

Chapter 9

Visualization–Driven Approach to Fraud Detection in the Mobile Money Transfer Services

Evgenia Novikova

SPIIRAS, Russia & St. Petersburg Electrotechnical University “LETI”, Russia

Igor Kotenko

SPIIRAS, Russia & St. Petersburg ITMO University, Russia

ABSTRACT

Mobile money transfer services (MMTS) are widely spread in the countries lacking conventional financial institutions. Like traditional financial systems they can be used to implement financial frauds. The chapter presents a novel visualization-driven approach to detection of the fraudulent activity in the MMTS. It consists in usage of a set of interactive visualization models supported by outlier detection techniques allowing to construct comprehensive view on the MMTS subscriber behavior according to his/her transaction activity. The key element of the approach is the RadViz visualization that helps to identify groups with similar behavior and outliers. The scatter plot visualization of the time intervals with transaction activity supported by the heat map visualization of the historical activity of the MMTS subscriber is used to conduct analysis of how the MMTS users' transaction activity changes over time and detect sudden changes in it. The results of the efficiency evaluation of the developed visualization-driven approach are discussed.

INTRODUCTION

Firstly introduced in 2000 in Philippines, mobile money, the electronic cash card associated with a mobile phone account, has gained a solid market segment especially in the developing countries. Currently the mobile money transfer services (MMTS) are available in over 80 countries and work on smartphones and basic feature phones offering a good alternative to bank accounts. For example, M-PESA, mobile

DOI: 10.4018/978-1-5225-5693-0.ch009

money transfer service supported by Safaricom, Kenya's largest mobile network operator is arguably the most developed mobile money transfer system in the world. It has over 18.2 million subscribers in a country of 43.2 million (Kamana, 2014). Other M-PESA markets such as Gabon, Ghana, Kenya, Namibia, Tanzania, India and Romania have more than 40% of active mobile money users. (Corkin, 2016). Another popular mobile money transfer service is Orange Money that is deployed in 10 countries and gathers around 14% of the mobile subscribers of these countries (Orange Money, 2017).

In general case, 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, to accept payments for goods and services from the customers via their mobile phones, and to withdraw deposits for regular money. People in Kenya can now also use M-Pesa to top up cashless travel cards for public transport (Kamana, 2014). 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 usage of the MMTS from one side makes business owners less susceptible to the risks of handling cash, such as theft and fake currency. From the other side, the mobile financial services create novel opportunities for fraud (CGAP Report, 2017). For example, the MMTS provide higher level of anonymity, speed and portability compared to traditional banking systems. Thus, additional risks caused by the large number of non-bank participants are introduced (Merrit, 2010). Therefore, it is required to determine new approaches to detect frauds in mobile money transfer services.

In this chapter the authors present *a novel visualization-driven approach to the analysis of the MMTS subscribers' transactions* that can assist in anomaly detection. It allows an analyst to form overall understanding of the MMTS users' activity by providing a metaphoric presentation of their behavior in the system and then focus on users of the particular interest by drilling down into their contacts and transactional activity. Its key elements are (1) *the RadViz visualization* (Ankerst et al., 1998) of the MMTS users that helps to determine groups of similarities and outliers among them, (2) *the scatter plot presentation* of the time periods with the subscriber's transactional activity targeted to explore suspicious changes in it supported by the graph-based presentation of the subscriber's contacts and (3) *the heat map presentation* of the transaction attributes used to form temporal profile of the user's activity.

The main contribution of the authors is the interactive visual representation of the *MMTS subscribers allowing detection of the groups of users with similar behavior and outliers*. To the best of authors' knowledge, this work is the first to exploit the RadViz visualization technique to visualize MMTS subscribers and the scatter plot presentation to analyze transactional activity of the particular user. This chapter is extended version of the paper (Novikova et al, 2014). It contains detailed description of the proposed approach, including its enhancement targeted to detect short-term types of the behavior frauds (such as theft of mobile phones), suggested analysis workflow as well as discussion of the introduced modification and its influence on the efficiency of the proposed approach.

The rest of the chapter is structured as follows. Section "SUBJECT AREA AND RELATED WORK" presents the overview of the mobile money transfer service, its structure and the related work. Section "THE PROPOSED VISUALIZATION-DRIVEN APPROACH" describes the approach suggested, including the analysis workflow and its key elements. Section "USAGE SCENARIOS" outlines the case studies used to demonstrate the proposed approach for fraud detection in mobile payments. Section "EFFICIENCY EVALUATION AND DISCUSSION" considers the results of the efficiency evaluation. Final sections define the directions of the future research, and sum up the authors' contribution.

30 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/visualization-driven-approach-to-fraud-detection-in-the-mobile-money-transfer-services/208462

Related Content

Face Recognition System using Discrete Cosine Transform combined with MLP and RBF Neural Networks

Fatma Zohra Chelali and Amar Djeradi (2012). *International Journal of Mobile Computing and Multimedia Communications* (pp. 11-35).

www.irma-international.org/article/face-recognition-system-using-discrete/73718

Understanding One-Handed Use of Mobile Devices

Amy K. Karlson, Benjamin B. Bederson and Jose L. Contreras-Vidal (2008). *Handbook of Research on User Interface Design and Evaluation for Mobile Technology* (pp. 86-101).

www.irma-international.org/chapter/understanding-one-handed-use-mobile/21825

Mobile Data Offloading Using Opportunistic Communication and AP Deployment: A Case Study

Sanjit Kumar Dash, Sasmita Mishra and Jibitesh Mishra (2017). *International Journal of Mobile Computing and Multimedia Communications* (pp. 66-84).

www.irma-international.org/article/mobile-data-offloading-using-opportunistic-communication-and-ap-deployment/193260

Innovative Formalism for Biological Data Analysis

Calin Ciufudean (2019). *Advanced Methodologies and Technologies in Network Architecture, Mobile Computing, and Data Analytics* (pp. 390-402).

www.irma-international.org/chapter/innovative-formalism-for-biological-data-analysis/214630

Environments for Mobile Learning

Han-Chieh Chao, Tin-Yu Wu and Michelle T.C. Kao (2009). *Mobile Computing: Concepts, Methodologies, Tools, and Applications* (pp. 117-121).

www.irma-international.org/chapter/environments-mobile-learning/26493