Interactive Multi-View Visualization for Fraud Detection in Mobile Money Transfer Services

Evgenia Novikova, Saint Petersburg Institute for Informatics and Automation (SPIIRAS), Saint Petersburg, Russia

Igor Kotenko, Saint Petersburg Institute for Informatics and Automation (SPIIRAS), Saint Petersburg, Russia

Evgenii Fedotov, Saint Petersburg Electrotechnical University (LETI), Saint Petersburg, Russia

ABSTRACT

Mobile money transfer services (MMTS) have gained a solid market segment and are widely used for domestic and international money transfers. Like traditional financial systems they can be used to conduct illegal financial activity including money laundering or usage of malicious software to gain access to mobile money. The paper considers an interactive multi-view approach for detection of the fraudulent activity in the MMTS. It considers a set of visualization techniques enabling comprehensive analysis of the behavior of the MMTS subscriber according to his/her transaction activity. The authors suggest a metaphoric visualization of the MMTS users' behavior based on RadViz visualization that is able to identify groups with similar behavior and outliers. They demonstrate how the proposed approach can be used to reveal money laundering scenarios, behavior frauds, present and discuss the results of the efficiency evaluation of the visualization techniques used to detect fraudulent activity.

Keywords *Emerging Security Threats, Fraud Detection, Mobile Money Transfer Services, RadViz Visualization, Visual Analytics, Visual Defense Technologies*

INTRODUCTION

Starting in 2000, with the introduction of Smart Money in the Philippines, the world's first electronic cash card linked to a mobile phone account— mobile money transfer services (MMTS) — have gained a solid market segment especially in the developing countries. For example, M-Pesa, which was launched firstly in Kenya in 2007, displayed in December 2011 about 19 million subscribers, namely 70% of all mobile subscribers in Kenya (StatReport, 2012) and is

DOI: 10.4018/IJMCMC.2014100105

used now in Tanzania, Afghanistan, South Africa, India and Romania (M-Pesa, 2015). Orange Money, another mobile money transfer service, is deployed in 10 countries and gathers around 14% of the mobile subscribers of these countries (Orange Money, 2012). The MMTS allows users to deposit money into an account stored on their cell phones and called mWallet, to transfer mobile money to other users, including sellers of goods and services, and to withdraw deposits for regular money. Users are charged a small fee for sending and withdrawing money using the service. In such services, transactions are made with electronic money, called mMoney (Merrit, 2010).

The risks inherent to all payment systems present in the mobile environment (FATF, 2010). However, as mobile money transfer services are operated by mobile network operators which are not classed as deposit-taking institutions, and, therefore, rely on usage of mobile technologies, additional risks caused by the large number of non-bank participants, rapidity of transactions are introduced (Merrit, 2010). Besides, the MMTS provide higher level of anonymity compared to traditional banking systems. Therefore, it is required to determine new approaches to detect frauds in mobile money transfer services.

In this paper the authors present *a novel interactive multi-view visualization approach* that provides a better insight in the large data sets describing MMTS activity and can assist in anomaly detection. It allows an analyst to get a global overview of the MMTS subscribers' activity and then focus on users of the particular interest by drilling down into their transactions. It is based on a RadViz visualization (Ankerst et al., 1998) of the MMTS users that helps to determine groups of similarities and outliers among them and is supported by graph-based and table views assisting in analyzing structural links of users. An analyst has a possibility to monitor changes in transaction activity using a heat map visualization of the transaction attributes. The heat map presentation of the user transaction activity is used to form his temporal profile which could be helpful when analyzing suspicious bursts of activity or changes in transactions amounts.

The main contribution of the authors is the *interactive visual representation of the MMTS subscribers allowing detection of groups of users with similar behavior*. To the best of researchers' knowledge, this work is the first to exploit the RadViz visualization technique to visualize MMTS subscribers. This paper is extended version of the paper presented on CD-ARES 2014 (Novikova & Kotenko, 2014). It contains detailed description of the developed visualization technique, extended by the heat map visualization of the MMTS user activity, proposed usage scenarios and comprehensive usability evaluation which includes expert assessment of the effectiveness of the proposed visualization technique for money laundering schemes and behavior fraud detection.

The rest of the paper is structured as follows. *Section 2* presents overview on mobile money transfer service and its structure, 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* outlines the case studies used to demonstrate the proposed approach for financial fraud detection in mobile payments. *Section 5* presents and discusses results of the efficiency evaluation of the proposed of visualization technique. *Section 6* sums up the authors' contributions.

SUBJECT AREA AND RELATED WORK

Mobile Money Transfer Services, also referred as mobile payment, mobile money, and mobile wallet, generally denote to money transfer and microfinancing services operated under financial regulation and performed from or via a mobile device (Merrit, 2010). In the developing countries,

mobile payment solutions have been deployed as means of extending financial services to the community lacking easy access to traditional banking institutions.

This paper is based on the MMTS use case detailed in (Achemlal et al., 2011; Jack et al., 2010). This section outlines the major points to understand the use case. The MMTS are managed by a mobile network operator (MNO). MNO not only provides infrastructure to financial services but emits mobile money, known as *mMoney*, in partnership with a financial institution. The *mMoney* can only be used by subscribers of the MMT service. The service enables its users to deposit and withdraw money, transfer money to other users and non-users, pay bills, purchase airtime and, transfer money between service subscribers. Subscribers can have different roles, i.e. retailers, merchants, end users. They hold a prepaid account known as *mWallet* and 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.

The most widely deployed tools used to detect financial frauds are based on rules, linear regression and neural network. For example, in the Kenyan MMT service M-Pesa (M-Pesa, 2015), fraud detection is carried out by the Minotaur tool which uses neural networks (Neural-technologies, 2015; Okutyi, 2012).

Rieke et al. (2013) suggested an approach for financial fraud detection in MMTS based on checking conformance of the current process to a model one using event data. It constructs a process model and maps event data describing transactions on it in order to identify deviations of current user behavior from the expected one. To the best knowledge of the authors there are no other publicly available papers presenting fraud detection techniques in the mobile payment use case described above.

In other payment systems, several fraud detection techniques have been applied. For example, in the field of credit card fraud detection, neural networks, expert systems, case-based reasoning, genetic algorithms, inductive logic programming, regression, Bayesian networks, decision trees and Hidden Markov Models are used (Al-Khatib, 2012; Delamaire et al., 2009; Bhattacharyya et al., 2011; Coppolino et al., 2015).

Ron and Shamir (2013) suggested a graph-based approach to explore the data related to the transactions in the Bitcoin payment system in order to highlight awkward transactions schemes.

Application of automated analysis techniques for fraud detection assumes that data is clearly structured, complete and correct and does not change over time, and the problem is well defined (Keim et al., 2008). The real life data rarely meets these preconditions. Visual analytics techniques help to cope with enormous volumes of heterogeneous and noisy data. They 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 (Keim et al., 2008; Kotenko & Novikova, 2013; Novikova & Kotenko, 2013).

Due to the complexity of financial data (often with multidimensional attributes), many sophisticated visualization and interaction techniques have been proposed, which support visually decision making (Marghescu, 2007-1). Parallel coordinates, scatter-plot matrices, survey plots, special glyphs (Schreck et al., 2007), treemaps (Wattenberg, 1999), stacked and iconic displays, dense pixel-displays (Ziegler et al., 2010), dendrograms, fish-eye views (Lin et al., 2005) are applied to explore financial data. In the most cases they support such financial tasks as analysis of the financial market as a whole, or single assets in particular, estimation of financial performance of the companies, assessment of long time investments (Marghescu, 2007-2; Ziegler et al., 2010).

However, the visualization means applied for fraud detection are rather limited. The most of commercial software (Fiserv, 2015; Nice Actimize, 2015; SAS, 2015) extensively uses 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 (Fiserv, 2015; Nice Actimize, 2015).

In (Fiserv, 2015) visual presentation of statistically calculated behavior of a peer group and deviations from it is used as 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 an analyst to extract all data associated with the given key value, i.e. account or credit card number (Fiserv, 2015; SAS, 2015). However, identifying hidden relationships, based on data from multiple sources, and tracking the movement of money made between a varieties of entities is difficult using tabular methods. For this reason the graph-based representation of users' financial contacts is applied in fraud detection systems (Nice Actimize, 2015; SAS, 2015) and adopted by different forensic companies (Delloite, 2015; Westphal, 2012). 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 & Łuszczyk (2011) address the problem of graphical representation of sequential financial operations in readable manner. Exploration of transaction chains assists 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.

The similar problem is solved in (Xie et al., 2014). Xie et al. (2014) developed VAET − a visual analytics system for analyzing electronic transactions and discovering temporal trends. A probabilistic decision tree learner is used to estimate a specific saliency value for each transaction which describes relevance of the transaction for a certain analysis task, for example, detection of the suspicious transactions. The variation of this measure over time calculated for a specific group of transactions is displayed using pixel-oriented display. The detailed information on a selected sequence of transactions is outlined using new visual metaphor called KnotLines inspired by music notation. In this view, lines reveal the connections among transactions while knots encode the detailed information of the associated transactions the pixel-based display and KnotLines are coordinated together that enables quick identifying of interesting transactions from a large dataset.

Chang et al. (2007) 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 heat map 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 group of users. Authors suggest an interesting modification of the clustering algorithm applied to form groups of similarities. They treat each account as a point in 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 the 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.

To the authors' knowledge, there are no public works concerning the study and the adaptation of visual analytics fraud detection methods to mobile payment systems use case. Therefore, we cannot easily compare our work to existing systems.

VISUAL ANALYTICS MODELS AND TECHNIQUES

MMTS Data

Data from existing MMTS is not publicly available and in the most cases confidential. The possible solution of the lack of real world MMTS data necessary for developing and evaluating visual analytics models and techniques is the usage of artificially generated data. This approach is widely used to train automatic fraud detection techniques based on pattern recognition and machine learning (Gaber et al., 2013).

In this work the MMTS log synthetic simulator (Gaber et al., 2013) is used. It models the mobile money transfer platform and the behavior of its legitimate or fraudulent users. The MMTS log synthetic simulator was developed within European FP7 project MASSIF and can be used to generate test data containing different fraudulent scenarios. The simulated transactions are based on the properties of the real world transaction events (Gaber et al., 2013). They also contain *ground proof* field which could be used to validate the results obtained during analysis process.

The generated logs are transactions logs, although different kinds of logs (MMTS user registration, signing in/out, access, transfer, etc.) exist in the MMTS system. They 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.

To demonstrate suggested approach in use we examined various case studies, generated using this simulator. In generated scenarios each MMTS subscriber has only one account and role associated with him (her).

Models and Techniques

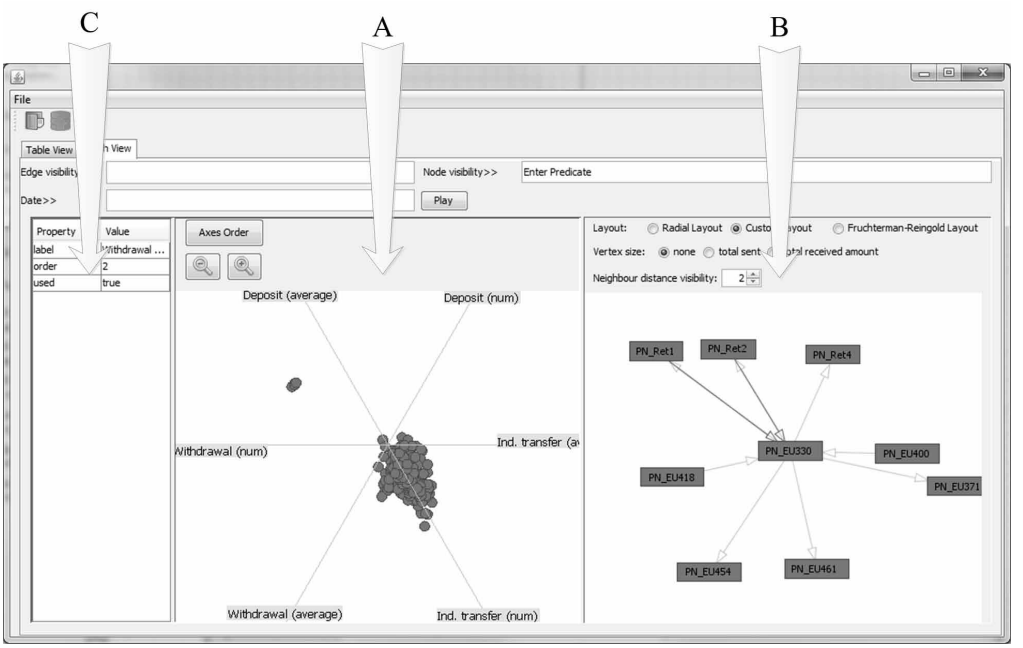
When designing MMTViewer, a tool demonstrating the approach, the authors followed Shneiderman's information seeking mantra (Shneiderman, 2003) that consists in having the overview first and then focusing on particular areas of interests. Thus, an analyst is provided several views, implementing different visualization techniques and designed to inspire him/her to dive into data, generate hypothesis and verify them.

The goal of the first set of views, displayed on one screen, is to support analysis of the MMTS users' behavior, according on how they use MMTS (Figure 1). It consists of

A. RadViz-based view;
B. Graph-based view;
C. Table view.

The goal of the RadViz-based view (A) is to provide the general overview of the transaction activity in the MMTS during selected period of time. 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.

Figure 1. The first group of interconnected views implementing RadViz visualization of the MMTS users (A), graph-based representation of MMTS user contacts (B) and table view of the details (C)



The second set of views, implementing heat map based visualizations of transaction parameters, could be used to trace changes in transaction activity of the MMTS users and form their temporal profile (Figure 2).

Similarly to RadViz-based view, heat map based view D also provides a general overview of the activity in the MMTS during a given period of time, however, it displays only one parameter describing transactions of the MMTS users. View E provides a magnified view of the selected area of the view D. View F displays temporal profile of the MMTS user selected in the view E.

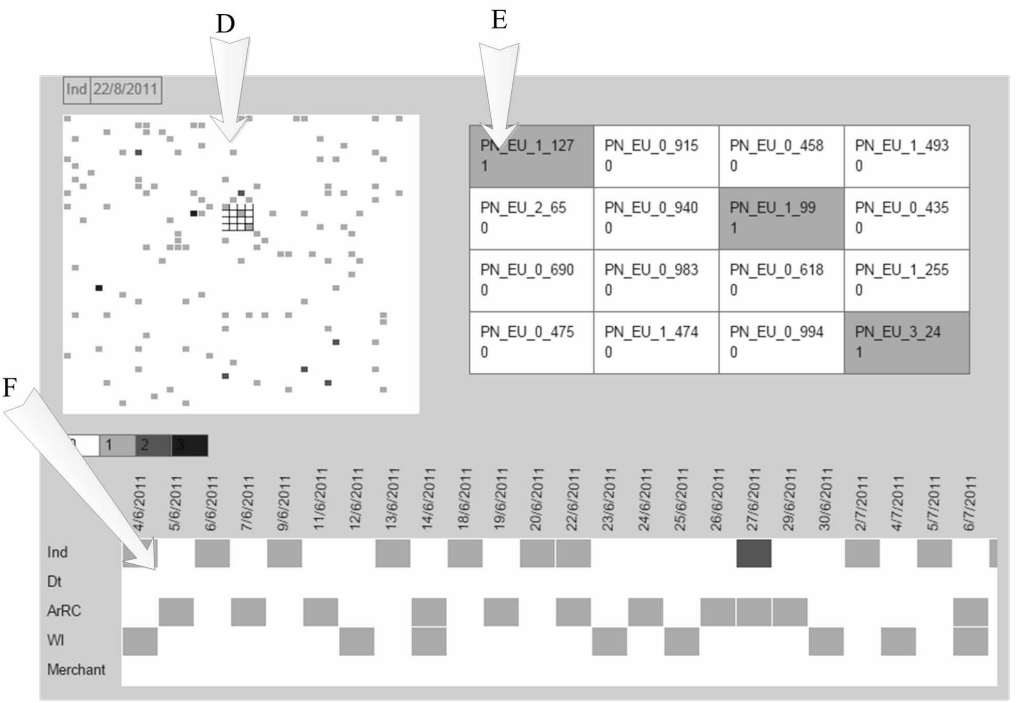
With these tightly linked views the analyst can interact with users and transactions in order to understand how the data correlates. The authors suppose such approach is significantly more powerful that using the views separately. The tool described in the paper is written in Java. All visual models are implemented using Prefuse Toolkit (Prefuse, 2015), which allows development of highly interactive visualizations. It can be easily integrated into Swing applications or Java applets.

The RadViz-based View

The central view of the first group of views is a RadViz visualization (Ankerst et al., 1998) of the MMTS users. Its goal is to highlight groups of users with similar "transaction" behavior and disclose outliers.

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

Figure 2. The second group of interconnected heat map based views displaying transaction activity of all MMTS subscribers (D), a set of the selected MMTS users (E) and temporal profile of the MMTS user (F)



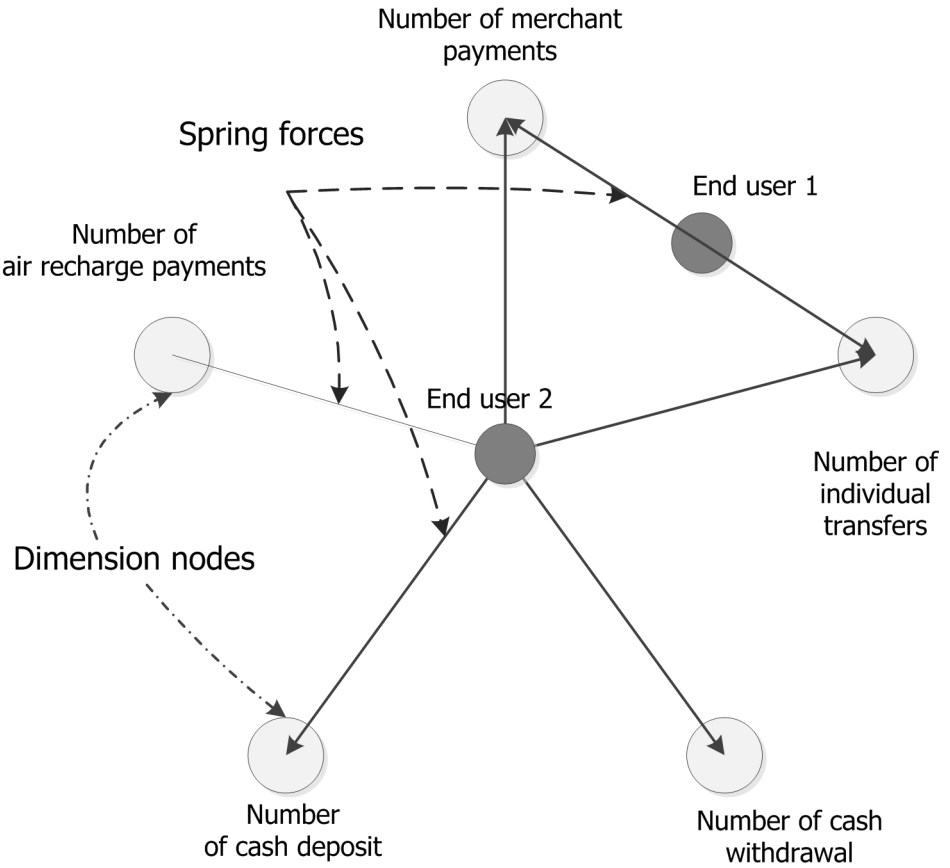
nodes placed around the perimeter of a circle. Then the objects are displayed as points inside the circle, with their positions determined by a metaphor from physics: each point is connected by *n* springs to the *n* respective dimension nodes.

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 having higher value for some attribute then for the others are set closer to the corresponding dimension node. If all *n* coordinates have the same value (regardless of whether they are low or high), the data point lies exactly in the centre of the circle. If object has attributes with similar values whose dimension nodes are opposite each other on the circle the corresponding data point lies near the center.

For example, analyzing Figure 3, it is possible to conclude that *end user 1* uses MMTS to make merchant payments and individual transfers only; furthermore, the frequencies of these transactions are comparable; while *end user 2* makes use of all available types of financial services with equal frequency.

The important feature of the RadViz technique is that it supports visualization of 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 characterized by low complexity O(*n*).

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



The following attributes of the user are suggested to use as dimension anchors because these properties are commonly used in detecting anomalous activity both in financial systems and scientific research tools (Al-Khatib, 2012; Delloite, 2015; Fiserv, 2015; Nice Actimize, 2015) and can rather exactly describe the "transaction" behavior of the user:

- 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;
- Mean amount of individual transfers for a given period of time;
- Mean amount of cash deposit operations for a given period of time;
- Mean 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.

The MMTS subscribers are displayed as colored points inside the unit circle. The color is used to encode their role in the MMTS. The authors assume that users having the same role should merge in clusters, exhibiting 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, they also expected to form clusters. In this case the signs of potential fraud could be as follows: a user does not belong to any cluster or is 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.

There are two major problems of the RadViz visualization.

The *first one* is an appropriate selection of the dimension nodes' layout which determines the quality of the posterior visualization and ability to detect clusters.

For n variables there are $(n - 1)! / 2$ possible RadViz projections (Di Caro et al., 2010). This means that selecting three transactions attributes only as dimension nodes, it is possible to produce one non-trivial RadViz projection.

Table 1 shows a default dimension anchor layout implemented in the MMTViewer tool. However, we provide an analyst a possibility to adjust the layout of dimension nodes by selecting them from the predefined list and setting their order.

The *second problem* of RadViz visualization consists in that many users can be mapped to the same position because they have comparable values for the selected attributes. This RadViz property could hide bursts of anomalous activity in transactions of a certain type.

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

Let us consider the following example. The *user 1* actively uses MMTS to make individual transfers, that's why he/she regularly cashes in his/her mobile wallet, while withdrawal operations are not typical for this user. Let us assume that the *user 1* usually makes four individual transfers, four deposit transactions and null withdrawal transactions during a given time unit. Then system registers four withdrawal operations made using mobile account of the *user 1* during the same time unit. This sudden burst of withdrawal activity could remain unspotted by the analyst when exploring transaction activity using RadViz visualization only as the *user 1* will be mapped at the same position with users who make individual transfers, cash in/cash out operations with equal frequencies, i.e. one individual transfer, one cash in and one cash out operations per a selected time unit.

To solve this problem, it is suggested using heat map based visualization of the MMTS users that allows quantitative analysis of the selected parameters.

The Heat Map-based View

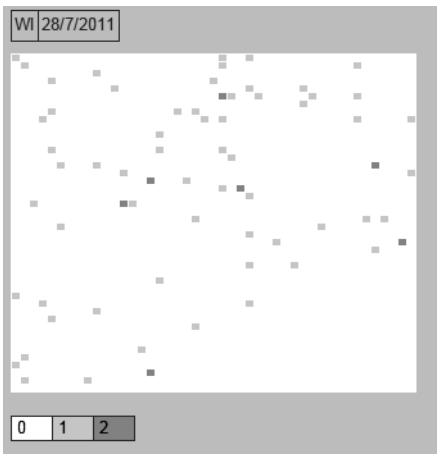
The key element of the second group of transactions log visualizations is a heat map. The heat map is a graphical representation of data where the individual values contained in a matrix are represented as colors. This visualization technique is widely used when visualizing big data sets. It used to monitor large IP spaces (Kintzel et al., 2011), port activity (McPherson et al., 2004), to represent spatial distributed file system activity patterns (Chukwa project, 2015).

In the tool the heat map view is used to display activity of the MMTS subscribers during selected time unit. Each heat map element represents a MMTS user, and the color of the point is determined by the numeric value of the parameter describing MMTS user activity (Figure 4).

The set of parameters available to analyst matches the set of parameters used as dimension nodes in RadViz visualization. They are the number of individual transfers, withdrawals, deposits, and merchant payments, amounts of these operations. An analyst has an option to choose what parameter to display. The darker color of the matrix element – the higher the value of the corresponding parameter.

Figure 4 shows the number of the withdrawal operations made in the MMTS during one day. It is clearly seen that only few users made more than four withdrawal transactions during that day, while the rest users made one or two withdrawal operations or did not withdraw electronic

Figure 4. Heat map representation of the withdrawal activity during one day



money at all. However, very often a security analyst is not interested much in what occurred during particular time unit but rather what changed across a range of time units. Therefore, the analyst may select any set of time units and see not a depiction of the actual values for each subscriber but a variance of the selected parameters. Suppose, for instance, the analyst selects a week, during which the user made 4 individual transfers of electronic money (78549, 11482, 72302 and 70084), then the system calculates the variance of this set of values and displays it. The significant amount of variance may be a sign of mobile bot activity as the infected mobile devices periodically send small sums of electronic money. We use color saturation to highlight the amount of the variance. White color means no variance, meaning that the corresponding users had the same level of the activity in all selected time units. Light grey users have a very small level of variance, grey users have a larger amount of variance, and dark grey users have the most variance.

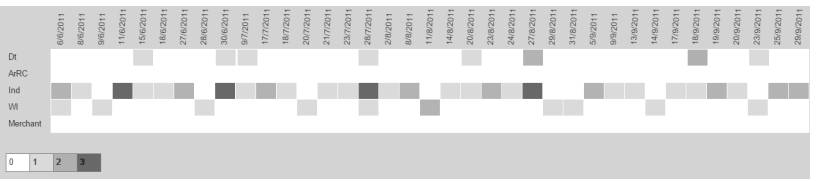
The heat map visualization of the sufficiently large number of the MMTS users on one screen poses certain difficulties in the analysis of their behavior due to minute and thus illegible details of the generated image. To solve this problem, a special zooming mechanism called *magnification area selector* is introduced. The analyst could select an arbitrary set of heat map elements and display them in a separate view (view E, Figure 2). This view is also a heat map visualization of the selected MMTS users which provides account ID and value of the parameter being examined. Each element of this heat map is selectable. Mouse clicking on it results in displaying historical data about activity of the selected user. This data includes information about all types of transactions available to the MMTS subscriber and is presented using heat map which with time axis (Figure 5). Depending on what analyst was examining in the previous views – amount of transaction, number of transaction or variance of the selected parameter, the heat map element represents the corresponding data for the other types of transactions. We suppose that heat map with time axis helps to form temporal profile of the MMTS subscriber activity as it reflects how they use their account. Adjusting the time unit of the time axis it is possible to construct a temporal profile of the user for a year, month or week. We also implemented *user ID search* mechanism that allows an analyst to specify user ID and find him on the main heat map visualization in order to analyze his temporal profile.

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 (Novikova & Kotenko, 2014).

In the tool the graph vertexes represent users, while edges − transactions between them. As mentioned above in our case study, 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,

Figure 5. Temporal profile of the MMTS subscriber represented using heat map



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 role of the user in the MMTS as well as transaction types. Both color schemes were created using Color-Brewer2 (2015). 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. This option helps to discover subscribers, who participate in large cash flows.

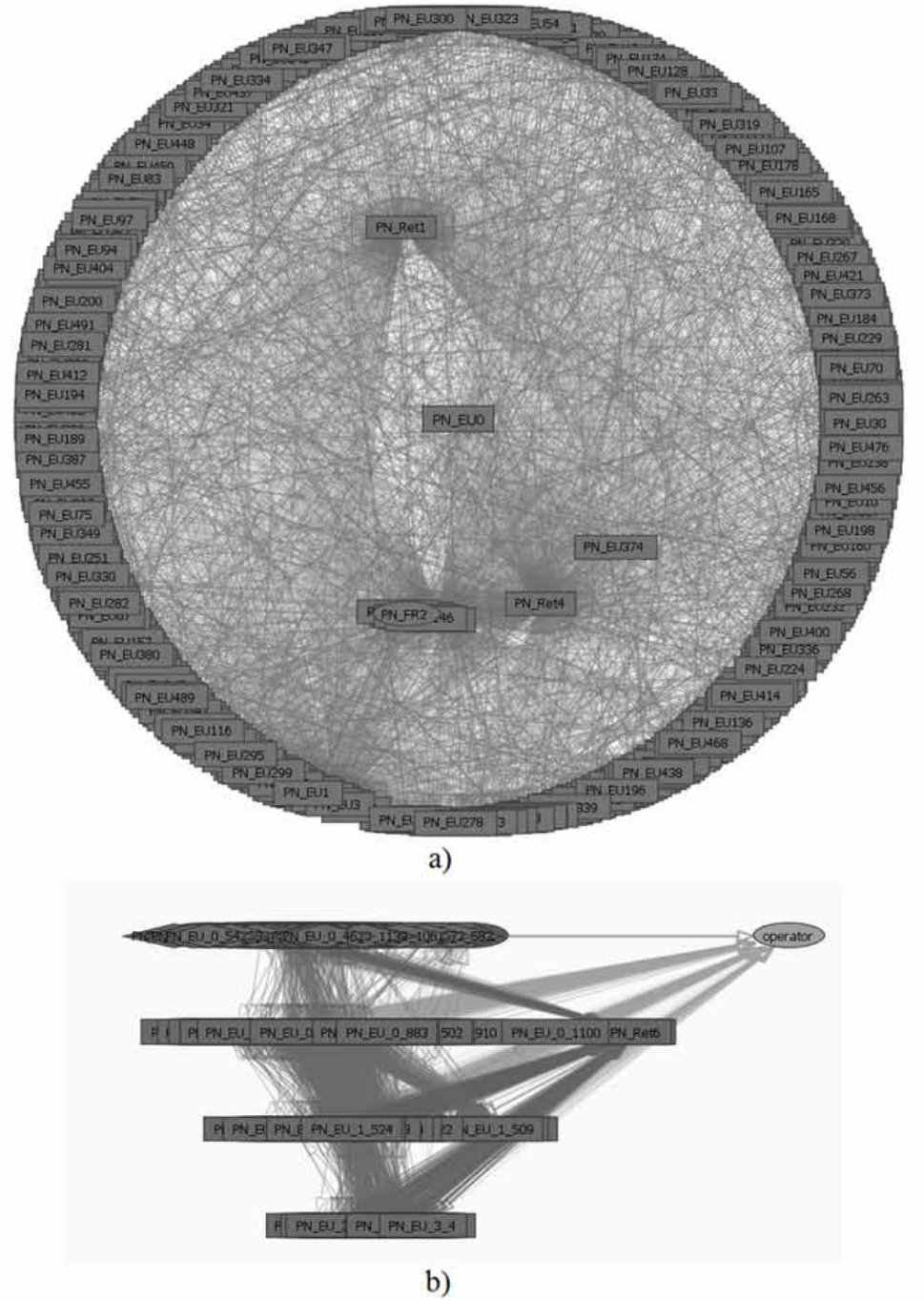
To support visual exploration of the data, the following interaction techniques are implemented. Flexible *filtering* mechanism allows specifying different complex logical expressions to filter data. *Linking and brushing* effect can be applied in order to highlight contacts of the MMTS user. When switched 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, amount of the transaction, etc., the user can get detailed information on every element of 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 custom one, based on scatter plot (Figure 6).

In order to construct the latter, the total number of all transactions made by him/her and the number of different transaction types used are calculated for each subscriber. 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. The heightened activity can be also a sign of potential fraud.

USAGE SCENARIOS

Designing the visualizations the authors kept in the mind the following analysis scenario. The security analyst might want to explore the activity in the MMTS over given period of time to discover that a set of users exposed a lot of activity during particular hour/day/week. They may then focus on the selected users and study their activity in the context of their normal activity and in case of necessity carry out further link analysis and detailed investigation of the transactions of the given MMTS subscriber. Therefore, the following usage scenario for the proposed visualization techniques to analyze MMTS transaction logs could be suggested. The starting point of the analysis could be the RadViz visualization as it gives overall view of the MMTS subscribers' activity during a given time unit. If the analyst is able to spot suspicious outliers he may then focus on the contacts of the suspicious users using graph based representation of the transactions and evaluate their temporal profile to prove his/her hypothesis. If it is impossible to determine any suspicious users using RadViz visualization, the analysis could be started with exploring different transaction parameters applying heat map visualization in order to detect

Figure 6. Graph-based representation of the financial contacts of the MMTS user using radial layout (a) and scatter plot-based layout (b)



sudden bursts or drops of transaction activity. The detected anomalies then can be evaluated in the context of temporal profile of the user and validate hypothesis using link analysis.

The authors tested our tool on a set of benchmark datasets containing different fraudulent activity. These datasets were generated using synthetic MMTS log simulator mentioned above. The investigated malicious scenarios are the following: money laundering scheme, theft of mobile phone and mobile botnet infection.

Money Laundering Misuse Case

Several money laundering schemes exist (FATF, 2010). The money laundering scenario generated assumes the use of chains of mules. Using mules allows hiding the fraudulent origin of money. Fraudsters having 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. Chains of mules may be composed of several layers. In the scenario analyzed only one layer of several mules is used. However, this limitation does not restrict the proposed approach to fraud detection as far as the authors are focusing on determining anomalous activity in MMTS but not on determining particular malicious scheme.

The scenario is composed of 500 legitimate users, 10 mules and 4 retailers and 5317 transactions.

When detecting anomalous activity using our tool, we made 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, a fraudster could be described by

I. Greater number of individual money transfers and withdrawal operations and
II. Smaller average amount of these transactions.

Basing on these assumptions the following attributes were selected as anchors: number of individual transfers, mMoney withdrawals and deposits.

The result of MMTS users' visualization using RadViz technique is shown in Figure 7. It is seen that there is a group of retailers who lie separately from other MMTS subscribers because they are involved only in withdrawal and deposit operations. It is possible to spot two end users who lie apart from the rest end users. They are marked in Figure 7 by *End users 1* label. Their location is explained by prevailing of the individual money transfers over other mobile money services. Additionally, from the graph-based view it is seen that one of these users only sends money, while another - only receives them. 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 (Figure 8).

According to this, one can conclude that PN_FR1 and PN_FR2 could be potential fraudsters and the subscribers connected with them are the mules.

Behavioral Fraud Case Study

Behavioral frauds occur when the behavior of the fraudster is superimposed on the legitimate user's one. This could happen when the mobile account is taken over after mobile phone is stolen

Figure 7. RadViz visualization of MMTS users in money laundering scenario

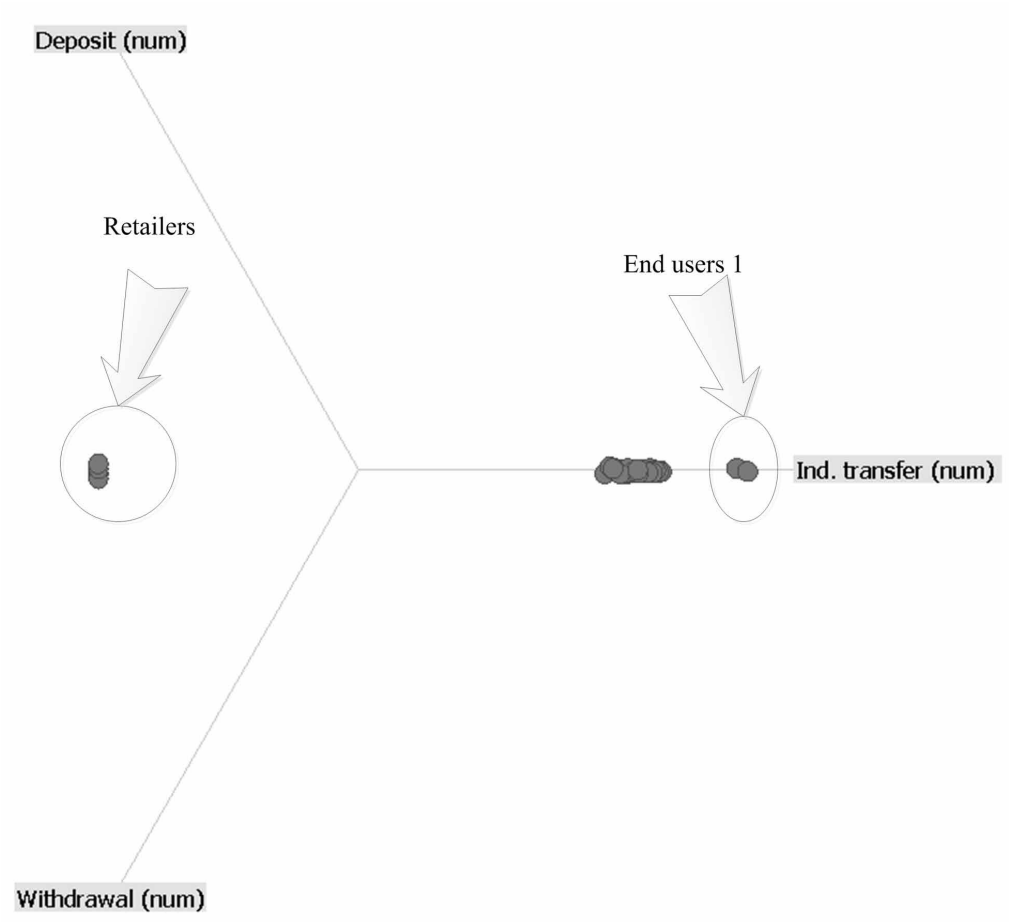
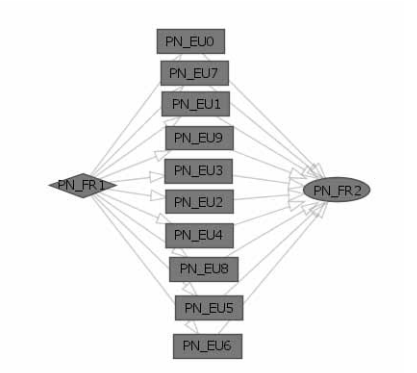


Figure 8. The structure of the examined money laundering scenario



or infected by malware. In this case both actors – legitimate and malicious – use the mobile device to carry out transactions in the same window of time. The benchmark dataset contained 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 laundering 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.

In general case when behavior fraud occurs, the following behavior shifts are observed: changes in the user's average transaction amount and transaction frequency. That's why when detecting mobile botnet, the following assumptions were considered: (i) the amount of fraudulent transactions is slightly inferior than the average amount of the regular users transactions, (ii) the time elapsed between two 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. The following transaction attributes were chosen as dimension nodes: number of individual transfers, *mMoney* withdrawals and deposits, number of merchant and air recharge payments. Figure 9 shows the results of the RadViz visualization of the MMTS subscribers. It is seen that there are groups of merchants and retailers that lie separately due to peculiarities of their roles in the MMTS. The majority of the end users are located near the center of the RadViz visualization that means that they use different types of mobile money services rather uniformly. However, there is a group of four end users that have individual money transfers significantly prevailing over transactions of other types. They are labeled as *End users 2* in the Figure 9.

The link analysis of these users shows that the sets of MMTS subscribers making individual transfers are intersecting. These two facts allow us to conclude that these four 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 Figure 10.

The temporal profile of the mules is shown in Figure 11. It is clearly seen that they regularly make up to 6 withdrawal operations per day.

Though the RadViz visualization of the MMTS users was helpful when revealing mules in the money laundering and mobile botnet scenarios it was not useful when detecting cases of the mobile phones. That is why the authors investigated the test dataset using heat map visualization. As in case of mobile phone theft the fraudster tries to withdraw money several times during a short range of time the changes in number of the withdrawal transactions changes during four months were monitored. The authors set one day as time unit to track the changes and discovered that MMTS users usually make one or maximum two withdrawal operations during one day and, thus, spotted four bursts of suspicious withdrawal activity during all time period being examined. Figure 12 shows day with "normal" withdrawal activity. Under "normal" activity the authors understand the activity typical for the majority of the days examined. Figure 13 shows a day with burst of withdrawal activity: 20 subscribers made 4 withdrawal operations within one day. The examination of their temporal profiles showed that such activity is not typical to them (Figure 14). Analysis of their contacts showed that there are no intersections in their contacts, so we may conclude that it is not a case of money laundering scheme, but could be a case of mobile phone theft. The analysis of the first case of such anomalous activity showed that the thief tries

Figure 9. RadViz visualization of MMTS users in behavioral fraud scenario

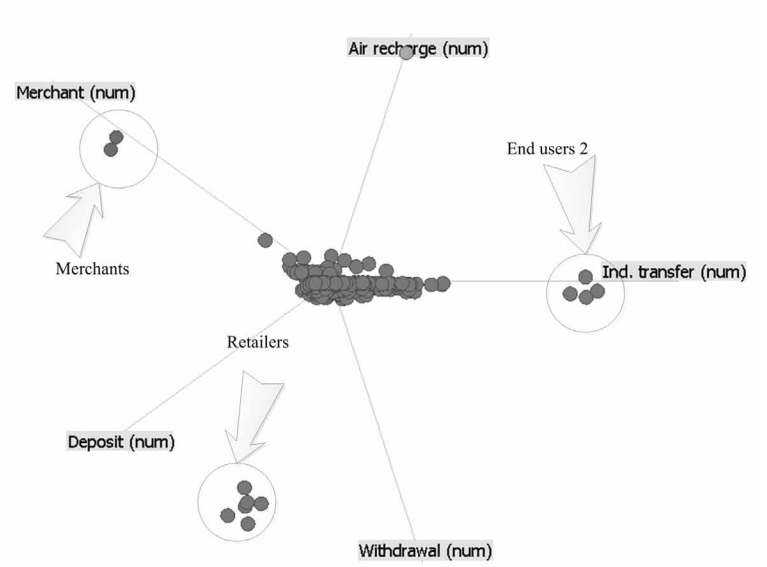


Figure 10. Detection of mobile botnet structure using graph-based presentation of the MMTS user' contacts

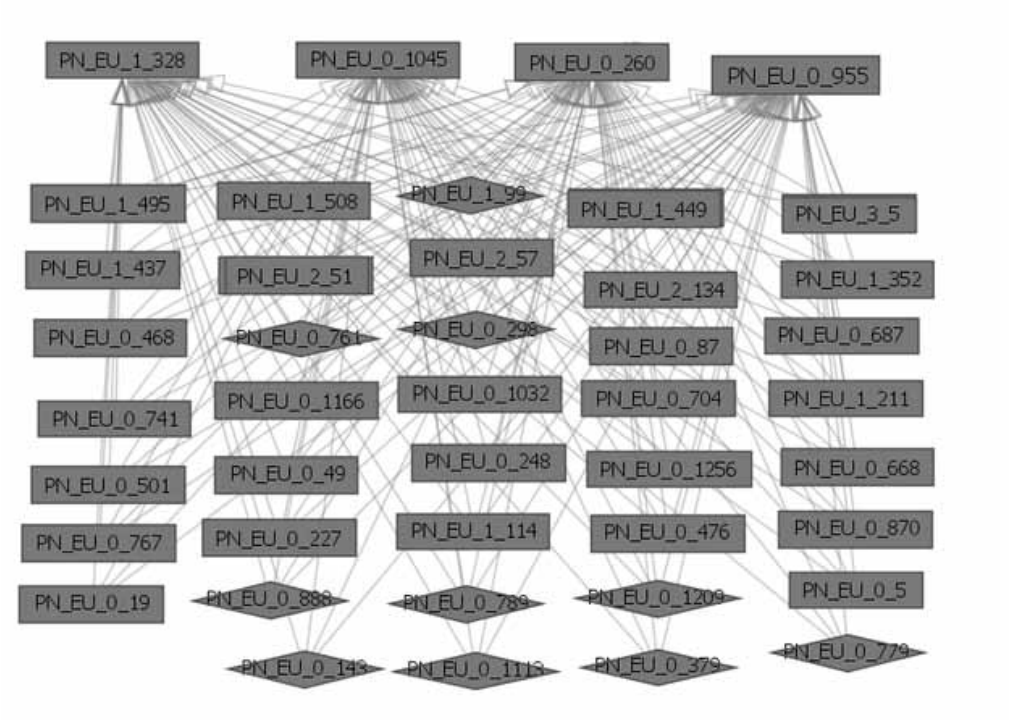
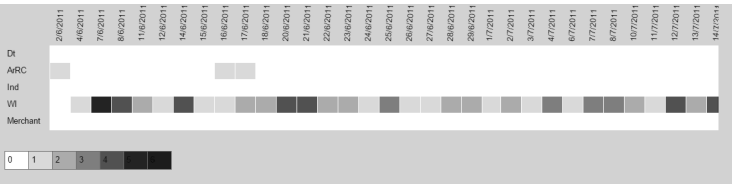


Figure 11. Temporal profile of the mule in the mobile botnet



to withdraw money four times by referring to different retailers. The similar attack scenario was observed for the rest three cases of anomalous bursts of withdrawal activity.

USABILITY EVALUATION AND DISCUSSION

To assess the efficiency of the designed visualization technique the authors used ISO/IEC 9126-1 (2001) standard purposed to evaluate the software quality. This standard specifies a model for quality which has the following characteristics: effectiveness, productivity (efficiency), safety and satisfaction. In this research the authors focused on evaluating the effectiveness of the proposed visualization technique. The ISO/IEC 9126 defines effectiveness as "accuracy and completeness with which the users achieve specified goals" (ISO/IEC 9126-1, 2001) and provides three metrics to measure effectiveness – task effectiveness, task completion and error frequency which are used to assess the proportion of the correctly achieved goals of the task, the proportion of the completed tasks and the frequency of errors. To evaluate this metrics the authors used *inspection* evaluation method which assumes a usage of "benchmark (real or artificial) datasets and expert evaluators to examine subjectively the effectiveness of different visualization techniques for different tasks, by visually inspecting the output of the visualization techniques" (Marghescu, 2007-1, p.46).

There were 5 datasets of MMTS transactions created using MMTS log synthetic simulator (Gaber et al., 2013), one of these datasets did not contain any fraudulent activity, while the rest of them contained different fraudulent scenarios: money laundering activity, mobile phone theft and mobile botnet infection. The brief description of the datasets used in evaluation process is shown in Table 2.

The focus group consisted of 5 specialists having solid experience in information security and intrusion detection techniques and 10 graduate students studying information security. Among specialists there were both practitioners and scientific researchers. As participants had almost no knowledge in MMTS as well as in fraud detection used in these systems we presented them a brief introductory workshop. Within this workshop the authors described basic principles of the MMTS functioning: key user roles, basic operations, how they are implemented. A particular attention was paid on presenting different types of frauds that could present in the systems as well on what parameters of transaction activity should be examined when detecting frauds. Afterwards the authors introduced the MMTView tool to the participants, describing its visual design, characteristics of the RADViz visualization and available interaction techniques. Before analyzing test datasets the participants practiced with the MMTS tool and had a possibility to ask questions if they occurred. Then they were given 5 datasets and were asked to answer following questions:

1. Determine whether dataset contains any suspicious activity.

Figure 12. The "normal" withdrawal activity represented using heat map

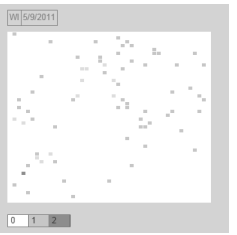


Figure 13. The heat map representation of the day with anomalous burst of withdrawal activity

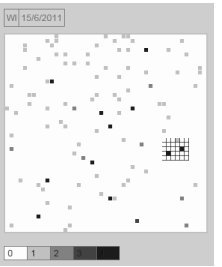


Figure 14. Temporal profile of the users whose mobile device was stolen

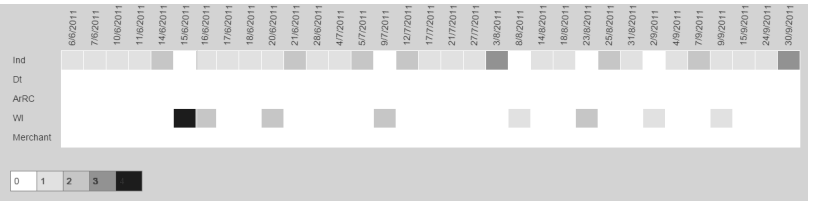


Table 2. Description of the test datasets

#	**Dataset description**
1	Money laundering activity (500 regular users, 10 mules, 6 merchants, 4 retailers)
2	Mobile botnet infection and mobile phone theft (2 merchants, 6 retailers and 4010 users, 4 of which are mules; 3 thieves and 39 infected mobile devices)
3	Only legitimate activity
4	Money laundering activity (500 regular, users, 5 mules, 8 merchants, 4 retailers)
5	Mobile botnet infection and mobile phone theft (2 merchants, 5 retailers and 4000 users, 5 of which are mules; 2 thieves and 25infected mobile devices)

2. If the fraudulent activity is present, determine what type of fraud is present. Note that data set may contain several fraudulent scenarios.
3. If the mobile botnet is detected, determine its structure: users-mules, users, whose accounts are used to withdraw money. Describe malicious scenario (average transaction sum, transaction frequency).
4. If the case/cases of mobile phone theft is determined, a) list a number of victims, b) describe the malicious scenario (average transaction sum, number of malicious transaction).
5. If the money laundering activity is present, determine the structure of the money laundering scheme: fraudsters who send or withdraw money, mules, whose accounts are used to transfer money.

After the completion of the analysis tasks the participants were asked to evaluate the system GUI by filling up the questionnaire, consisted of 4 questions and were encouraged to tell their suggestions or critics. Answering on questions, they had to score the system from 1 to 5 (1 = very easy, 5 = very difficult). The four questions are as follows:

1. Is it easy or difficult to learn the MMTViewer?
2. Is it easy or difficult to explore data using MMTViewer (assess interaction mechanisms)?
3. Is it easy or difficult to interpret results of RadViz visualization?
4. Is it easy or difficult to interpret results of scatter plot based visualization of the MMTS users?
5. Is it easy or difficult to explore transactions using a set of heat map visualizations?

The results of the test tasks implementation are presented in Table 3. The accuracy rate equals to 93% for the experts and 84% for the students. As it seen from the table almost all participants correctly determined the character of the transaction activity in the dataset being examined, only one student made an error in assessing dataset #3 which contained only legitimate activity. This happened because a few MMTS users in this dataset periodically exhibited rather high withdrawal activity during short period time which was mistakenly interpreted as case of the mobile phone theft. However, periodic high withdrawal activity is not a sign of this fraud. The participants correctly answered all questions relating to the mobile botnet infection and money laundering scenarios. The detection of all cases of mobile phone thefts caused a certain difficulties for both experts and students. One of the experts failed to determine one case of mobile phone theft, however, he correctly described the patterns of the attack for the rest cases. Two students did not discovered cases of mobile phone theft at all. Lately, when discussing the results with them, the authors found out that this happened because they did not choose the correct time unit to monitor the changes in transactions activity. Two students among those who correctly determined all cases of mobile phones made mistakes in determining the number of victims. They mistakenly classified one user as victim because he exhibited high withdrawal activity at the same time period when the case of mobile phone took place; however, according to his temporal profile the high periodical withdrawal activity is typical for him/her. The analysis of the errors and discussion of the test results with participants showed that some errors were made due to lack of experience and attention to details such as correct interpretation of the temporal profiles in conjunction with user contact analysis. The results could be noticeably better if additional interaction mechanisms were provided. The experts advised to implement a search-by-example mechanism for the main heat map based view that could significantly simplify a detection of cases of fraudulent activity with similar patterns. They also marked that a possibility to get temporal profile of the user by

clicking on element of RadViz visualization or graph visualization could be a very helpful option. However, all participants liked the visual models selected to explore transactions activity in the MMTS, they marked that results of the RadViz visualization is easy to interpret. Most of the participants including experts think that MMTViewer is able to support transaction analysis even by a non-specialist in mobile payments field after the short introduction course. The experts marked that the tool is able to find new patterns of the fraudulent scenarios. Thus, in general, the feedback on the tool was positive, and according to overall ranking the usage of the MMTViewer is easy and helpful when exploring transaction logs (2.3 of 5).

Summarizing the results of the efficiency evaluation of the proposed visualization technique for MMTS transaction activity the authors can conclude that RadViz visualization is helpful when detecting fraudulent scenarios which make use of mules - users whose behavior significantly differs from the behavior of the other MMTS subscribers. It allows also detecting frauds which cause shifts in user behavior with cumulative effect and thus could be revealed when choosing relatively long time unit, i.e. month, to explore MMTS transactions. That is why this technique was effective when detecting mules in the money laundering scheme and the mobile botnet. If attacks are characterized by change of only one transaction behavior attribute, i.e. withdrawal frequency, the usage of heat map visualization is preferable. Another important prerequisite of successful detection of fraudulent activity is a right choice of the time unit for a time scale. If the time unit is longer than attack time window there is a possibility to miss the attack. However, by setting up a short time unit to replay MMTS transactions an analyst may need to examine large sequence of views presenting transactions activity during time period being analyzed. In order to simplify this process it is necessary to implement additional interaction mechanisms speeding up the process of pattern search. The example of such mechanism is a search-by-example mechanism which allows specifying a rule and choosing all entities relevant to it.

CONCLUSION

The analysis of the state-of-art in fraud detection techniques in the mobile money transfer services showed that the most widely technique to explore electronic transactions is interactive graph-based data presentation. It supports link analysis of the user's contacts visually and

Table 3. Results of the test tasks

Task description		**Rate of the correct answers, %**	
		experts	**students**
Determine the presence of malicious activity		100	90
Money laundering scheme	Determine if present in the test dataset	100	100
	Describe the structure of fraudulent scheme	100	100
Mobile botnet infection	Determine if present in the test dataset	100	100
	Determine mules and infected accounts	100	100
	Describe fraudulent scenario pattern	100	100
Mobile phone theft	Determine all cases of mobile phone theft	80	70
	Determine the number of victims	80	71
	Describe the pattern of fraudulent scenario	80	71

enables application of graph-theoretic algorithms in order to discover structural peculiarities such as bridges and cliques.

The authors proposed to form metaphoric presentation of the MMTS subscriber behavior according to his/her transaction activity. The user's activity is assessed basing on mean amount of transactions made, their frequency, and type of operations used. The RadViz visualization technique supports graphical presentation of the MMTS users according to their behavior and allows determining clusters of users exhibiting similar behavior and outliers. The RadViz visualization of the MMTS users is considered as a starting point of transaction analysis supported by traditional graph-based presentation of subscribers' transactions. To be able to analyze changes in users' behavior we developed a set of heat map based views which are used to monitor the MMTS subscribers' activity and form their temporal profile. The latter could be used to assess suspicious changes in transactions attributes in context of everyday activity.

The authors described a usage scenario that could be used to detect fraudulent activity and implemented the efficiency evaluation of the proposed visualization technique. The experts who participated in the efficiency evaluation process highlighted the ability of the tool to detect different patterns of the fraudulent activity in MMTS and gave valuable recommendations how to improve interaction mechanisms for searching similar transaction patterns.

The future research will be devoted to the elaboration interaction techniques supporting similarity search functionality, and designing data reduction techniques for pixel based visualization.

ACKNOWLEDGMENT

This work was supported by the Ministry of Education and Science of the Russian Federation (contract # 14.604.21.0137, unique contract identifier RFMEFI60414X0137).

REFERENCES

Achemlal, M., et al. (2011). *Scenario requirements*. (Tech. rep.) MASSIF FP7-257475 project.

Al-Khatib, A. (2012). Electronic Payment Fraud Detection Techniques. *World of Computer Science and Information Technology Journal (WCSIT)* (2), 137-141.

Ankerst, M., Berchtold, S., & Keim, D. A. (1998). Similarity Clustering of Dimensions for an Enhanced Visualization of Multidimensional Data. *Proceedings of the IEEE Symposium on Information Visualization (INFOVIS '98)* (pp. 52-60). Washington: IEEE Computer Society. doi:10.1109/INFVIS.1998.729559

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602–613. doi:10.1016/j.dss.2010.08.008

Chang, R., Ghoniem, M., Kosara, R., Ribarsky, W., Yang, J., Suma, E., & Ziemkiewicz, C., Kern, & D., Sudjianto, A. (2007). WireVis: Visualization of Categorical, Time-Varying Data From Financial Transactions. *Proceedings of the IEEE Symposium on Visual Analytics Science and Technology (VAST 2007)* (pp.155-162) Washington: IEEE Computer Society. doi:10.1109/VAST.2007.4389009

Chukwa project. (2015). Retrieved from https://chukwa.apache.org/

ColorBrewer2. (2015). Retrieved from http://colorbrewer2.org

Coppolino L., D'Antonio S., Formicola V., Massei C., Romano L. (2015). Use of the Dempster–Shafer theory to detect account takeovers in mobile money transfer services. Journal of Ambient Intelligence and Humanized Computing.

Delamaire, L., Abdou, H., & Pointon, J. (2009). Credit card fraud and detection techniques: a review. Banks and Bank systems, 4(2), 57-68.

Delloite. (2015). Visual Analytics: Revealing Corruption, Fraud, Waste, and Abuse. Presentation of the Forensic Center. Retrieved from http://www.slideshare.net/ DeloitteForensicCenter/visual-analytics-revealing-corruption-fraud-waste-and-abuse-13958016

Di Caro, L., Frias-Martinez, V., & Frias-Martinez, E. (2010). *Analyzing the Role of Dimension Arrangement for Data Visualization in Radviz. Advances in Knowledge Discovery and Data Mining. LNCS* (Vol. 6119, pp. 125–132). Berlin, Heidelberg: Springer-Verlag. doi:10.1007/978-3-642-13672-6_13

FATF. (2010). Money Laundering using New Payment Methods. Retrieved from http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneyla

Fiserv (2015). Financial Crime Risk Management solution. Retrieved from http://www.fiserv.com/risk-compliance/financial-crime-risk-management.htm

Gaber, C., Hemery, B., Achemlal, M., Pasquet, M., & Urien, P. (2013). Synthetic logs generator for fraud detection in mobile transfer services. *Proceedings of the Int. Conference on Collaboration Technologies and Systems (CTS 2013)*. (pp.174-179). New York: IEEE. doi:10.1109/CTS.2013.6567225

ISO. IEC 9126-1 (2001). Product quality. Part 1: Quality model. Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22749

Jack, W., Tavneet, S., & Townsend, R. (2010). Monetary Theory and Electronic Money: Reflections on the Kenyan Experience. *Economic Quarterly*, 96(1), 83-122.

Keim, D., Andrienko, G., Fekete, J.-D., Goerg, C., Kohlhammer, J., & Melancon, G. (2008). Visual Analytics: Definition, Process, and Challenges. In A. Kerren et al. (Eds.), Information Visualisation, LNCS (Vol. 4950, pp.154-175). Berlin, Heidelberg: Springer-Verlag.

Kintzel, C., Fuchs, J., & Mansmann, F. (2011). Monitoring Large IP Spaces with ClockView. *Proceedings of the International Symposium on Visualization for Cyber Security (VizSec)*. New York: ACM. doi:10.1145/2016904.2016906

Korczak, J., & Łuszczyk, W. (2011). Visual Exploration of Cash Flow Chains. *Proceedings of the Federated Conference on Computer Science and Information Systems*, (pp.41–46). New York: IEEE.

Kotenko, I., & Novikova, E. (2013). VisSecAnalyzer: a Visual Analytics Tool for Network Security Assessment. *8th International Conference on Availability, Reliability and Security (ARES 2013). LNCS* (Vol. 8128, pp. 345-360). Berlin, Heidelberg: Springer-Verlag.

Lin, L., Cao, L., & Zhang, C. (2005). The fish-eye visualization of foreign currency exchange data streams. *Proceedings of the Asia-Pacific Symposium on Information Visualisation (APVis)*, (*Vol. 45,* pp. 91-96). Darlinghurst: Australian Computer Society, Inc.

M-Pesa. (2015). Mobile Payment System. Retrieved from http://www.vodafone.com/content/index/about/about-us/money_transfer.html

Marghescu, D. (2007-1). *Evaluating Multidimensional Visualization Techniques in Data Mining Tasks. TUCS Dissertations*, 107. Turku: Turku Centre for Computer Science.

Marghescu, D. (2007-2). *Multidimensional Data Visualization Techniques for Financial Performance Data: A Review* (TUCS Tech. Rep. No 810). Turku, Finland: University of Turku.

McPherson, J., Ma, K.-L., Krystosk, P., Bartoletti, N., & Christensen, M. (2004). *PortVis: A Tool for Port Based Detection of Security Events. Proceedings of the ACM workshop on Visualization and data mining for computer security (VizSEC/DMSEC '04)* (pp. 73–81). New York: ACM. doi:10.1145/1029208.1029220

Merrit, C. (2010). *Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments. (Tech. rep.)*. Atlanta, USA: Federal Reserve Bank of Atlanta.

Neural-technologies. (2015). Minotaur Fraud Detection Software - Finance Sector. Retrieved from http://www.neuralt.com/fraud_detection_software.html

Nice Actimize. (2015). Integrated Fraud Management. Retrieved from http://www.niceactimize.com/index.aspx?page=solutionsfraud

Novikova, E., & Kotenko, I. (2013). Analytical Visualization Techniques for Security Information and Event Management. *Proceedings of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013)* (pp. 519-525). New York: IEEE. doi:10.1109/PDP.2013.84

Novikova, E., & Kotenko, I. (2014). Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services. Availability, Reliability and security in information systems, LNCS (LNCS) (Vol. 8708, pp. 63-78). Berlin, Heidelberg: Springer-Verlag.

Okutyi, E. (2015). Safaricom tightens security on M-Pesa with fraud management system. Retrieved from http://www.humanipo.com/news/1341/Safaricom-tightens-security-on-M-Pesa-with-Fraud-Management-system

Orange Money. (2012). 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)

Prefuse (2015). Information Visualization toolkit. Retrieved from http://prefuse.org/

Rieke, R., Zhdanova, M., Repp, J., Giot, R., & Gaber, C. (2013). Fraud Detection in Mobile Payments Utilizing Process Behavior Analysis. *The 2nd International Workshop on Recent Advances in Security Information and Event Management (RaSIEM 2013)* (pp. 662-669). New York: IEEE.

Ron, D., & Shamir, A. (2013). Quantitative Analysis of the Full Bitcoin Transaction Graph. *The 17th Int. Conference on Financial Cryptography and Data Security, LNCS* (Vol. 7859, pp.6-24). Berlin, Heidelberg: Springer-Verlag.

SAS. (2015). Fraud detection solutions. Retrieved from http://www.sas.com /offices/europe/uk/industries/banking/fraud-detection.html

Schreck, T., Tekusova, T., Kohlhammer, J., & Fellner, D. (2007). Trajectory-based visual analysis of large financial time series data. *ACMSIGKDD Explorations Newsletter*, *9*(2), 30–37. doi:10.1145/1345448.1345454

Shneiderman, B. (2003). Dynamic queries for visual information seeking. *The Craft of Information Visualization: Readings and Reflections*, 14-21.

StatReport (2012). Second quarter of the financial year 2012/2013. Quarterly sector statistics report. Communications Commission of Kenya. Retrieved from http://www.cofek.co.ke/Quarterly%20Sector%20Statistics%20Report%20Second%20Quarter%20of%20the%20Financial%20Year%202012-13%20Oct-Dec.pdf

Wattenberg, M. (1999). *Visualizing the stock market. CHI Extended Abstracts on Human Factors in Computing Systems* (pp. 188–189). New York: ACM.

Westphal, C. R. (2012). Patterns for Financial Intelligence Units (FIUs) and Anti-Money Laundering (AML) Operations. Retrieved from [REMOVED HYPERLINK FIELD]http://support.visualanalytics.com/technicalArticles/whitePaper/pdf/VAI%20AML%20FIU%20Patterns%20Presentation.pdf

Xie, C., Chen, W., Huang, X., Hu, Y., Barlowe, S., & Yang, J. (2014). VAET: A Visual Analytics Approach for E-Transactions Time-Series. *IEEE Transactions on Visualization and Computer Graphics*, *20*(12), 1743–1752. doi:10.1109/TVCG.2014.2346913 PMID:26356888

Ziegler, H., Jenny, M., Gruse, T., & Keim, D. A. (2010). Visual Market Sector Analysis for Financial Time Series Data. *Proceedings of the IEEE Symposium on Visual Analytics Science and Technology (VAST)* (pp.83-90). New York: IEEE. doi:10.1109/VAST.2010.5652530