УДК 004.056.5 **DOI** 10.15622/sp.48.2

Е.С. Новикова, И.В. Котенко

ВЫЯВЛЕНИЕ АНОМАЛЬНОЙ АКТИВНОСТИ В СЕРВИСАХ МОБИЛЬНЫХ ДЕНЕЖНЫХ ПЕРЕВОДОВ С ПОМОЩЬЮ RADVIZ-ВИЗУАЛИЗАЦИИ

Новикова Е.С., Котенко И.В. **Выявление аномальной активности в сервисах мобильных денежных переводов с помощью RADViz-визуализации.**

Аннотация. Сети мобильной связи представляют собой удобную инфраструктуру для предоставления финансовых сервисов, поскольку они обладают рядом достоинств, связанных с широким распространением и достаточно низкой себестоимостью финансовых транзакций. В настоящей работе рассматривается сценарий мобильных денежных переводов, в которых оператор сотовой связи не только предоставляет инфраструктуру, но и выпускает виртуальные денежные средства.

В работе авторы предлагают новый подход к анализу транзакций, основанный на использовании группы взаимосвязанных интерактивных моделей визуализации данных, характеризующих действия пользователей в системе денежных переводов. В его основе лежит графическое представление пользователей с помощью методики визуализации RadViz. Она позволяет выделить группы пользователей, обладающих схожим поведением, и абонентов, своим поведением отличающихся от основной массы, и при этом обладает низкой вычислительной сложностью. Анализ научных работ показал, что авторы первыми предложили использовать данную методику визуализации для исследования денежных переводов. RadViz-визуализация пользователей сервиса мобильных денежных переводов поддерживается графом их контактов. Граф контактов является наиболее распространенной методикой графического представление операций в финансовых системах, поскольку он позволяет изучить структурные свойства связей между пользователями, выявив мосты и клики графа.

Разработанная методика визуального анализа была апробирована на тестовых данных, содержащих различные сценарии мошеннической деятельности в СМДП. Анализ применения RadViz-визуализации пользователей системы на различных тестовых данных показал, что она полезна при обнаружении мошеннических сценариев, которые предполагают использование пользователей-мулов, чье поведение существенно отличается от поведения других абонентов СМДП. Таким образом, она позволяет выявить финансовые правонарушения, которые связаны с длительными, возможно, незначительными изменениями в поведении пользователей, однако имеющих кумулятивный эффект, и поэтому могут быть раскрыты при выборе достаточно длительного периода времени. По этой причине данная модель визуализации оказалась эффективна при обнаружении мулов в схеме отмывания денег и мобильной бот-сети.

1. Введение. Сети мобильной связи представляют собой удобную инфраструктуру для предоставления финансовых сервисов, поскольку они обладают рядом достоинств, связанных с широким распространением и достаточно низкой себестоимостью финансовых транзакций. В настоящей работе рассматривается сценарий мобильных денежных переводов, в которых оператор сотовой связи не только предоставляет инфраструктуру, но и выпускает виртуальные денежные

средства. Этот сервис позволяет своим пользователям вносить и снимать деньги, переводить деньги другим пользователям, оплачивать счета, оплачивать сотовую связь. Пользователи таких сервисов могут иметь различные роли в системе, они могут быть розничными агентами оператора мобильной связи, с помощью которых осуществляются операции пополнения мобильного счета и снятия с них денежных средств, поставщиками различных услуг и товаров и обычными пользователями финансовых сервисов.

Рост покрытия сотовых сетей, а также их доступность обеспечивает широкое распространение сервисов мобильных денежных переводов (СМДП), особенно в развивающихся странах, таких как Кения, Индия, Уганда и Филиппины [1, 2]. Особенно эти сервисы востребованы у людей, которые не имеют своего собственного банковского счета и которым намного удобнее и проще использовать мобильный телефон для выполнения платежей и денежных переводов другим пользователям. В последнее время наблюдается рост популярности подобных сервисов и в развитых странах, в которых жители лишились банковского счета в результате распространения финансового кризиса, и провайдеры финансовых сервисов оценивают потенциал новых платежных систем, возникших в развивающихся странах для удовлетворения потребностей пользователей.

Однако по мере роста рынка СМДП повышаются и риски, связанные с их использованием, поскольку они становятся объектом атаки опытных и высоко мотивированных злоумышленников, а большие объемы данных значительно снижают способность механизмов обнаружения вредоносной активности своевременно выявлять нарушения. Как и другие системы денежных переводов, СМДП могут быть использованы в схемах отмывания денежных средств или получения доступа к данным пользователей СМДП для получения финансовой выгоды (кража мобильного устройства или заражение вредоносным программным обеспечением) и т.д.

В настоящей статье авторы предлагают новый подход к анализу транзакций, основанный на использовании группы взаимосвязанных интерактивных моделей визуализации данных, характеризующих действия пользователей СМДП и способствующих обнаружению аномалий и возможных правонарушений. Выбранные модели визуализации позволяют аналитику получить общее представление об активности в системе, а затем сосредоточиться на пользователях, представляющих особый интерес, путем детализации их операций. В основе предложенного подхода лежит графическое представление пользователей с помощью методики визуализации RadViz [3]. Она позволяет выделить группы пользователей, обладающие схожим

поведением, и абонентов, своим поведением отличающихся от основной массы, и при этом обладает низкой вычислительной сложностью.

Статья структурирована следующим образом. В разделе 2 представлены методики визуализации, используемые для обнаружения финансовых махинаций. В разделах 3 и 4 детально описываются исходные данные и предложенный подход, в том числе разработанные модели визуализации и методики взаимодействия с ними. В разделе 5 представлена общая методика работы с предложенными моделями визуализации, а в разделах 6 и 7 представлены результаты ее использования для выявления финансовых мошенничеств различного типа в СМДП. В заключении подводятся итоги исследования и обозначаются дальнейшие направления исследований.

2. Методики визуального анализа для обнаружения аномальной активности в СМДП. Применение автоматических методик анализа для обнаружения любых схем мошенничества предполагает, что данные четко структурированы, полны и корректны, не изменяются с течением времени, и задача четко определена [4]. Реальные данные редко отвечают этим требованиям. Кроме того, эти методики в большинстве случаев воспринимаются конечными пользователям как черные ящики, выдающие конечный результат без его пояснения. Методы визуальной аналитики помогают справиться с огромными объемами разнородных и зашумленных данных. Их можно рассматривать как процесс генерации и проверки гипотезы, который интуитивно понятен и не требует явного применения сложных математических и статистических методов [4-10].

Сложность структуры финансовых данных позволяет применять различные методики визуализации для их анализа — графы на параллельных координатах, матрицы рассеивания, специальные глифы, карты деревьев, представления на основе иконок и пикселей, дендрограммы. В большинстве случаев они предназначены для решения таких задач, как анализ финансового рынка в целом или отдельных сегментов в частности, оценку финансовых показателей компаний, оценку инвестиций за длительное время.

Модели визуализации, применяемые для обнаружения подозрительной активности в финансовых системах, достаточно просты. Большая часть коммерческого программного обеспечения [11-13] использует линейные графики, круговые диаграммы, гистограммы и глифы в виде измерительных приборов для отображения характеристик финансовых потоков, количества зарегистрированных предупреждений, их типа и критичности и т.д. Выбор этих визуальных моделей объясняется простотой их понимания и способностью передавать наиболее важную информацию. Кроме того, они легко

могут быть включены в отчеты любого уровня и назначения. Помимо стандартных визуальных моделей, в системах обнаружения подозрительной финансовой деятельности часто присутствуют географические карты, поскольку они позволяют обнаруживать регионы с высоким уровнем финансовых рисков, а также определять границы ответственности организации.

Выявление скрытых взаимосвязей между пользователями и отслеживание денежных потоков чаще всего осуществляется с помощью графов контактов пользователей [12-15]. Вершинами графа могут быть различные объекты финансовой деятельности: счета, идентификаторы пользователей, телефоны, кредитные карты, адреса, организации и т.д. Ребра между ними указывают на использование или участие соответствующего объекта в финансовых операциях, а толщина линии обозначает частоту сделки транзакций субъектами. Графы позволяют обнаруживать скрытые связи между клиентами финансовых организаций, формировать паттерны денежных потоков, характерные для мошеннических операций.

Интересная графическая метафора KnotLines для представления последовательности электронных транзакций предложена в [16]. В ее основе лежит нотная нотация: линии отображают связи между операциями, а узлы кодируют подробную информацию о сделках. Это представление поддерживается пиксельным-ориентированным представлением, которое отображает меру схожести транзакции заданному логическому выражению. Сочетание этих двух представлений позволяет достаточно быстро идентифицировать представляющие интерес сделки из большого набора данных.

Похожий подход реализован в инструменте WireVis [17], который был разработан в сотрудничестве с Банком Америки. Транзакции отображаются с помощью специального графического представления, названного Strings and Beads (строки и бисер), в котором строки ссылаются на счета или кластера счетов в течение длительного времени, а бусинки относятся к конкретным операциям, выполненным за заданный день. Основной акцент в нем делается на частотный анализ ключевых слов транзакций.

3. Исходные данные СМДП. В общем случае информация о персональных данных пользователей, а также данные по операциям, совершаемых ими в СМДП, является конфиденциальной и, как следствие, закрытой для исследователей. Одним из возможных решений проблемы отсутствия реальных данных, необходимых как для разработки, так и оценки моделей и методик визуального анализа, используются искусственно сгенерированные данные. Этот подход

широко применяется при обучении моделей анализа данных в системах автоматического обнаружения и предотвращения вторжений [18].

Для моделирования платформы мобильных денежных платежей и действий пользователей в работе используется генератор транзакций СМДП [18]. Он позволяет создавать тестовые наборы данных, содержащие различные сценарии аномальной активности. Используемые в генераторе модели легитимного и вредоносного поведения пользователей построены на основе свойств реальных транзакций СМДП. Кроме того, они содержат специальное поле ground proof, определяющее тип транзакции — легитимная или мошенническая, которое может быть использовано для проверки корректности результатов, полученных в процессе анализа.

Генератор транзакций СМДП формирует только логи транзакций, которые содержат следующую информацию: номера телефонов отправителя и получателя, идентификаторы их счетов, роль абонентов в системе (подписчик системы, поставщик услуг, оператор и т.д.), идентификатор транзакции, метка времени, тип транзакции (индивидуальные денежные переводы между физическими лицами, пополнение и снятие денежных средств из мобильного кошелька, и т.д.), сумма денежного перевода, статус транзакции (успешно завершена, ошибка), а также баланс отправителя и приемника до и после операции. Исследование показало, что этих данных достаточно для того, чтобы выявить признаки нелегитимного использования системы мобильных денежных переводов.

Разработанная методика визуального анализа была апробирована на тестовых данных, содержащих различные сценарии мошеннической деятельности в СМДП. Следует отметить, что в сгенерированных сценариях каждый подписчик СМДП имеет только одну учетную запись в системе и роль, связанную с ним (ней), однако это не влияет на точность полученных результатов.

4. Модели визуализации и методики взаимодействия с ними. В основе предлагаемой авторами методики лежит RadViz-визуализация транзакций СМДП. Она позволяет выявить группы пользователей, характеризующих схожим поведением в системе. Под поведением пользователя в системе авторы понимают, какие типы операций обычно совершает пользователь в СМДП, как часто и на какие суммы.

RadViz-визуализация является нелинейной методикой визуализации многомерных данных, которая выполняет отображение n-мерных данных на 2-мерное пространство. Исследуемые признаки объектов представляются в виде координат, размещаемых по окружности. Затем объекты отображаются в виде точек внутри круга,

их положение определяется с помощью метафоры из физики: каждая точка соединяется с помощью *n* пружин к *n* координатным узлам.

Жесткость каждой пружины пропорциональна значению соответствующего атрибута объекта. Таким образом, точка располагается в месте, где силы растяжения пружин находятся в равновесии. Очевидно, что объекты, имеющие более высокое значение определенного атрибута, будут располагаться ближе к соответствующему координатному узлу. Если все *n* атрибутов имеют одинаковые значения, то точка данных находится точно в центре круга. Если объект имеет атрибуты с одинаковыми значениями, а соответствующие координатные узлы располагаются друг напротив друга на окружности, то точка лежит недалеко от центра. В качестве примера рассмотрим рисунок 1.

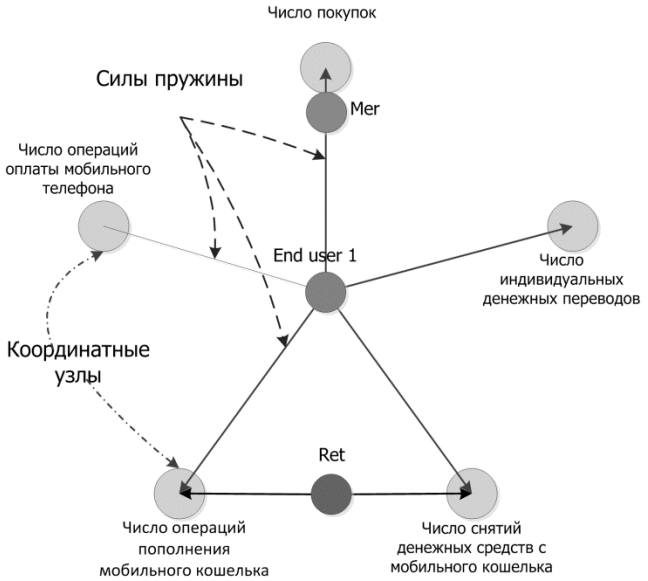

Рис. 1. Схема представления пользователей СМДП с помощью RadViz-визуализации (цвета с учетом схемы)

В соответствии с рисунком 1 пользователь ***Mer*** расположен на оси *Число покупок*, что означает, что он участвует только в операциях предоставления различных розничных услуг и покупок, что, возможно, объясняется его ролью в системе. Пользователь ***Ret*** в равной мере участвует в операциях пополнения мобильного кошелька денежными

средствами и снятием их со счета. Пользователь ***End user 1*** расположен в центре единичного круга, что говорит о том, что одинаково часто пользуется всеми доступными операциями в СМДП: пополнение мобильного кошелька денежными средствами, снятие денег с мобильного кошелька, оплата услуг мобильной связи, покупка товаров и перевод денежных средств другим пользователям системы. Данную методику визуализации можно рассматривать как алгоритм кластеризации, имеющий низкую вычислительную сложность — $O(n)$, где n — число объектов.

Авторы предлагают использовать следующие атрибуты в качестве координатных узлов для описания поведения пользователя в системе мобильных денежных платежей: количество операций различного типа за заданный период времени; средняя сумма денежных переводов с разбиением по типам операций; минимальная или максимальная сумма денежного перевода за заданный период времени с разбиением по типам операций.

Пользователи СМДП отображаются в виде точек разного цвета внутри единичной окружности. Цвет используется для кодирования их роли в СМДП, например, конечные пользователи закрашиваются оранжевым цветом, оператор сотовой связи — желтым, поставщики розничным услуг — пурпурно-красным и т.д. Авторы предполагают, что пользователи, имеющие одинаковую роль в системе, должны формировать группы точек, расположенных рядом, что объясняется схожим поведением в системе. Например, точки, обозначающие поставщиков розничных услуг, должны образовать группу. Расположение конечных пользователей предсказать труднее, поскольку они в общем случае обладают разнообразным поведением в системе, тем не менее они также могут образовывать кластеры точек. Таким образом, следующие особенности расположения точек на графе могут являться признаками потенциального мошенничества:

– пользователь не принадлежит ни к одному кластеру или входит в группу пользователей, имеющих другую роль;

– расположение небольшой группы пользователей существенно отличается от остальных.

Эти аномалии могут стать отправной точкой в анализе действий пользователя в СМДП.

Следует отметить, что расположение точек на плоскости при RadViz-визуализации сильно зависит от выбора координатных узлов и их расположения, т.е. не для каждого набора выбранных атрибутов имеется возможность выявить кластеры и выбросы в данных. Для n

атрибутов существует (n - 1)! / 2 возможных проекций RadViz [19]. Из этого утверждения следует, что при выборе трех атрибутов транзакции в качестве координатных узлов формируется только одна нетривиальная RadViz-проекция объектов, поэтому авторы рекомендуют использовать следующие три атрибута в качестве координат:

– количество индивидуальных переводов за заданный период времени;

– количество операций пополнения мобильного кошелька за заданный период времени;

– количество операций по снятию наличных денег за заданный период времени.

Тем не менее в системе, реализующей предложенную разработанную методику, предусмотрена возможность настройки координат RadViz-визуализации, что позволяет аналитику экспериментировать с исследуемыми данными, выбирая атрибуты из предопределенного списка и задавая их последовательность.

Для исследования контактов пользователей СМДП авторы предлагают использовать граф. Граф контактов является наиболее распространенной методикой графического представления операций в финансовых системах [7, 13, 15, 17]. Основным преимуществом использования графов является возможность изучить структурные свойства связей между пользователями, выявив мосты и клики графа.

В предложенной методике визуального анализа граф используется традиционным образом: его вершины обозначают пользователей системы, а связи между ними — транзакции, связывающие их. Как и в случае RadViz-визуализации, цвет используется для обозначения роли пользователя в СМДП, он также применяется для кодирования типа транзакции. Следует отметить, что все используемые в прототипе цветовые схемы предназначены для отображения категорийных данных, подчеркивают их отличия между собой и созданы с помощью специальной утилиты Color-Brewer [20]. Она позволяет формировать цветовые схемы с учетом типа исходных данных (качественные или количественные), а также характера решаемой задачи (выявление выбросов, сравнение последовательных значений). Кроме того, она позволяет выбрать цвета, которые являются безопасными для людей, страдающих нарушением цветоощущения.

Форма вершины графа зависит от того, является ли пользователь только отправителем транзакций (ромб), получателем (эллипс) или выполняет обе роли (прямоугольник). Эта опция помогает упростить процесс обнаружения абонентов, чьи счета используются только для

снятия наличных или пополнения мобильных кошельков. Если пользователи связаны между собой множеством транзакций одного типа, то они отображаются одной линией, толщина которой определяется мощностью этого множества. Аналитик может управлять размером вершин графа: он может быть определен суммой как принятых, так и отправленных денежных переводов за определенный период времени. Эта опция помогает обнаружить абонентов, которые участвуют в крупных денежных потоках.

Процесс визуального анализа графа поддерживается различными механизмами взаимодействия: фильтрация данных, эффект связывания, управление укладкой вершин графа и получение детальной информации.

Механизм фильтрации позволяет задавать аналитику сложные логические выражения для отображения множества пользователей СМДП или транзакций данных, отвечающих поставленным условиям. Применение эффекта связывания и затемнения позволяет изучить контакты конкретного пользователя: в этом режиме видимыми остаются все входные и выходные ребра выбранного узла, а остальные — скрываются.

Различные способы укладки вершин графа дают возможность аналитику изучить структуру графа. Авторы предлагают использовать два способа укладки графа — радиальный и специальный, в основе которого лежит график рассеивания.

Укладка вершин графа на основе графика рассеивания строится следующим образом. Для каждого узла рассчитываются два параметра — общее число транзакций, совершенных пользователем, и число различных типов транзакций, используемых им. Эти два параметра определяют положение соответствующего узла на плоскости: x-координата определяется общим количеством всех сделок, а y-координата определяется количеством различных типов транзакций (рисунок 2).

Радиальное расположение вершин графа удобно для изучения контактов уже выбранного пользователя. Укладка узлов графа на основе графика рассеивания позволяет быстро разбить пользователей на группы с различным уровнем активности и числом различных типов операций, и поэтому она может быть особенно полезна на начальном этапе изучения логов системы СМДП, поскольку позволяет проверить корректность структурных связей между пользователями.

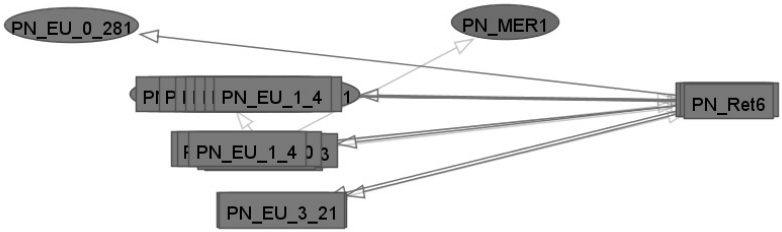

Рис. 2. Расположение вершин графа контактов пользователей СМДП на основе графика рассеивания

Информация о вершинах и ребрах графа доступна в виде всплывающей подсказки и таблицы свойств объектов. Всплывающая подсказка содержит краткую информацию об элементе графа: идентификатор пользователя, количество совершенных операций, тип транзакции, отправитель и получатель денежного перевода. Таблица свойств объекта предоставляет детальную информацию по выбранному объекту. Для вершин графа, представляющих пользователей СМДП, выводятся следующие данные: число выполненных операций с разбивкой по их типам; минимальная, максимальная и средняя суммы денежных переводов с детализацией по типам операций; общая сумма полученных и отправленных денежных переводов. По клику мышки по ребру графа в таблице свойств отображается информация о типе транзакции, ее получатель и отправитель, число транзакций между ними, минимальная и максимальная суммы денежных переводов, статус транзакций.

5. Сценарии использования методики. Любой процесс поиска информации может быть описан следующим образом: общий вид → масштабирование, фокусирование → детали по требованию [21]. Следуя этому принципу, процесс исследования транзакций СМДП может быть описан следующим образом.

На первом этапе аналитик формирует общее понимание об активности всех пользователей в СМДП в рамках выбранного периода времени и выявляет множество пользователей, деятельность которых по каким-либо признакам отличается от остальных. Эта задача может быть выполнена с помощью RadViz-визуализации данных или графа контактов с применением специальной укладки вершин графа.

На следующем этапе аналитик исследует контакты каждого пользователя из определенного ранее множества, и при необходимости

проводит детальный анализ непосредственно транзакций данного пользователя СМДП.

Разработанная методика визуального анализа данных была реализована в программном прототипе MMTViewer, написанном на языке программирования Java. Модели визуализации и механизмы взаимодействия реализованы с использованием графической библиотеки Prefuse Toolkit [22], которая позволяет создавать сложные интерактивные графические представления.

Предлагаемая в работе методика была апробирована на множестве тестовых данных, содержащих следующие сценарии финансовых мошенничеств: отмывание денег, кража мобильного телефона и заражение устройств вредоносным ПО. Все тестовые данных были получены с помощью генератора транзакций СМДП, представленного выше.

6. Выявление схем по отмыванию денежных средств. Существует несколько схем по отмыванию денег [23]. Используемый в работе сценарий финансового правонарушения предполагает использование так называемых пользователей-мулов, с помощью которых обычно скрывается происхождение нелегитимных денег и затрудняется отслеживание финансовых потоков. Мошенники, имеющие определенную сумму денег для отмывания, обычно разделяют ее на несколько частей и отправляют их пользователям-мулам. Позже они выводят эти деньги, используя пользователей, выполняющих роль поставщиков различных услуг и товаров. Последовательности мулов могут состоять из нескольких слоев. В анализируемом сценарии применяется только один слой из нескольких мулов. Тем не менее это условие не ограничивает возможности предлагаемого подхода к обнаружению мошенничества, поскольку задачей предлагаемой методики является выявление аномальной активности в СМДП любого типа, а не конкретной мошеннической финансовой схемы.

При обнаружении аномальной активности с помощью разработанной методики мы использовали следующие исходные предположения: сумма нелегитимных операций меньше, чем средняя сумма обычных, легитимных транзакций; мулы также выполняют законные сделки; внезапное изменение в передаваемых денежных суммах соответствует аномалии.

Эти предположения определили, какие атрибутов транзакций следует использовать в качестве координатных узлов модели визуализации RadViz: количество индивидуальных денежных

переводов, количество операций пополнения мобильного кошелька и количество операций снятия денежных средств из него.

Результат RadViz-визуализации пользователей СМДП представлен на рисунок 3. Видно, что существует группа агентов оператора мобильной связи, обозначенных подписью ***Агенты***, которая расположена обособленно от других абонентов СМДП, это объясняется тем, что они участвуют только в операциях снятия денежных средств с мобильного кошелька и его пополнения. Обычные пользователя СМДП образуют достаточно большую группу точек оранжевого цвета, расположенных достаточно плотно и равномерно вдоль оси Ind. Transfer (num), обозначающей индивидуальные денежные переводы. Это говорит о том, что данный тип финансовых операций преобладает над двумя другими типами. Положение точек на сравнительно равноудаленном расстоянии от координатных узлов Deposit (num) и Withdrawal (num) свидетельствует о том, что пользователи в равном количестве совершают операции пополнения и снятия денежных средств с мобильного кошелька. На рисунке 3 легко можно увидеть двух обычных пользователей системы, которые лежат отдельно от остальных конечных пользователей ***Пользователи 1***. Они отмечены подписью ***Пользователи 2***.

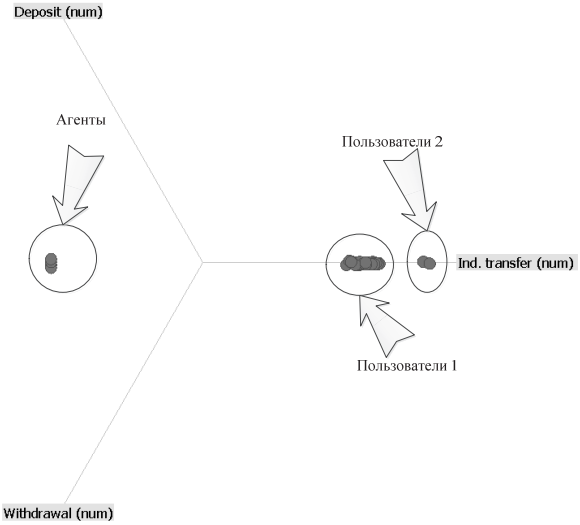

Рис. 3. RadViz-визуализация пользователей СМДП в исследуемом сценарии по отмыванию денег

Их расположение объясняется значительным преобладанием индивидуальных денежных переводов над финансовыми операциями других типов. Граф контактов показал: (1) один из этих пользователей (пользователь PN_FR1) посылает деньги, а другой (пользователь PN_FR2) только получает их; 2) они соединены друг с другом через конечное множество пользователей (рисунок 4). Следовательно, можно сделать вывод, что PN_FR1 и PN_FR2 могут быть потенциальными мошенниками, а подписчики, связанные с ними, — мулы.

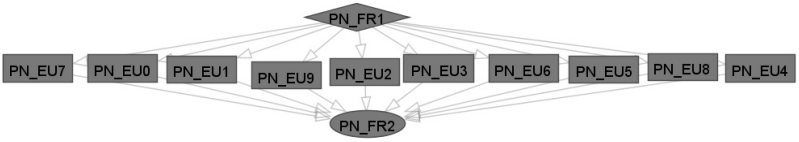

Рис. 4. Структура пользователей-мулов в исследуемом сценарии по отмыванию денег

7. Выявление поведенческих финансовых мошенничеств. Под поведенческим мошенничеством понимаются сценарии незаконной финансовой деятельности, в которых действия мошенника накладываются на легитимные операции обычного пользователя. Примерами такого типа финансовых нарушений являются кража мобильного телефона или заражение мобильного устройства вредоносным программным обеспечением. В этих случаях одно мобильное устройство используется двумя пользователями (легитимным и злоумышленником) одновременно.

Используемые тестовые данные содержали два сценария поведенческого мошенничества. В первом сценарии моделировалось заражение мобильных устройств вредоносным кодом. После заражения вредоносная программа выполняет несколько денежных переводов пользователям-мулам, которые затем снимают деньги с мобильного кошелька в течение 72 часов после их получения. Эта схема мошенничество довольно похожа на схему по отмыванию денег, отличаются лишь суммы денежных переводов, и пользователи-мулы используются здесь для того, чтобы скрыть конечное место перевода украденных денег, а не их происхождение. Вторая схема поведенческого мошенничества соответствует краже мобильного телефона. После кражи мобильного устройства злоумышленник в течение достаточно короткого отрезка времени совершает несколько попыток снять деньги с мобильного кошелька, пытаясь успеть до того момента, как кража телефона будет обнаружена, а телефон отключен.

Очевидно, что поведенческие мошенничества характеризуются изменениями в частоте транзакций и переводимой сумме денег. По этой причине в качестве координатных узлов модели визуализации RadViz были выбраны число индивидуальных переводов, число снятий мобильных денег и пополнения мобильного кошелька, число переводов за покупки и оплата эфирного времени сотовому оператору в единицу времени. На рисунке 5 показаны результаты RadViz-визуализации пользователей СМДП. Видно, что есть группы точек фиолетового и розового цвета, обозначающие поставщиков розничных услуг (***Продавцы***) и агентов оператора мобильной связи (***Агенты***) соответственно, и лежащих обособленно в силу особенностей их роли в СМДП. Большинство конечных пользователей расположены кучно в центре единичного круга, что означает, что они достаточно равномерно используют операции, выбранные в качестве координат RadViz-визуализации. Однако есть группа, состоящая из четырех пользователей, у которых индивидуальные денежные переводы значительно преобладают над транзакциями других типов. На рисунке 5 они помечены как ***Пользователи 1***.

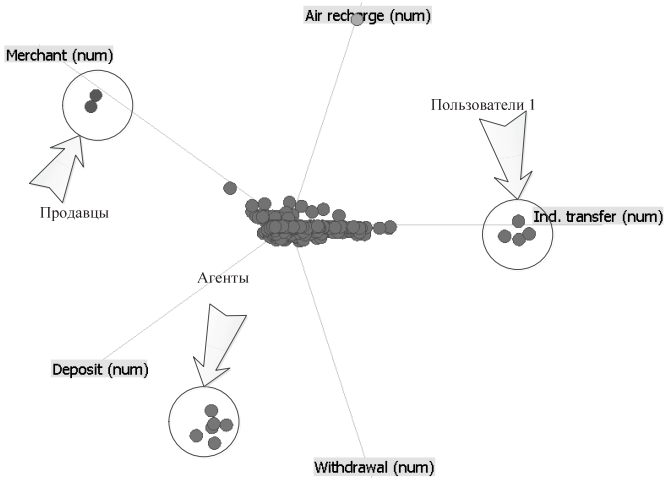

Рис. 5. RadViz-визуализация пользователей СМДП в сценарии поведенческих мошенничеств

Кроме того, анализ контактов этих пользователей выявил, что множества пользователей СМДП, отправляющие им денежные средства, пересекаются. Эти два факта позволяют сделать вывод, что выявленные четыре пользователя являются мулами, чьи учетные

записи используются для получения, а затем снятия мобильных денег с мобильного кошелька.

RadViz-визуализация пользователей СМДП оказалась полезной при выявлении мулов в схеме по отмыванию денег и сценарии заражения мобильных устройств вредоносным кодом, однако выявить случаи кражи мобильных телефонов с ее помощью оказалось невозможно.

8. Заключение. В настоящей работе авторы предложили методику визуального анализа данных, в основе которой лежит метафорическое представление поведения пользователей СМДП на основе RadViz-визуализации. Анализ применения RadViz-визуализации пользователей системы на различных тестовых данных показал, что она полезна при обнаружении мошеннических сценариев, которые предполагают использование пользователей-мулов, чье поведение существенно отличается от поведения других абонентов СМДП. Таким образом, она позволяет выявить финансовые правонарушения, которые связаны с длительными, возможно, незначительными изменениями в поведении пользователей, однако имеющих кумулятивный эффект, и поэтому могут быть раскрыты при выборе достаточно длительного периода времени. По этой причине данная модель визуализации оказалась эффективной при обнаружении мулов в схеме отмывания денег и мобильной бот-сети.

Авторы предлагают использовать данную модель графического представления данных в качестве отправной точки анализа транзакций, который поддерживается также традиционным представлением транзакций пользователя в виде графа. В работе описан сценарий использования предложенной методики визуального анализа транзакций на примере обнаружения схемы отмывания денежных средств и поведенческих мошенничеств.

Дальнейшие исследования будут связаны с реализацией методик взаимодействия, осуществляющих поиск объектов по заданному шаблону, а также проработкой вопросов масштабирования предложенных методик с учетом больших объемов данных.

Литература

1. Mobile Payment System. URL: http://www.vodafone.com/content/index/about/about-us/money_transfer.html (дата обращения 22.05.2016).
2. Infographic: Tanzania's Mobile Money Revolution. URL: http://www.cgap.org/data/infographic-tanzanias-mobile-money-revolution (дата обращения 22.05.2016).
3. *Ankerst M., Berchtold S., Keim D.A.* Similarity Clustering of Dimensions for an Enhanced Visualization of Multidimensional Data // Proc. of 1998 IEEE Symposium on Information Visualization (INFOVIS '98). IEEE Computer Society. 1998. pp. 52–60.

4. *Keim D., Andrienko G., Fekete J.-D., Goerg C., Kohlhammer J., Melancon G.* Visual Analytics: Definition, Process, and Challenges // Information Visualisation. Springer-Verlag, Berlin Heidelberg. 2008. vol. 4950. pp.154–175.
5. *Kotenko I., Novikova E.* VisSecAnalyzer: a Visual Analytics Tool for Network Security Assessment // Proc. of the 3rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013). Springer. Heidelberg. 2013. vol. 8128. pp. 345–360.
6. *Novikova E., Kotenko I.* Analytical Visualization Techniques for Security Information and Event Management // Proc. of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). 2013. pp. 519–525.
7. *Novikova E., Kotenko I.* Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services // Lecture Notes in Computer Science. Berlin. Heidelberg: Springer-Verlag. 2014. vol. 8708. pp. 63–78.
8. *Котенко И.В., Новикова Е.С.* Визуальный анализ защищенности компьютерных сетей // Информационно-управляющие системы. Санкт-Петербург. 2013. № 3. С. 56–61.
9. *Котенко И.В., Новикова Е.С.* Методики визуального анализа в системах управления информационной безопасностью компьютерных сетей // Вопросы защиты информации. Москва. 2013. № 3. С. 33–42.
10. *Новикова Е.С., Котенко И.В.* Анализ механизмов визуализации для обеспечения защиты информации в компьютерных сетях // Труды СПИИРАН. 2012. № 4(23). С. 7–30.
11. Financial Crime Risk Management solution. URL: http://www.fiserv.com/risk-compliance/financial-crime-risk-management.htm (дата обращения 22.05.2016).
12. Nice Actimize Integrated Fraud Management. http://www.niceactimize.com/index.aspx?page=solutionsfraud (дата обращения 22.05.2016).
13. SAS Fraud detection solutions. URL: http://www.sas.com/offices/europe/uk/industries/banking/fraud-detection.html (дата обращения 22.05.2016).
14. Delloite. Visual Analytics: Revealing Corruption, Fraud, Waste, and Abuse. Presentation of the Forensic Center. URL: http://www.slideshare.net/DeloitteForensicCenter/visual-analytics-revealing-corruption-fraud-waste-and-abuse-13958016 (дата обращения 22.05.2016).
15. *Westphal C.R.* Patterns for Financial Intelligence Units (FIUs) and Anti-Money Laundering (AML) Operations. URL: http://support.visualanalytics.com/technicalArticles/whitePaper/pdf/VAI%20AML%20FIU%20Patterns%20Presentation.pdf (дата обращения 22.05.2016).
16. *Xie C., Chen W., Huang X., Hu Y., Barlowe S., Yang J.* VAET: A Visual Analytics Approach for E-Transactions Time-Series // IEEE Transactions Visualization and Computer Graphics. 2014. vol. 20(12). pp. 1743–1752.
17. *Chang R. et. al*: Visualization of Categorical, Time-Varying Data From Financial Transactions // Proc. of IEEE Symposium on Visual Analytics Science and Technology (VAST 2007). 2007. pp. 155–162.
18. *Gaber C., Hemery B., Achemlal M., Pasquet M., Urien P.* Synthetic logs generator for fraud detection in mobile transfer services // Proc. of Int. Conference on Collaboration Technologies and Systems (CTS 2013). 2013. pp.174–179.
19. *Di Caro L., Frias-Martinez V., Frias-Martinez E.* Analyzing the Role of Dimension Arrangement for Data Visualization in Radviz // Proc. of Advances in Knowledge Discovery and Data Mining. 2010. LNCS 6119. pp. 125–132.
20. ColorBrew2. URL: http://colorbrewer2.org. (дата обращения 22.05.2016).

21. *Shneiderman B.* Dynamic queries for visual information seeking // The Craft of Information Visualization: Readings and Reflections. Morgan Kaufman Publishers. 2003. pp. 14–21.
22. Prefuse Information Visualization toolkit. URL: http://prefuse.org/ (дата обращения 22.05.2016).
23. Money Laundering using New Payment Methods. URL: http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneyla (дата обращения 22.05.2016).

Новикова Евгения Сергеевна — к-т техн. наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: визуальная аналитика, вредоносное программное обеспечение, двухключевая криптография. Число научных публикаций — 45. evgeshka19@mail.ru, http://www.comsec.spb.ru/en/staff/novikova; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328–2642.

Котенко Игорь Витальевич — д-р техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — 450. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328–2642, Факс: +7(812)328–4450.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

E.S. Novikova, I.V.Kotenko

DETECTION OF ANOMALOUS ACTIVITY IN MOBILE MONEY TRANSFER SERVICES USING RADVIZ-VISUALIZATION

Novikova E.S., Kotenko I.V. **Detection of Anomalous Activity in Mobile Money Transfer Services Using RadViz-Visualization.**

Abstract. Nowadays, mobile communication networks represent a key enabling infrastructure for financial service provision, since they offer significant opportunities for increasing the efficiency and pervasiveness of such services by expanding access and lowering transaction costs. In the paper, the authors analyze the use case of mobile money transfer services which are managed by a mobile network operator who not only provides infrastructure to financial services but also emits mobile money.

In this paper, we present an interactive multi-view visualization approach that provides a better insight in the large data sets describing MMTS activity. It is based on a RadViz-related visualization of the MMTS users that helps to determine groups of similarities and outliers among them and is characterized by low computational complexity. To the best of knowledge of the authors, this work is the first to exploit the RadViz-visualization technique to visualize MMTS subscribers. RadViz –based presentation of the MMTS users is supported by interactive graph based visualization of their contacts. The graph of the users' contacts is often used to analyze financial transactions as it allows discovering structural peculiarities such as bridges and cliques.

The proposed visual analytics technique was evaluated on different test data sets containing different fraudulent financial scenarios. Summarizing the results of the efficiency evaluation of the proposed visualization technique for MMTS transaction activity, we can say 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 also allows detecting frauds associated with shifts in user behavior which have cumulative character. Thus these frauds can be revealed when choosing a relatively long period of time (e.g. a month) to explore MMTS transactions. That is why this technique was effective when detecting mules in the money laundering scheme and the mobile botnet.

Novikova Evgenia Sergeevna — Ph.D., senior researcher of the computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: security visual analytics, malware, public key cryptography. The number of publications — 45. evgeshka19@mail.ru, http://www.comsec.spb.ru/en/staff/novikova; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328–2642.

Kotenko Igor Vitalievich — Ph.D., Dr. Sci., professor, head of computer security problems Laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism. The number of publications — 450. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328–2642, Fax: +7(812)328–4450.

Acknowledgements. This research is supported by RFBR (projects No. 14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482), in part by the budget (projects No. 0073-2015-0004 and 0073-2015-0007) and by the grant of RSF 15-11-30029 in SPIIRAS.

References

1. Mobile Payment System. Available at: http://www.vodafone.com/content/index/about/about-us/money_transfer.html (accessed 22.05.2016).
2. Infographic: Tanzania's Mobile Money Revolution. Available at: http://www.cgap.org/data/infographic-tanzanias-mobile-money-revolution (accessed 22.05.2016).
3. Ankerst M., Berchtold S., Keim D.A. Similarity Clustering of Dimensions for an Enhanced Visualization of Multidimensional Data // Proceedings of 1998 IEEE Symposium on Information Visualization (INFOVIS '98). IEEE Computer Society. 1998. pp. 52–60.
4. Keim D., Andrienko G., Fekete J.-D., Goerg, C., Kohlhammer, J., Melancon, G. Visual Analytics: Definition, Process, and Challenges. *Information Visualisation*. Springer-Verlag, Berlin Heidelberg. 2008. vol. 4950. pp. 154–175.
5. Kotenko I., Novikova E. VisSecAnalyzer: a Visual Analytics Tool for Network Security Assessment. Proceedings of the 3rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013). Springer. Heidelberg. 2013. vol. 8128. pp. 345–360.
6. Novikova, E., Kotenko, I. 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). 2013. pp. 519–525.
7. Novikova E., Kotenko I. Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services. Proceedings of the 4th IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2014). Springer. Heidelberg: Springer-Verlag. 2014. vol. 8708. pp. 63–78.
8. Kotenko I.V., Novikova E.S. [Visual analysis of the security of computer networks]. *Informacionno-upravljajushhie sistemy – Information and Control Systems*. 2013. vol. 3. pp. 56–61. (In Russ.).
9. Kotenko I.V., Novikova E.S. [Methods of visual analysis in control systems for information security of computer networks]. *Voprosy zashhity informacii – Information security issues.* 2013. vol. 3. pp. 33–42. (In Russ.).
10. Novikova E.S., Kotenko I.V. [Analysis of the Visualization Techniques used for Information Security in the Computer Networks]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2012. vol. 4(23). pp.7–30. (In Russ.).
11. Financial Crime Risk Management solution. Available at: http://www.fiserv.com/risk-compliance/financial-crime-risk-management.htm (accessed 22.05.2016).
12. Nice Actimize Integrated Fraud Management. Available at: http://www.niceactimize.com/index.aspx?page=solutionsfraud (accessed 22.05.2016).
13. SAS Fraud detection solutions. Available at: http://www.sas.com/offices/europe/uk/industries/banking/fraud-detection.html (accessed 22.05.2016).
14. Delloite. Visual Analytics: Revealing Corruption, Fraud, Waste, and Abuse. Presentation of the Forensic Center. Available at: http://www.slideshare.net/DeloitteForensicCenter/visual-analytics-revealing-corruption-fraud-waste-and-abuse-13958016 (accessed 22.05.2016).
15. Westphal C.R. Patterns for Financial Intelligence Units (FIUs) and Anti-Money Laundering (AML) Operations Available at: http://support.visualanalytics.com/

technicalArticles/whitePaper/pdf/VAI%20AML%20FIU%20Patterns%20Presentation.pdf (accessed 22.05.2016).
16. Xie C., Chen W., Huang X., Hu Y., Barlowe S., Yang J. VAET: A Visual Analytics Approach for E-Transactions Time-Series. *IEEE Transactions Visualization and Computer Graphics*. 2014. vol. 20(12). pp. 1743–1752.
17. Chang R. et. al. Visualization of Categorical, Time-Varying Data From Financial Transactions. Proceedings of IEEE Symposium on Visual Analytics Science and Technology (VAST 2007). 2007. pp. 155–162.
18. Gaber C., Hemery B., Achemlal M., Pasquet M., Urien P. Synthetic logs generator for fraud detection in mobile transfer services. Proceedings of Int. Conference on Collaboration Technologies and Systems (CTS 2013). 2013. pp.174–179.
19. Di Caro L., Frias-Martinez V., Frias-Martinez E. Analyzing the Role of Dimension Arrangement for Data Visualization in Radviz. Proceedings of Advances in Knowledge Discovery and Data Mining. 2010. LNCS 6119. pp. 125–132.
20. ColorBrew2. Available at: http://colorbrewer2.org. (accessed 22.05.2016).
21. Shneiderman B. Dynamic queries for visual information seeking. *The Craft of Information Visualization: Readings and Reflections*. Morgan Kaufman Publishers. 2003. pp. 14–21.
22. Prefuse Information Visualization toolkit. Available at: http://prefuse.org/ (accessed 22.05.2016).
23. Money Laundering using New Payment Methods. Available at: http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneyla (accessed 22.05.2016).