АВТОМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА. – 2014. – No.3. – С.40-51.

ОБ АНАЛИЗЕ СТАТИСТИКИ МОБИЛЬНЫХ ПОСЕТИТЕЛЕЙ

Д. НАМИОТ, *кандидат физико-математических наук*
Факультет Вычислительной Математики и Кибернетики МГУ им. М.В. Ломоносова
Ленинские горы, 119991 Москва, Россия
E-mail: dnamiot@gmail.com

М. ШНЕПС-ШНЕППЕ, *доктор технических наук, профессор*
Институт математики и информатики Латвийского Университета
бульв. Райня 29, LV-1459 Рига, Латвия
E-mail: manfreds.sneps@gmail.com

Тема статьи относится к услугам мобильной сети, связанным с местоположением. Рассматривается задача подсчета мобильных пользователей (мобильных телефонов) в некоторой выделенной области. Для подсчета используется информация, доступная из анализа беспроводных протоколов (Wi-Fi, Bluetooth). Цель исследования состоит в построении аналога систем веб-статистики, оперирующих с реальными мобильными абонентами (вместо данных о посещении веб-страниц, как в веб-статистике). В результате получаем информацию о посещаемости, определение и анализ трендов в пользовательском трафике, поиск ядра постоянных посетителей и раскрытие его динамики. В статье приведены алгоритмы вычисления сетевой близости, примеры использования.

Ключевые слова: Wi-Fi, *probe request*, местоположение, статистика, сетевая близость, облачные сообщения

1. ВВЕДЕНИЕ

В статье рассматриваются услуги мобильной сети, связанные с местоположением (*Location-based service*, LBS). Но в отличие от традиционного подхода к определению местоположения мобильного телефона пользователя по гео-информации, мы определяем местоположение посредством анализа близости мобильного абонента к определенным сетевым узлам (например, к точкам доступа Wi-Fi). Мобильный телефон рассматривается как сенсор близости и гео-позиционная информация заменяется данными о сетевой близости (*network proximity*) [1].

Известны способы определения местоположения в помещениях, которые не обязательно привязаны к определению истинного географического положения [2], а используют, например, данные о расположении точек доступа Wi-Fi. То есть мобильные операционные системы могут использовать информацию об объектах сетевой инфраструктуры для уточнения (или даже определения) истинного положения абонента. Анализируя силу сигнала и видимость точек доступа, строятся различные метрики о местоположении мобильных посетителей.

Основной слабостью существующих методов является требование наличия заранее подготовленной радио-карты сетевой инфраструктуры. Подготовка радио-карты занимает достаточно много времени, а условия распространения сигнала могут постоянно меняться. Например, расстановка мебели (аппаратуры) в помещениях может существенно поменять картину распространения. Поэтому мы рассматриваем автоматическое определение местоположения, и готовы мириться с более низкой точностью такого определения. Мы говорим о локальной области, ограниченной видимостью (доступностью) некоторого узла беспроводной сети (узла Wi-Fi или *Bluetooth*).

Если появляется возможность автоматически определять местоположение мобильных абонентов, то этот же функционал можно использовать и для сбора статистики. Здесь имеется в виду не статистика посещения каких-то выделенных объектов, а их совокупности. Подобного рода отметки о посещении (традиционно известные как *check-in* [3, 4]) всегда требуют явной активности со стороны пользователя (абонента). Поэтому статистика посещений будет не полной, смещенной по социальным группам: это в основном активные пользователи соответствующих приложений (*Foursquare, Facebook, Twitter* и т.д.). Мы рассматриваем пассивный сбор статистики, что не предполагает специальной активности от мобильного абонента, тем самым является более представительным. Этот способ имеет аналогию с веб-статистикой [5], т.е. со сбором данных о посещении веб-приложений. Посещение веб-страницы регистрируется скриптом (программой), который связан с данной страницей (т.е. установлен на ней), и, естественно, не требует никаких отдельных действий со стороны посетителя.

Применение подобного рода систем достаточно очевидно. В первую очередь, это различные приложения для торговли (*retail*), которые подсчитывают статистику помещений, различные прикладные решения для умного города (*Smart City*). Вместе с тем, применение пассивного мониторинга имеет свои особенности, которые и служат предметом рассмотрения данной статьи.

Далее подробно рассмотрены основы пассивного мониторинга мобильных посетителей (в разделе 2), измерители (метрики) сетевой близости (в разделе 3), примеры приложений и особенности измерений сетевой близости (в разделах 4 и 5). Раздел 6 описывает дополнительные сервисы, которые можно построить на базе сетевой близости и облачных сообщений.

2. ОСНОВЫ ПАССИВНОГО МОНИТОРИНГА

Основой пассивного Wi-Fi мониторинга являются так называемые *Probe Requests*, описанные в спецификации Wi-Fi [6]. Это широковещательная рассылка, которую осуществляют Wi-Fi клиенты. Согласно спецификации, одна станция (сетевой узел) может посылать такой запрос при необходимости получения информации от другой станции (сетевого узла). Например, Wi-Fi клиент посылает такой запрос, чтобы определить, какие точки доступа существуют поблизости. Информационные потоки Wi-Fi запроса показаны на рисунке 1.

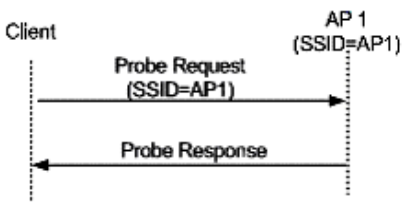

Рис.1. Запрос Wi-Fi *Probe Request*.

Очевидным достоинством является то, что информация о местоположении неявно присутствует в такой схеме просто по определению. Само распространение сигнала ограничено возможностями протокола 802.11. Другим преимуществом является то, что Wi-Fi клиент посылает такой запрос, даже будучи не присоединенным к какой-либо точке доступа. Применительно к мобильным телефонам это означает, что достаточно просто включить Wi-Fi на телефоне [7]. Дополнительным преимуществом является также то, что в такой схеме не происходит точного раскрытия местоположения клиента. Оно просто не требуется. Достаточно того факта, что клиент находится где-то в зоне распространения Wi-Fi сигнала. Это дополнительный аргумент в защиту приватности (*privacy*).

Технически, сетевые пакеты, рассматриваемые в данном подходе, могут содержать следующие данные [8]:

- Исходный адрес (MAC-*address*)
- SSID (идентификация точки доступа)
- Поддерживаемые характеристики обмена (скорости, например)
- Дополнительные данные силу сигнала RSSI и др.
- Расширенные характеристики
- Информация, добавленная конкретным производителем

Чтение и анализ (разбор) такого рода пакетов и есть основа для статистики. Каждый новый принятый пакет – это аналог того, что в веб-статистике скрывается под словом хит (запрос веб-страницы). MAC-адрес позволяет идентифицировать (точнее – различать) абоненты. Соответственно, последовательные запросы от одного и того же MAC-адреса позволяют говорить о сессии. В данном случае – это некоторое продолжительное пребывание абонента (мобильного пользователя) в анализируемой области.

Технически, чтение пакетов можно произвести с помощью какого-либо выделенного устройства, Wi-Fi маршрутизатора или даже с помощью произвольной сетевой карты с поддержкой Wi-Fi, если только в ней присутствует режим анализа широковещательных рассылок. Отметим, между прочим, что поиск *Bluetooth* узлов может происходить по аналогичной схеме. Значимое с практической точки зрения отличие – это скорость работы: поиск Wi-Fi узлов работает в несколько раз быстрее.

Как указано выше, уникальным атрибутом в каждом запросе является MAC-адрес. Помимо идентификации собственно мобильного устройства, он может предоставлять еще и информацию о производителе. Первые три октета адреса (24 бита) известны как "*Organizationally Unique Identifier*" (OUI) [9]. Список назначенных OUI ведется на международном уровне в IEEE. Это позволяет определить производителя устройства (*User-Agent* в терминах веб-статистики). Говоря о приватности, отметим, что MAC-адрес в задачах пассивного мониторинга используется только для последующей реидентификации клиента. Следовательно, его точное значение несущественно, и мы можем легко заменить его подходящим хэш-кодом. Таким образом, хранение точных MAC-адресов посетителей в системе сбора статистики является необязательным.

Из дополнительной информации, присутствующей в пакете, можно отметить RSSI (силу сигнала). Этот параметр может быть использован в описанных ниже метриках близости.

Обсуждение. Основной проблемой, связанной с пассивным Wi-Fi мониторингом, является отсутствие 100% надежности. Иными словами, нет гарантии, что мобильное устройство (даже с включенным Wi-Fi интерфейсом) вообще будет транслировать запросы *Probe Request*. Устройства (более точно – мобильные операционные системы и их разные версии) ведут себя по-разному

в плане отправки специальных пакетов. По нашим экспериментам, например, iOS устройства отправляют их в среднем чаще, чем *Android*, планшеты с *Android* – чаще, чем телефоны. Впрочем, эта картина может поменяться с обновлением версий операционных систем. Наши собственные статистические эксперименты показали, что описанным выше способом в среднем, определяется примерно 70% из присутствующих мобильных устройств [10]. Эти данные подтверждаются и другими авторами [11]. Во всех экспериментах мы отмечали, что мобильное устройство (это было справедливо и для iOS, и для *Android*) всегда посылает *Probe Request* непосредственно после включения (при включении), если Wi-Fi интерфейсы включены по умолчанию. Процент детектирования возрастает, если присутствует активная точка доступа Wi-Fi. Но в любом случае процент обнаружения был меньше 100. Этот факт следует учитывать при оценке данных о сетевой близости. Проводя параллели с веб-статистикой, можно сказать, что мы сталкиваемся с потерей измерений. Но для веб-статистики такая потеря (при правильном выборе методов регистрации) всегда связана с какими-либо техническими неисправностями (проблемами) реализации. Здесь же эта "потеря" измерений является органической частью процесса.

3. КАК ИЗМЕРИТЬ СЕТЕВУЮ БЛИЗОСТЬ

При наличии нескольких измерительных устройств, которые регистрируют служебные пакеты, открывается новый интересный класс задач. Несколько устройств (при условии, естественно, что база измерений будет единой) дадут возможность отслеживать путь мобильного абонента внутри контролируемой области. Аналог из веб-статистики – переходы по страницам сайта. Вместе с возможностью отслеживать "сессии" (время пребывания) это дает возможность представлять популярные и легко понятные визуальные решения карты плотности посетителей (типа *heat-maps*) [12], пример которых представлен на рис.2. Несколько регистрирующих устройств дают возможность воспользоваться метриками, которые позволяют оценивать взаимное положение абонентов.

Рис.2. Пример *heat map* для мобильного трафика [13].

Радио-сигнатура. Формальное определение для оценки местоположения мобильных абонентов, основанное на сетевой близости, приводится во многих статьях. Например, простейший подход, описанный в работе [14]. Метрика близости основана на подсчете количества раз, которое конкретное устройство видело определенную точку доступа [15]. Мобильное приложение на телефоне периодически записывает адреса видимых точек доступа Wi-Fi. Радио-сигнатура (так называемый Wi-Fi *fingerprint*) определяется на основе подсчета процента времени (доли временных интервалов), в течение которых конкретный MAC-адрес присутствовал во всех записях. Со-

вокупность (вектор) таких долей и есть то, что называется Wi-Fi *fingerprint*. Она (сигнатура) вычисляется для каждого интересующего нас места. Эта сигнатура используется для сравнения позиций мобильных абонентов.

Сравнение двух сигнатур f_1 и f_2 выполняется следующим образом. Пусть M есть объединение MAC-адресов в f_1 и f_2. Для MAC-адреса $m \in M$ обозначим его доли вхождения как $f_1(m)$, так и $f_2(m)$. Тогда схожесть S сигнатур f_1 и f_2 может быть вычислена следующим образом:

$$S = \sum_{m \in M} (f_1(m) + f_2(m)) * \text{Min Max}(m),$$

где MinMax(I) = $\min(f_1(m), f_2(m)) / \max(f_1(m), f_2(m))$.

Понятно, что значение S будет возрастать, если в сравниваемых сигнатурах присутствует больше одинаковых адресов. Отметим, что для пассивного мониторинга ситуация с измерениями может быть обращена – не мобильное устройство видит точку доступа Wi-Fi, а регистратор "видит" мобильный телефон.

Ранговая корреляция измерений. Использование радио-сигнатур базируется на предположении, что Wi-Fi устройство всегда измеряет сигнал одинаково. Очевидно, что это является жестким предположением. В реальных условиях заряд батареи, например, не будет одинаковым, и одно и то же устройство может выдавать разные значения в зависимости от заряда батареи, ориентации и т.д. Поэтому в сравнениях вместо абсолютного значения силы сигнала используют ранжирование. То есть, сравнивают списки точек доступа, отсортированные по силе сигнала. Например, если получили три точки доступа с соответствующими значениями RSSI (SS_A; SS_B; SS_C) = (-50; -20; -40), то мы можем заменить абсолютные значения рангом (R_A; R_B; R_C) = (3; 1; 2) [16]; а сравнивать ранги можно с помощью коэффициента ранговой корреляции Спирмена (*Spearman rank-order correlation coefficient*) [17].

Корреляция абсолютных значений. Для анализа абсолютных значений RSSI в пространстве сигналов можно ввести Евклидово расстояние или вычислять коэффициент *Tanimoto* [18]. В обоих случая расчеты начинаются с вычисления средних значений сигнала. Для каждой точки доступа по измеренным векторам сигналов S_x вычисляется вектор средних значений S'_x. В случае Евклидова расстояния используется попарное сравнение векторов S'_a и S'_b, где один из них представляет некоторый недостижимый эталон с уровнями сигналов, например, равным -100 dBm, и вычисляем значение расстояния

$$d_{a,b} = \| S'_a - S'_b \|.$$

Для вычислений на основе коэффициента *Tanimoto* расстояние подсчитывается следующим образом [18]:

$$d_{a,b} = 1 - (S'_a \cdot S'_b) / (\| S'_a \|^2 + \| S'_b \|^2 - S'_a \cdot S'_b).$$

В обоих случаях расстояние между векторами увеличивается при расхождении абсолютных значений векторов.

4. ПРИМЕРЫ ПРИЛОЖЕНИЙ

Как известно, подавляющую долю времени (около 90%) люди проводят в помещениях. Поэтому изобретено множество систем пассивного мониторинга

Navizon. К числу подобных систем сбора статистики для мобильных абонентов относятся, например, *Navizon Indoor Triangulation System* (*Navizon* ITS) [19]. Ее работу демонстрирует рис.3. В качестве WiFi stations выступают смартфоны и другие устройства с WiFi интерфейсом. Узлы (*Nodes*) следят за этими устройствами. Сетевой шлюз (*Gateway*) имеет выход в Интернет. Каждый узел охватывает территорию в 15–50 метров, поэтому для больших площадей часть узлов должна вы-полнять роль повторителей (*repeaters*).

GiSi Indoors. Система мониторинга компании *GiSi Indoors* [20] находит применение в торговых и развлекательных центрах, больницах и т.д. На рис.4 приведен пример карты скопления посетителей (*heat map*), которая построена системой *GiSi Indoors*.

Cisco. Еще один пример – *Cisco Mobility Service Engine* [21]. Рис.5 иллюстрирует отчет о распределении посетителей по времени в течение дня.

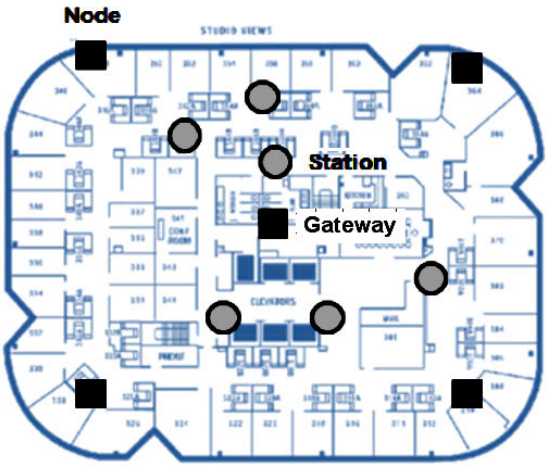

Рис.3. Navizon I.T.S.

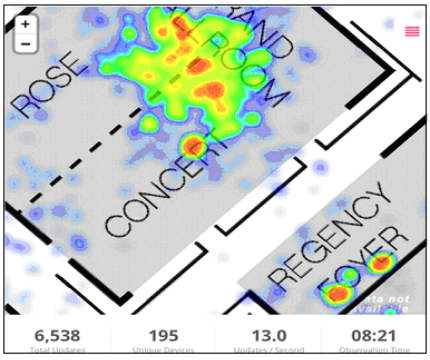

Рис.4. Пример Heat Map.

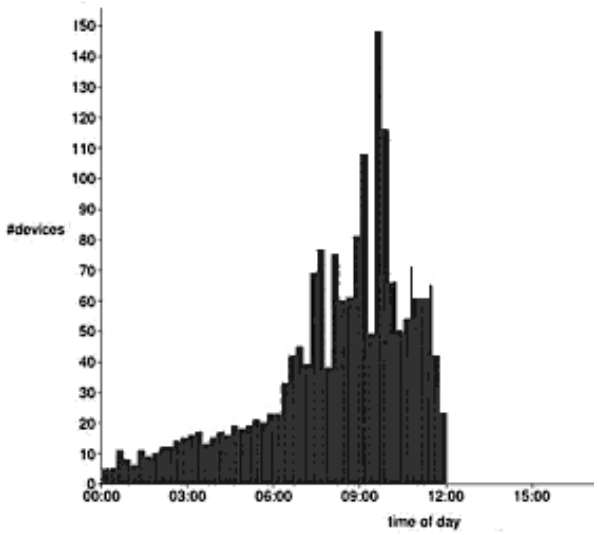

Рис.5. Гистограмма посетителей *Time of Day Distribution*.

В этой же области работают, например, *Aruba Networks, iInside, Euclid, RetailNext*. Традиционной областью применения является торговля, так называемый *proximity marketing*. Эта область является наиболее перспективной с точки зрения монетизации сервисов.

Услуга SpotEx. Как показано в проектах типа *SpotEx* [22], вопросы, связанные с доставкой локальной информации мобильным абонентам, могут быть решены на основе сетевой близости (*network proximity*) без непосредственного обращения к гео-позиционным данным. В наших собственных разработках мы использовали регистрирующее устройство от компании *Libelium* [23]. Основное ее достоинство – открытость. Измерения могут накапливаться, например, во внешней базе данных MySQL и, следовательно, открыты для сторонних разработчиков. Другим достоинством системы является то, что измерительное устройство технически представляет собой еще и обычный Wi-Fi маршрутизатор. Этот маршрутизатор может определять и присутствие *Bluetooth* устройств (рис.6).

Рис.6. Обнаружение смартфонов шлюзом *Libelium*.

5. ОСОБЕННОСТИ ИЗМЕРЕНИЙ СЕТЕВОЙ БЛИЗОСТИ

Остановимся подробнее на аналогии между пассивным мониторингом и сбором веб-статистики. Параллели с веб-статистикой являются наиболее очевидными. Укажем, например, систему *Google Analytics* для реальных посетителей. Но нельзя забывать, что в обоих случаях нельзя получить полного охвата посетителей. Пропущенные посетители будут не только по причине отсутствия включенного телефона, но и потому, что запрос *Probe Request* просто не всегда отправляется. Поэтому более точной аналогией может служить сравнение с дополнением к браузеру, типа *Alexa toolbar*. Такое расширение в браузерах позволяет собирать статистику о сайтах, которые посещают пользователи, установившие *Alexa toolbar*. Поскольку заведомо известно, что они не установлены у всех пользователей, то собираемая ими статистика не является полной статистикой посещаемости сайта. Мы можем говорить только о статистике посещаемости среди пользователей того или иного расширения. Точно так же выглядит и картина с пассивным мониторингом.

Отсюда следуют два важных замечания. Во-первых, такого рода пассивная статистика будет интересна для пользователей только в случае некоторой значимой общей посещаемости. В любом случае наш статистический анализ будет оперировать только с частью этой величины, и она, естественно, должна быть достаточно значимой.

Во-вторых, это означает, что основным применением подобного рода статистики будет сравнительный анализ. Мы не можем достоверно предсказать, какой процент из реальных посетителей будет определен. Следовательно, абсолютные цифры являются, по определению, не точными. Но предположение о том, что доля распознанных смартфонов примерно одинакова на всем временном интервале, выглядит весьма обоснованным. Именно это и позволяет сравнивать данные за разные дни. Кстати, статистика типа *Alexa toolbar* именно так и используется – для сравнения посещаемости различных сайтов, а не для подсчета абсолютных значений.

Следовательно, основная цель мониторинга заключается в сравнении временных рядов. Например, типичным вопросом веб-статистики является – какова оценка количества постоянных посетителей сайта (например, сколько пользователей заходят на сайт постоянно в течение недели и т.д.). Применительно к мобильной статистике, можно спросить, как изменилось число постоянных посетителей для контролируемой (замеряемой) области за последние 7 дней, по сравнению с такой же неделей один месяц назад.

Повторяющиеся регистрации пользователей (MAC-адресов) будут являться аналогом веб-сессии. Следовательно, можно задаваться вопросом о том, как долго посетители остаются в данной области, как часто они возвращаются и т.д.

На некоторые вопросы, связанные с поведением пользователей можно ответить и без сравнения. Например, чтобы определить посетителя, который за последнюю неделю был чаще, чем в среднем все остальные и т.д.

С пользовательской точки зрения, конечное применение – это, например, анализ результатов воздействия каких-либо внешних событий на посещаемость. Целью будет являться, например, подтверждение (опровержение) статистически значимой разницы в посещаемости. Другим интересным вопросом, с практической точки зрения, будет определение (выявление) “необычных” (не наблюдавшихся в предыдущих измерениях) шаблонов поведения. Например, повышение частоты регистрации выше определенного уровня.

6. ДОПОЛНИТЕЛЬНЫЕ СЕРВИСЫ НА БАЗЕ СЕТЕВОЙ БЛИЗОСТИ

Статистика пассивного мониторинга может и не ограничиваться традиционной регистрацией посещений (хитов в терминах веб-статистики). В этой связи мы можем упомянуть работы по

анализу траекторий движения (перемещения) мобильных абонентов, где информация о позиционировании заменяется данными о сетевой близости [24]. Сбор данных о сетевых устройствах в процессе перемещения мобильного абонента может осуществляться как на его собственном телефоне [25], так и с помощью системы пассивного мониторинга [26, 27]. В указанных работах рассматривались вопросы определения именно согласованного движения (для этого вводится понятие конвоя), поскольку прикладным выходом были все те же приложения для *proximity marketing*.

Другим полезным дополнительным сервисом могут быть локальные сообщения [28]. Идея состоит в построении типичного *мэшапа*, то есть совместного использования двух сервисов: пассивного мониторинга и облачных сообщений от мобильных операционных систем. Облачные сообщения – это способ доставки сообщений мобильным приложениям, не абонентам, как в операторских сервисах типа SMS или MMS, а мобильным приложениям [29].

Например, система облачных сообщений *Google* (*Google Cloud Messaging*, GCM) позволяет организовать рассылку данных от сервера к пользователям устройств с операционной системой *Android*. Сообщения представляют собой данные объемом до 4 Kb, отправляемые сервером при наступлении определенного типа событий. GCM управляет возникающими при отправке очередями сообщений, а также доставкой сообщений до целевого приложения [30]. Это проиллюстрировано на рис.7.

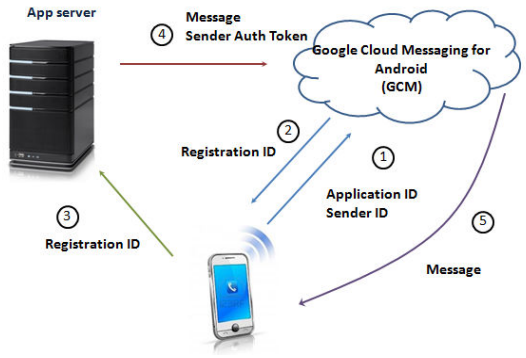

Рис.7. Схема услуги GCM.

По аналогичной схеме устроены подобные сервисы *Apple* и *Microsoft*. Приложение подписывается на получение сообщений, создается уникальный идентификатор, который и используется для отправки сообщения конкретному адресату (конкретной инсталляции приложения, то есть на конкретный мобильный телефон). Важно, что после начальной регистрации приложение вовсе не обязательно должно быть запущенным, чтобы получать уведомления. Именно последняя опция и делает систему удобной для использования в приложениях распродаж (ритейла). После начальной регистрации мобильный абонент (покупатель) не обязан запускать приложение при каждом походе в магазин.

Идея *мэшапа* состоит в том, что при стандартной подписке вместе с сознанным уникальным идентификатором подписчика будет запоминаться еще и его MAC-адрес (или его *хеш*-код). А далее, в процессе эксплуатации, сохраненный адрес (*хеш*-код) будет сравниваться с базой адресов (*хеш*-кодов), собранной системой пассивного мониторинга. Это позволит отправлять сообщения не просто подписчикам, а только тем из них, кто именно в данный момент находится в интересующей нас области [31].

7. СТАТИСТИЧЕСКИЙ АНАЛИЗ ДАННЫХ О СЕТЕВОЙ БЛИЗОСТИ

В этом разделе мы хотели бы представить возможные подходы к анализу накапливаемых данных пассивного мониторинга. Как уже отмечалось выше, простое суммирование данных о посещаемости не может дать полезных ответов в силу того, что нам неизвестно точное число пропущенных (незарегистрированных) устройств. Поэтому, основным предположением является допущение о том, что доля пропущенных устройств остается примерно одинаковой. Следовательно, основным инструментом является сравнительный анализ. Примерами таких задач являются:

– сравнение дневной посещаемости в течение текущей недели (месяца) и такой же недели (месяца) в прошлом. Целью является выявление изменения (двоичный ответ – да или нет) и направление этого изменения (растет посещаемость, падает или остается на том же уровне);

– определение движения ядра (постоянных посетителей). В качестве постоянных посетителей рассматриваются MAC-адреса, повторно регистрируемые в течение некоторого заданного времени, например, каждый день в течение одной недели. В силу вышесказанного о ценности абсолютных значений, интерес опять-таки представляет именно сравнительный анализ. А именно, подтверждение растущего (падающего, стабильного) тренда для ядра.

В таком случае пассивный анализ данных о посещаемости будет использоваться (с практической точки зрения), в первую очередь, для подтверждения (отрицания) результатов различных маркетинговых акций. Например, для ответа на вопросы о том, как изменилась посещаемость после рекламной компании, введения программы лояльности и т.п. Нам представляется, что ниша для подобного рода продуктов практически пуста, и это является весьма перспективным направлением исследований.

Вместе с тем, необходимо отметить некоторые направления исследований, которые используют информацию, специфичную именно для мобильного мониторинга. Например, если проводить параллели с веб-статистикой, в данных мобильного мониторинга отсутствует поле *Referer*, которое может указывать на то, откуда пришел запрос (посетитель на сайт). Но при этом присутствует поле SSID, которое описывает Wi-Fi сеть, к которой данный пользователь был когда-то присоединен в прошлом. Это позволяет проводить анализ по выявлению связей между мобильными пользователями. Можно исходить из предположения, что если мы постоянно видим повторяющиеся сети у разных мобильных пользователей, то они как-то связаны между собой. Это рассматривается в работе [32].

Другая возможность выявления связей между мобильными абонентами рассматривается в работе [33]. Это выделение групп пользователей, на основе анализа времени регистрации. Идея состоит в построении специальной формы кластеризации, которая позволяет эмпирически сгруппировать визиты мобильных посетителей в течение дня, а затем проверить повторяемость найденных групп на каком-то промежутке времени (например, 7 или 30 дней). Это позволяет выделить устойчивые группы среди посетителей.

8. О БУДУЩЕЙ РАБОТЕ

Активность ведущих компаний мира (*Cisco*, *Google*, *Apple* и др.) на рынке средств для пассивного мониторинга мобильных посетителей подтверждает актуальность и перспективность исследований в данной области.

Проведенный в статье анализ состояния услуг и средств пассивного мониторинга выявил актуальность разработки математических методов для измерения сетевой близости, принятия решений по замерам траектории перемещения мобильных посетителей. Мы предложили возможные направления работ, первые результаты которых мы планируем изложить в следующих статьях.

Перспективной областью работ является также разработка дополнительных сервисов на базе сетевой близости и облачных сообщений. Мы предполагаем, что сервисы на основе близости (сетевой близости) получат в ближайшее время существенное ускорение за счет внедрения тегов (типа *iBeacons* от *Apple* на базе *Bluetooth Low Energy* [34]). Здесь уже будет происходить расширение модели пассивного мониторинга. Мобильное приложение будет видеть определенные теги, и эта информация может быть использована как отметка о присутствии мобильного абонента. При этом может не быть зависимости от конкретного мобильного приложения, за счет поддержки BLE на уровне мобильной операционной системы (например, iOS).

СПИСОК ЛИТЕРАТУРЫ

[1] *Namiot D. and Sneps-Sneppe M.* Proximity as a service. // Future Internet Communications (BCFIC), 2012 2nd Baltic Congress on (pp. 199-205). IEEE. DOI: 10.1109/ BCFIC.2012.6217947. (2012, April).

[2] *Namiot D. and Sneps-Sneppe M.* Geofence and Network Proximity. // Internet of Things, Smart Spaces, and Next Generation Networking, Lecture Notes in Computer Science. Volume 8121, 2013, pp. 117-127, DOI: 10.1007/978-3-642-40316-3_11.

[3] *Namiot D. and Sneps-Sneppe M.* A new approach to advertising in social networks-business-centric check-ins. // Intelligence in Next Generation Networks (ICIN), 2011. 15th International Conference on (pp. 92-96). IEEE. DOI: 10.1109/ICIN.2011.6081110. (2011, October).

[4] *Namiot D. and Sneps-Sneppe M*. Customized check-in procedures. // Smart Spaces and Next Generation Wired/Wireless Networking (pp. 160-164). Springer Berlin Heidelberg. DOI: 10.1007/978-3-642-22875-9_14. (2011).

[5] *Kim Sun K. and Jin-Wook Ro*. Indoor Location Analytics for Designing a Location-Based Product-Service System.// Functional Thinking for Value Creation. Springer Berlin Heidelberg, 2011. 183-187.

[6] *Chandra R. et al*. A Beacon-Stuffing: Wi-Fi without Associations Mobile Computing Systems and Applications, 2007. // HotMobile 2007. 8th IEEE Workshop on, pp.53-57.

[7] *Gast M.* 802.11 Wireless Networks: The Definitive Guide. O'Reilly Media, Inc., 2005.

[8] *Namiot D.* Local Area Messaging for Smartphones // International Journal of Open Information Technologies, 1(2), pp. 8-11. (2013).

[9] *Kumar U. et al*., A Comparing wireless network usage: laptop vs smart-phones. // Proceedings of the 19th annual international conference on Mobile computing & networking (pp. 243-246). ACM. (2013, September).

[10] *Namiot D. and Sneps-Sneppe M.* Local messages for smartphones. // Future Internet Communications (CFIC), 2013 Conference on, pp.1- 6, IEEE, DOI: 10.1109/CFIC.2013.6566322.

[11] *Musa A. and Eriksson J.,* Tracking Unmodified Smartphones Using Wi-Fi Monitors. // SenSys'12, November 6–9, 2012, Toronto.

[12] *Han Y. et al*. A visual analytics system for radio frequency fingerprinting-based localization. // Visual Analytics Science and Technology, 2009. VAST 2009. IEEE Symposium on (pp. 35-42). IEEE. (2009, October).

[13] *Bickersteth J. And Ainsley C.* Mobile phones and visitor tracking. // Museums and the Web 2011: Proceedings.

http://www.museumsandtheweb.com/mw2011/papers/mobile_phones_and_visitor_tracking.html.

[14] *Azizyan M. et al*. SurroundSense: mobile phone localization via ambience fingerprinting. // MobiCom '09 Proceedings of the 15th annual international conference on Mobile computing and networking, pp. 261-272, DOI: 10.1145/1614320.1614350.

[15] *Namiot D. and Sneps-Sneppe M.* Wireless Networks Sensors and Social Streams. // Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on (pp. 413-418). IEEE. DOI: 10.1109/WAINA.2013.27. (2013, March).

[16] *Chen Y. et al*. Accuracy characterization for metropolitan-scale Wi-Fi localization. // ACM MobiSys, 2005.

[17] *Stuart A*. The correlation between variate-values and ranks in samples from a continous distribution// British Journal of Statistical Psychology Vol. 7, Issue 1, pp. 37–44.

[18] *Kjaergaard M. et al*. Mobile sensing of pedestrian flocks in indoor environments using WiFi signals. // Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference on, pp. 95 – 102.

[19] Navizon ITS. http://its.navizon.com/doc/index.html Retrieved: Oct, 2013.

[20] GiSi Indoors. http://gisiindoors.com/ Retrieved Oct, 2013.

[21] Cisco MSE http://www.cisco.com/en/US/products/ps9742/index.html Retrieved: Oct 2013.

[22] *Namiot D.* Context-Aware Browsing – A Practical Approach. // Next Generation Mobile Applications, Services and Technologies (NGMAST), 2012 6th International Conference on, pp.18-23 DOI: 10.1109/NGMAST.2012.13

[23] Meshlium Xtreme http://www.libelium.com/products/meshlium Retrieved: Oct 2013.

[24] *Namiot D. and Shneps-Shneppe M.* Analysis of trajectories in mobile networks based on data about the network proximity // Automatic Control and Computer Sciences 47.3 (2013), pp.147-155, DOI: 10.3103/S014641161303005X

[25] Funf Open Sensing Framework. http://funf.media.mit.edu/ Retrieved: Sep 2013.

[26] *Namiot D.* Flock Patterns and Context// Applied Mathematical Sciences, 7(90), 4493-4497. (2013).

[27] *Namiot D. and Sneps-Sneppe M.* Discovery of Convoys in Network Proximity Log. // Internet of Things, Smart Spaces, and Next Generation Networking Lecture Notes in Computer Science Volume 8121, 2013, pp. 139-150, DOI:10.1007/978-3-642-40316-3_13.

[28] *Sneps-Sneppe M. and Namiot D.* Smart cities software: customized messages for mobile subscribers. // Wireless Access Flexibility (pp. 25-36). Springer Berlin Heidelberg. (2013).

[29] *Agarwal S.* Toward a push-scalable global internet. In Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on (pp. 786-791). IEEE. (2011, April).

[30] Google Cloud Messaging for Android http://developer.android.com/google/gcm/gs.html. Retrieved: Sep, 2013.

[31] *Sneps-Sneppe M. and Namiot D.* Spotique: A New Approach to Local Messaging. In Wired/ Wireless Internet Communication (pp. 192-203). Springer Berlin Heidelberg. DOI: 10.1007/978-3-642-38401-1_15. (2013).

[32] *D.E. Dilger*, "Inside iOS 7: iBeacons enhance apps' location awareness via Bluetooth LE," ed: Apple Insider, 2013.

Рукопись получена 18.10.2013,
финальная версия – 17.03.2014.