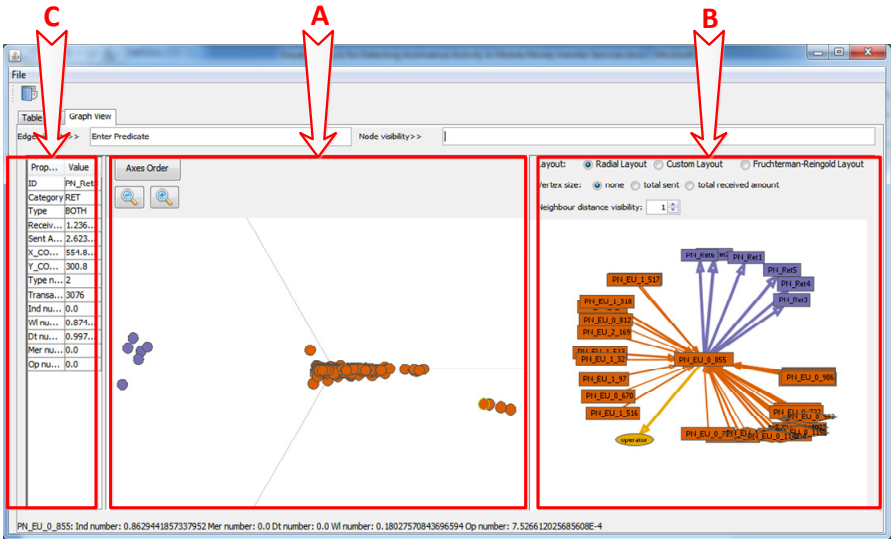


Fig. 2. The main window of MMTViewer

4.2.1. The RadViz-based View

The main view is a RadViz visualization [3] of the MMTS users. Its goal is to highlight groups of users with similar "transaction" behavior.

The Radviz is a non-linear multi-dimensional visualization technique that can map *n*-dimensional data into 2-dimensional space. The analyzed attributes are represented as dimension nodes placed around the perimeter of a circle. Then the objects are displayed as points inside the circle, with their positions determined by a metaphor from physics: each point is connected by *n* springs to the *n* respective dimension nodes. The stiffness of each spring is proportional to the value of the corresponding attribute. Thus, the point is located at the position where the spring forces are in equilibrium. Prior to visualization, all used attribute values are normalized. The objects set close to some dimension node have higher values for the corresponding attribute then for the others. For example, analyzing Fig. 3 it is possible to conclude that the merchant payments and individual transfers are prevailing among all other end user's financial operations, furthermore their quantity is comparable. The important feature of the Radviz technique is that it supports visualizing all dimensions of a dataset at once and is very useful when searching for clusters and outliers in multidimensional data. It can be effectively used as clustering tool that is characterized by low complexity O(*n*).

We suggest using the following attributes of the user as dimension anchors because these properties are commonly used in detecting anomalous activity both in financial systems and scientific research tools [2, 6, 8, 20] and can rather exactly describe the "transaction" behavior of the user:

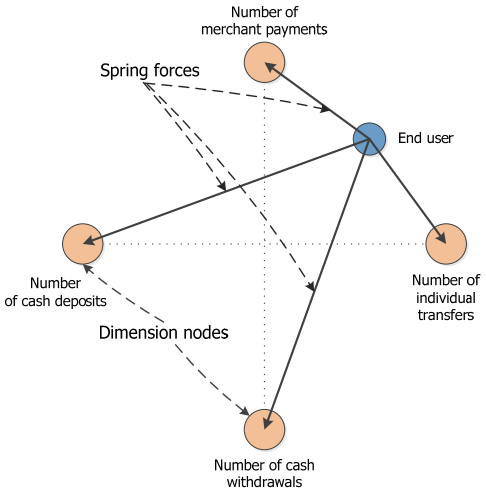


Fig. 3. Schema of the RadViz-based visualization of user transaction-based behavior

- a number of individual transfers for a given period of time;
- a number of cash deposit operations for a given period of time;
- a number of cash withdrawal operations for a given period of time;
- average amount of individual transfers for a given period of time;
- average amount of cash deposit operations for a given period of time;
- average amount of cash withdrawal operations for a given period of time;
- minimum and maximum amount of individual transfers for a given period of time;
- minimum and maximum amount of cash deposit operations for a given period of time;
- minimum and maximum amount of cash withdrawal operations for a given period of time.

As the major problem of the RadViz visualization is an appropriate selection of the dimension nodes' layout which determines the quality of the posterior visualization and ability to detect clusters [7], we use the arrangement of the anchors given in Table 1 as default. However, we implemented a mechanism that enables a user to adjust the layout of dimension nodes by selecting them from the predefined list and setting their order.

Table 1. Default order of dimension nodes in RadViz-based view

Order	Dimension node
0	a number of individual transfers for a given period of time
1	a number of deposit operations for a given period of time
2	a number of withdrawal operations for a given period of time

The MMTS subscribers are displayed as colored points inside the unit circle. The color is used to encode their role in the MMTS. We suppose that users having the same role should merge in clusters, showing thus similar behavior. For example, retailers who are mainly involved in operations of cashing in/out customers mobile

wallet should form a cluster. The location of end users is difficult to predict as they can show rather various behavior, nevertheless, we expect them also to be grouped in clusters. We consider that in this case the signs of potential fraud could be as follows:

- a user does not belong to any cluster or included in the group of the users having another role;
- location of a group of users significantly differs from the rest.

These anomalies in users' layout could be a starting point in the analysis of the transaction activity in the MMTS. The coloring of the nodes based on the users' role simplifies the process of anomaly detection immensely.

4.2.2. The Graph-based View

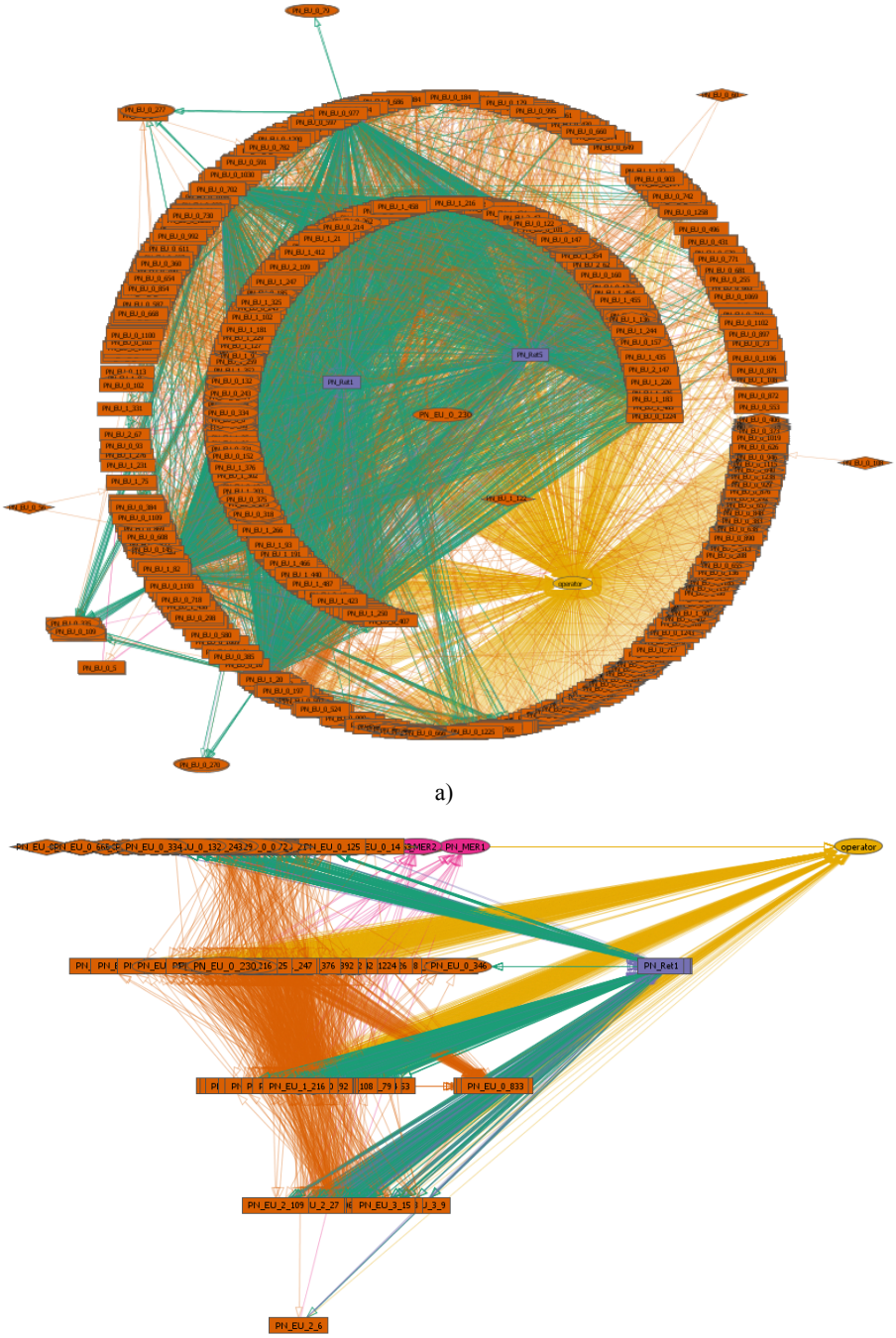
The graph-based visualization technique is a common way for presenting transactions in financial systems. The main advantage of the graph view is that it emphasizes structural properties of the connectivity between users.

In the tool the graph vertexes represent users, while edges – transactions between them. As mentioned above in our case studies, a user has only one mobile account associated with him, therefore we do not display mobile account as a separate vertex connected with the user. However, if the user has several accounts we suggest to aggregate them into one meta-node preserving all input and output links in order to improve readability of the generated image.

Color is used to encode the role of the user in the MMTS as well as the transaction type. Both color schemes were created using Color-Brewer2 [5]. The transaction types that are frequently used in detection of suspicious activity such as cash withdrawal, deposit and individual money transfers are encoded with color-blind safe colors. The shape of the vertex depends on whether the user is only transaction sender (diamond), receiver (ellipse) or both (rectangle). This feature can simplify the detection of subscribers whose accounts are used only for cash withdrawal or deposit operations. If the user is linked with another user by a set of transactions of the same type then they are displayed as one edge, whose thickness is determined by their quantity. The size of the graph vertex could be determined by a sum of received and sent amounts for a given period of time. We consider that this option helps to discover subscribers, who participate in large cash flows.

To support visual exploration of the data, we implemented the following interaction techniques. Flexible *filtering* mechanism allows specifying different complex logical expressions to filter data. *Linking and brushing* effect can be applied in order to highlight contacts of the MMTS user. When switched to this mode, it is possible to select the user by clicking on the corresponding node, this will make all input and output links visible while the rest will be hidden. The combination of this technique with filtering mechanism allows focusing on particular user transactions with given characteristics. Apart from *tooltip* that gives only brief information about the object, i.e. transaction type, its sender and receivers, etc., the user can get detailed information on every element of the graph (node or vertex) shown in table view by clicking on it. This information includes subscriber's id, role, number of transactions, total amount, minimum and maximum transaction amounts, transaction time, etc. This informational display is updated whenever a particular graph node or edge is selected.

We also implemented two graph layouts: radial and based on scatter plot (Fig. 4).



a)

b)

Fig. 4. Graph-based representation of the financial contacts of the MMTS user using radial layout (a) and scatter plot-based layout (b)

In order to construct the latter, we calculate for each subscriber the total quantity of all transactions made by him/her and the number of different transaction types used. These two attributes define the position of the corresponding node on the plane: *x*-coordinate is determined by the total quantity of all transactions, and *y*-coordinate is determined by number of different transaction types. This layout helps to reveal the most active users as the heightened activity can be a sign of potential fraud. However, it is clearly seen that these two graphical data presentation cannot be used to visualize a large set of data as generated image is overloaded with lines and labels which are in the most cases are simply unreadable. That is why we suggest using such presentation only when a particular set of users has been already selected. In this case the analyst can take all advantages of graph-based visualization for investigating users' links.

5 Case Studies and Discussion

5.1 Money Laundering Misuse Case

Several money laundering schemes exist. In this paper, the emphasis is made on the use of chains of mules. Using *mules* enables to hide the fraudulent origin of money. Chains of mules may be composed of several layers. Here, only one layer of several mules is considered. Fraudsters owning a certain amount of money to be laundered divide this amount and send it to several mules.

Later on, they withdraw this money from a complicit retailer. In reality, they would then send the cash obtained to another fraudster, but this money stream is not captured by the MMTS. The origin of the amount of money used by the first fraudster is not modeled here. The scenario is composed of 500 legitimate users, 10 mules and 4 retailers and 5317 transactions.

When assessing the efficiency of our tool we conducted almost "blind" experiment as we do not know number of malefactors, number of fraudulent transactions and their amounts, malefactors and mules themselves. We only know that this set of data may contain money laundering activity. The obtained results could be lately verified using special *ground proof* data field.

When detecting anomalous activity using our tool, we considered the following assumptions: (i) the amount of fraudulent transactions is smaller than the average amount of the users; (ii) the mules also perform legitimate transactions and (iii) a sudden change in transferred mMoney amounts corresponds to an anomaly.

Thus, we can expect that a fraudster is described by (i) greater number of individual money transfers and withdrawal operations and (ii) smaller average amount of these transactions.

These assumptions are made on base of analysis of existing money laundering scenarios described in [17, 18]. That is why we selected the following attributes as anchors: quantities of individual transfers, mMoney withdrawals and deposits, and their average amounts, respectively. The result of MMTS users' visualization using RadViz technique is shown in Fig. 5.

It is clearly seen that two subscribers are located apart from the others. This fact can be explained by that these users are mainly involved in the individual money transfers.

Additionally, from the graph-based view we see that one of them only sends money and another - only receives money. Further analysis of their contacts shows that these two subscribers (PN_FR1 and PN_FR2) are connected with each other via a set of users (Fig. 6). According to this, we can conclude that PN_FR1 and PN_FR2 could be potential fraudsters and the subscribers connected with them are the mules.

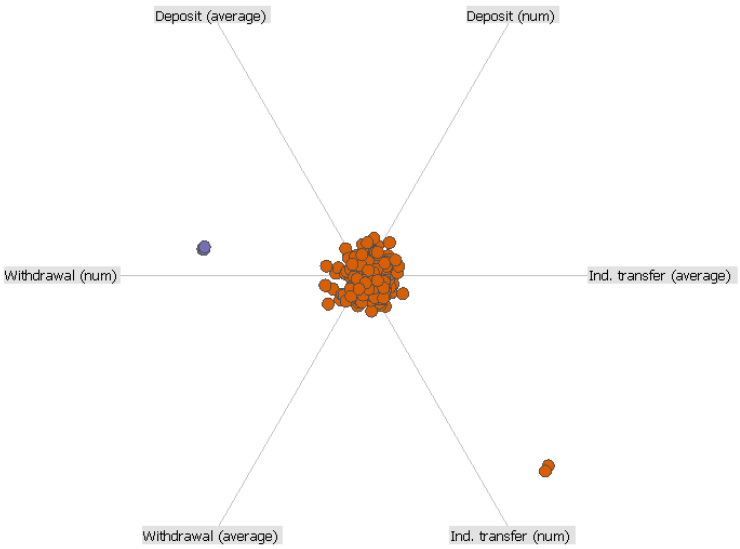


Fig. 5. RadViz visualization of MMTS users in money laundering scenario

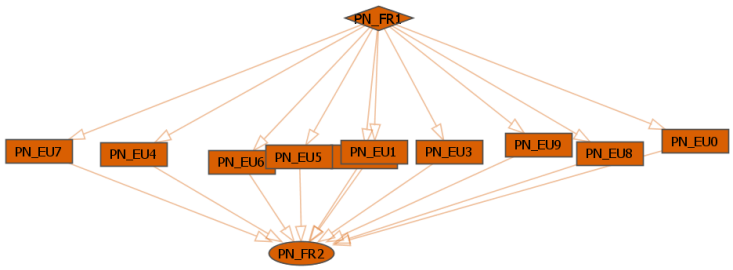


Fig. 6. RadViz visualization of MMTS users in money laundering scenario

5.2 Behavioral Fraud Case Study

Behavioral frauds occur when the behavior of the fraudster is superimposed on the legitimate user's one. Both actors use the mobile device to carry out transactions in the same window of time. In this paper, we consider two types of such fraud. The first one corresponds to a botnet which is deployed on several mobile devices. The malicious program carries out several transfers towards mules who withdraw the money within 72 hours after its reception. This scheme is rather similar to the money laun-

dering scheme except that the amounts involved are not the same, there is no complicit retailer, and the mules are used here to hide the destination of the stolen money and not its origin. Moreover, the fraudulent transactions are initiated by the malicious programs. The second case corresponds to a theft. The mobile device is stolen and the fraudster then tries to withdraw money several times during a short range of time before the phone's theft is reported and the phone is deactivated.

The generated scenario is made of 2 merchants, 6 retailers and 4010 users, 4 of which are mules, and 54222 transactions. There are 3 thieves and 39 infected mobile devices. As in previous use case we do not know the detailed information on simulated frauds: number of thieves, structure of the botnet and average amount of fraudulent transactions. When detecting the mobile botnet, we considered the following assumptions: (i) the amount of fraudulent transactions is slightly inferior than the average amount of the regular users transactions, (ii) the time elapsed between two fraudulent transactions is similar to the average interval between two legitimate transactions and (iii) the legitimate and fraudulent behavior occur during the same window of time. Like in the money laundering scenario, the infected subscribers as well as mules are characterized by increased transaction quantity. However, the amount of fraudulent transactions does not differ significantly from a normal one. That is why we use only attributes describing subscriber's transaction activity as anchors. The RadViz visualization of the MMTS users based on their transaction activity reveals four groups of users exposing similarities in behavior - *Retailers, Merchants, End users 1*, *End users 2* (Fig. 7).

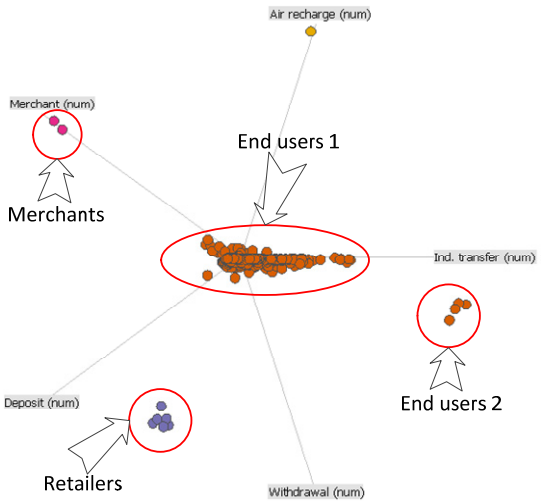
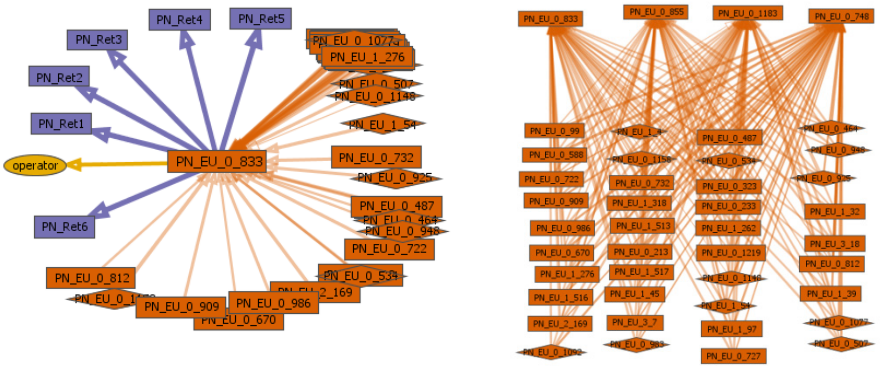


Fig. 7. RadViz visualization of MMTS users in the behavior fraud scenario

Groups *Retailers* and *Merchants* consist of retailers who are involved only in withdrawal and deposit operations, and merchants, respectively; group *End users 1*, the most numerous, consists of the subscribers who mostly uniformly make transactions of different types. Users belonging to the fourth group *End users 2* have individual money transfers significantly prevailing over transactions of other types. The link

analysis of the users shows that apart from individual transfers they make numerous withdrawal operations (Fig. 8a). These two facts allow us to conclude that these users are mules whose accounts are used to cash out mMoney from the mWallets. In order to detect a set of subscribers with infected mobile devices we filtered out all transactions that are not sent to the mules and this enabled us to detect the botnet. Its structure is presented in Fig. 8b.



(a) (b)

Fig. 8. Detection of mobile botnet: contacts of the mule (a) and botnet structure (b)

However, we failed to detect the theft of mobile devices. The detailed analysis of the raw data showed that the values of attributes selected as RadViz anchors of the compromised users are comparable to the ones of the subscribers using the MMTS comparatively rare during the selected period of time. And as the result their behavior is similar to the behavior of legal end users and they are in the group *End users 1*. Meanwhile it changes dramatically if observing his/her behavior in dynamics as legal activity fully stops.

5.3 Discussion

When choosing visualization technique for representation of the MMTS users and their transactions we aimed to produce a rather compact generalized view on users and their behavior, to divide them into relatively small groups uniting according to the similarities in their behavior and, thus, to decrease the amount of data to be investigated. We assumed that MMTS users could have similar behavior described in terms of average transaction amount, number of transactions and their types for a given period of time. Uniting them into groups allows focusing on these characteristics and determining subgroups or users in the group exposing anomalous behavior. Therefore, analysis of such groups could be a starting point in the investigation of the financial frauds of any type. The RadViz technique could be considered as a clustering tool that may be effectively used to solve this task. Its advantages such as low computational complexity ($O(n)$) and obvious representation of results of clustering procedure overweight its disadvantages which could be partly eliminated by providing a security officer a flexible mechanism for axis setup and layout.

Our experiments showed that the approach for analysis of the MMTS user behavior based on RadViz visualization used in conjunction with graph-based presentation of their transactions can be used effectively for money laundering scheme and botnet detection. These financial frauds are characterized by usage of mules, whose behavior usually significantly differs from ordinary users. Their accounts are used only as receivers of individual transfers and withdrawal operations, that means that corresponding points of the RadViz view lie apart from other users. These outliers can easily attract the attention of the analyst and cause additional investigation of their transactions. The analysis of the mules' transaction using graph-based visualization is able to reveal the botnet structure or the money-laundry scheme. Thus, we can assume that our approach can be effective in detection of financial frauds that have structural peculiarities involving usage of mules.

We failed to detect behavior frauds such as the theft of mobile devices using our approach. This failure is explained by the fact that we used statistical characteristics such as average transaction amount, number of transactions calculated for a given period of time to describe the user behavior. These statistical profiles of the users, whose mobile devices were stolen, were similar to rather large number of profiles of other users, making thus almost impossible to reveal them. In order to detect behavior frauds it is necessary to trace changes in users' behavior in time providing the analyst a possibility to compare selected attributes for different periods of time. Visualization techniques with time axes such as timelines or heat map with time axes enables historical analysis of data and could be used to monitor dynamics in users' behavior. However, the graphical representation of sufficiently large number of the MMTS users on one screen can cause certain difficulties in the analysis of their behavior due to illegible details of the generated image. Application of clustering techniques based on analysis of users' attributes and used to reduce data dimension can face the same difficulties as our approach. The possible solution of the problem within our approach is the usage of animated graphical data representation. Animation of user's location on RadViz visualization of the users and highlighting its trace if the changes in his/her behavior are significant can assist the analyst to spot a strange behavior.

6 Conclusions

The analysis of the state-of-art in fraud detection techniques in the mobile money transfer services showed that link analysis of subscribers' transactions using interactive graph-based data presentation is the most widely used visualization technique. It allows the analyst implementing link analysis of the user's contacts visually as well as applying graph-theoretic algorithms in order to discover structural peculiarities such as bridges and cliques. We proposed to form metaphoric presentation of the MMTS subscriber behavior according to his/her transaction activity. The user's activity is assessed using average amount of transactions, their quantity and usage of transactions of different type. This approach allows determining clusters of users exhibiting similar behavior and outliers. The latter is considered as a starting point of transaction analysis supported by traditional graph-based presentation of subscribers' transactions. However, the experiments implemented using the special synthetic simulator showed that our approach is able to detect fraud schemes that cause long term chang-

es in the average behavior of the MMTS subscribers or characterized by the specific behavior of the fraud scheme participants. In order to improve the efficiency of the proposed approach we defined future directions of the research concerning with exploration of the appropriate selection and arrangement of the dimension nodes in RadViz visualization and elaboration of the dynamic data presentation.

Acknowledgements. This research is being supported by grants of the Russian Foundation of Basic Research (projects 13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), the Program of fundamental research of the Department for Nanotechnologies and Informational Technologies of the Russian Academy of Sciences (2.2), by Government of the Russian Federation, Grant 074-U01, the State contract #14.BBB.21.0097, and the project ENGENSEC of the TEMPUS program.

References

1. Achemlal, M., et al.: Scenario requirements. Technical report. MASSIF FP7-257475 project (2011)
2. Al-Khatib, A.: Electronic Payment Fraud Detection Techniques. In: World of Computer Science and Information Technology Journal (WCSIT), Vol.2, pp.137-141 (2012)
3. Ankerst, M., Berchtold, S., Keim, D.A.: Similarity Clustering of Dimensions for an Enhanced Visualization of Multidimensional Data. In: 1998 IEEE Symposium on Information Visualization (INFOVIS '98). IEEE Computer Society, pp.52-60 (1998)
4. Chang, R., Ghoniem, M., Kosara, R., Ribarsky, W., Yang, J., Suma, E., Ziemkiewicz, C., Kern, D., Sudjianto, A.: WireVis: Visualization of Categorical, Time-Varying Data From Financial Transactions. In: IEEE Symposium on Visual Analytics Science and Technology (VAST 2007), pp.155-162 (2007)
5. ColorBrew2. http://colorbrewer2.org
6. Delloite. Visual Analytics: Revealing Corruption, Fraud, Waste, and Abuse. Presentation of the Forensic Center. http://www.slideshare.net/DeloitteForensicCenter/ visual-analytics-revealing-corruption-fraud-waste-and-abuse-13958016
7. Di Caro, L., Frias-Martinez, V., Frias-Martinez, E.: Analyzing the Role of Dimension Arrangement for Data Visualization in Radviz. In: Advances in Knowledge Discovery and Data Mining. LNCS. Vol. 6119, pp.125-132. Springer, Heidelberg (2010)
8. Fiserv. Financial Crime Risk Management solution, http://www.fiserv.com/risk-compliance/financial-crime-risk-management.htm
9. Gaber, C., Hemery, B., Achemlal, M., Pasquet, M., Urien, P.: Synthetic logs generator for fraud detection in mobile transfer services. In: Int. Conference on Collaboration Technologies and Systems (CTS 2013). pp.174-179 (2013)
10. Jack, W., Tavneet, S. Townsend, R.: Monetary Theory and Electronic Money: Reflections on the Kenyan Experience. In: Economic Quarterly, Vol.96-1, pp.83-122 (2010)
11. Keim, D., Andrienko, G., Fekete, J.-D., Goerg, C., Kohlhammer, J., Melancon, G.: Visual Analytics: Definition, Process, and Challenges. In: A. Kerren et al. (Eds.): Information Visualisation, LNCS 4950, pp.154-175. Springer-Verlag, Berlin Heidelberg (2008)
12. Korczak, J., Łuszczyk, W.: Visual Exploration of Cash Flow Chains. In: The Federated Conference on Computer Science and Information Systems, pp.41–46 (2011)
13. Kotenko, I., Novikova, E.: VisSecAnalyzer: a Visual Analytics Tool for Network Security Assessment. In: 3rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013). In conjunction with the 8th International Conference on Availability, Reliability and Security (ARES 2013). September 2-6, 2013, Re-

gensburg, Germany. Lecture Notes in Computer Science (LNCS), Vol.8128. pp. 345-360. Springer, Heidelberg (2013)
14. Lin, L., Cao, L., Zhang, C.: The fish-eye visualization of foreign currency exchange data streams. In: Asia-Pacific Symposium on Information Visualisation, pp.91-96 (2005)
15. Marghescu, D.: Multidimensional Data Visualization Techniques for Financial Performance Data: A Review, TUCS Technical Report No 810, University of Turku, Finland (2007)
16. Merrit, C.: Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments. Technical report. Retail Payments Risk Forum (2010)
17. [FinTRAC] Money Laundering and Terrorist Financing Trends in FINTRAC Cases Disclosed Between 2007 and 2011. FINTRAC Typologies and Trends Reports (2012)
18. [FATF] Money Laundering using New Payment Methods. FATF Report (2010)
19. Neural-technologies. MinotaurTM Fraud Detection Software - Finance Sector. http://www.neuralt.com/fraud_detection_software.html.
20. Nice Actimize Integrated Fraud Management. http://www.niceactimize.com/index.aspx ?page=solutionsfraud
21. Novikova, E., Kotenko, I.: Analytical Visualization Techniques for Security Information and Event Management. In: 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). Belfast, Northern Ireland, UK. pp.519-525. IEEE Computer Society (2013)
22. Okutyi, E.: Safaricom tightens security on M-Pesa with fraud management system. http://www.humanipo.com/news/1341/Safaricom-tightens-security-on-M-Pesa-with-Fraud-Management-system (2012)
23. Orange Money dépasse les 4 millions de clients et lance ses services en Jordanie et à Maurice. http://www.orange.com/fr/presse/communiques/communiques-2012/Orange-Money-depasse-les-4-millions-de-clients-et-lance-ses-services-en-Jordanie-et-a-l-Ile-Maurice (in French) (2012)
24. Prefuse Information Visualization toolkit. http://prefuse.org/
25. Rieke, R., Coppolino, L., Hutchison, A., Prieto, E., Gaber, C.: Security and Reliability Requirements for Advanced Security Event Management. In: Sixth International Conference "Mathematical Methods, Models, and Architectures for Computer Network Security" (MMM-ACNS-2012). LNCS. Vol. 7531, pp. 171-180. Springer, Heidelberg (2012)
26. Ron, D., Shamir, A.: Quantitative Analysis of the Full Bitcoin Transaction Graph. In: the 17 the Int. Conference on Financial Cryptography and Data Security. LNCS. Vol 7859, pp.6-24. Springer, Heidelberg (2013)
27. SAS Fraud detection solutions. http://www.sas.com/offices/europe/uk/industries/ banking/fraud-detection.html (viewed on the October 10th, 2013)
28. Schreck T., Tekusova T., and Kohlhammer J., and Fellner D.: Trajectory-based visual analysis of large financial time series data. In: ACMSIGKDD Explorations Newsletter, 9(2), pp.30-37 (2007)
29. Second quarter of the financial year 2012/2013. Quarterly sector statistics report. Communications Commission of Kenya (2012)
30. Shneiderman, B.: Dynamic queries for visual information seeking. In: The Craft of Information Visualization: Readings and Reflections, pp.14-21. Morgan Kaufman (2003)
31. Wattenberg, M.: Visualizing the stock market. In: CHI Extended Abstracts on Human Factors in Computing Systems, pp.188-189 (1999)
32. Westphal, C.R.: Patterns for Financial Intelligence Units (FIUs) and Anti-Money Laundering (AML) Operations. http://support.visualanalytics.com/technicalArticles/ whitePaper/pdf/VAI%20AML%20FIU%20Patterns%20Presentation.pdf
33. Ziegler, H., Jenny, M., Gruse, T., Keim, D.A.: Visual Market Sector Analysis for Financial Time Series Data. In: IEEE Symposium on Visual Analytics Science and Technology (VAST), 25-26 October 2010. pp.83-90 (2010)