К читателям!

Вашему вниманию предлагается подборка статей по Интернету Вещей и Интернету Нановещей. Еще год назад в подобной подборке речь шла только об Интернете Вещей — новейшей концепции развития сетей связи. Сегодня мы с удовольствием дополняем ее Интернетом Нановещей, ибо за последний год появились не только концептуальные положения по Интернету Вещей в наномире, но и вполне конкретные результаты исследовательских работ.

Подборка начинается со статьи А. И. Парамонова «Модели потоков трафика для сетей M2M». Как известно, вещи в концепции Интернета Вещей подразделяются на вещи физического и информационного мира. Сети машина-машина M2M (Machine-to-Machine) представляют собой реализацию концепции Интернета Вещей как раз для физических вещей. Их широкомасштабное внедрение уже начинается и исследование моделей трафика в сетях M2M является актуальной научной задачей. В результате исследований выявлено замечательное свойство потоков трафика в сетях M2M — их антиперсистентный характер вследствие возможной зависимости источников трафика.

В статье П. А. Абакумова «Алгоритм выбора головного узла кластера сенсорной сети в трехмерном пространстве» представлен новый алгоритм выбора головного узла, разработанный специально для использования в трехмерном пространстве. В этой области в настоящее время в мировой литературе практически отсутствуют реальные достижения, в связи с чем работа П. А. Абакумова вызывает существенный интерес. Разработанный алгоритм превосходит известные для двумерного пространства алгоритмы при использовании их для выбора головного узла в трехмерном пространстве по доле покрытия пространства в течение длительного времени. Это дает возможность увеличить длительность жизненного цикла сенсорной сети, в течение которого сеть выполняет свои функции с заданными параметрами.

Статья П. Н. Боронина «Особенности и принципы работы биоподобных алгоритмов для самоорганизующихся беспроводных сетей связи» отличается тщательным анализом основных известных в настоящее время биоподобных алгоритмов для подобных сетей. Применение биоподобных алгоритмов в таких сложных структурах, как самоорганизующиеся сети, зачастую дает улучшение характеристик маршрутизации, а значит и большую сетевую безопасность. В качестве направления дальнейших работ в области биоподобных алгоритмов для самоорганизующихся беспроводных сетей в статье предлагается использовать полеты Леви. Это может сыграть важную роль для обеспечения сетевой безопасности, например, для всепроникающих сенсорных сетей.

В статье наших коллег из Технологического университета Тампере (Финляндия) Е. А. Кучерявого и С. Баласупрамания «Интернет Нановещей и наносети» приводятся как необходимые определения в области Интернета Нановещей и наносетей, так и результаты исследовательских работ в области бактериальных наносетей. Наносети в любом случае — это сети, функционирующие только в наномире. В статье исследуются бактериальные наносети, в которых коммутация осуществляется путем конъюгации. В существующей сетевой классификации такие бактериальные наносети можно отнести к сетям, толерантным к задержкам.

Член редколлегии журнала «Электросвязь», д.т.н., профессор А. Е. Кучерявый

УДК 621. 395

МОДЕЛИ ПОТОКОВ ТРАФИКА ДЛЯ СЕТЕЙ M2M

А. И. Парамонов, доцент кафедры «Сети связи» СПбГУТ им. проф. М. А. Бонч-Бруевича, к.т.н.; alex-in-spb@yandex.ru

Прогнозируется объем трафика сетей машина-машина (M2M) до 2016 г., классифицируется трафик сетей M2M, разрабатываются модели этого трафика. По результатам исследования установлен антиперсистентный характер опосредованного трафика M2M и самоподобный с высокой степенью самоподобия характер псевдодетерминированного трафика M2M.

Ключевые слова: *трафик M2M, самоподобный трафик, антиперсистентный трафик.*

Введение. Трафик M2M (Machine-to-Machine) появился в сетях связи с тех пор, когда возникли первые телеметрические устройства. В сетях связи с коммутацией каналов до недавнего времени наиболее широкое распространение получили системы сигнализации (контроля доступа, пожарной, аварийной сигнализации) и системы телеметрии, выполняющие функции контроля над технологическими процессами или наблюдения за окружающей средой. Доля этого трафика и ресурсы сети связи, используемые для его обслуживания, были не столь значительны, чтобы оказывать заметное влияние на качество обслуживания (QoS) других видов трафика. Например, для охранной квартирной сигнализации использовались практически только ресурсы сети абонентского доступа (абонентские линии).

Трафик телеметрии при контроле технологических процессов, например, различных трубопроводов, сетей электропередачи, железных дорог и др. обслуживался, как правило, выделенными ресурсами ведомственных сетей связи. Иные формы реализации сетей M2M были не столь много-

численны, поэтому не возникало ни существенных проблем с качеством его обслуживания, ни проблем его влияния на QoS трафика других услуг.

Современный уровень развития вычислительной техники и технологий связи приводит к проникновению информационных технологий в области деятельности, которые ранее не были вовлечены в инфокоммуникационные сети. Развитие USN (Ubiquitous Sensor Networks) открывает чрезвычайно широкое поле применения информационных технологий практически во всех областях деятельности человека [1]. Развитие сетей автомобильного транспорта VANET (Vehicular Ad Hoc Networks) [2] и иных телекоммуникационных систем, предназначенных для реализации передачи данных (ПД) между машинами (автоматами), существенным образом влияет на долю трафика M2M [3] в сетях связи и, следовательно, увеличивает его влияние на качество предоставления услуг связи.

В [4] приведены оценки возможных перспектив развития USN и трафика, порождаемого этими сетях связи. В [5, 6, 7] доказан самоподобный характер потоков трафика USN и определены значения параметра Херста для различных приложений USN. Сети USN представляют собой один из вариантов реализации сетей M2M. Внедрение последних происходит ускоренными темпами и уже сегодня актуальна задача исследования влияния трафика M2M на существующие сети связи.

Наглядным примером интенсивного роста M2M трафика может служить развитие инфокоммуникационной структуры ЖКХ [8, 9]. Можно предположить, что в результате этого процесса будет построена сеть, объединяющая различного рода датчики контролируемых объектов. Как минимум, число таких датчиков определяется числом приборов учета объема потребляемых услуг (электроэнергия, водоснабжение и др.). Таким образом, число объединяемых датчиков в рамках только данного процесса потенциально может превысить число жителей [2]. Еще одним приоритетным направлением развития сетей M2M является развитие систем мониторинга окружающей среды, а также систем контроля общественного порядка и систем безопасности [3].

Упомянутые системы могут использовать для ПД как проводные, так и беспроводные сети связи. Число оконечных устройств сетей M2M уже в ближайшее время может превысить численность населения, следовательно, и фактическую численность абонентов сетей связи. Это подтверждает общую тенденцию, определенную как Интернет Вещей (IoT) [12].

Трафик M2M оказывает существенное влияние на QoS в беспроводных сетях связи и на процессы их эксплуатации [13, 14, 15]. Например, короткие сеансы связи M2M усложняют или полностью исключают возможность контроля качества каналов методом оценки продолжительности занятия (разговора), традиционно используемым операторами связи. Специфика области применения подобных систем контроля может выражаться в особенностях производимого трафика. В частности, поведение ряда устройств может быть зависимым, что может приводить к их массовой активности, выражающейся в неконтролируемом росте трафика.

Таким образом, сегодня необходимо иметь возможность оценки M2M трафика и его влияния на качество предоставления услуг связи, а также определить методы организации систем M2M, которые бы обеспечили их «гармоничное» взаимодействие с традиционными сетями связи.

Прогноз роста трафика M2M. Существует достаточно большое число прогнозов роста трафика M2M в мире [10], роста трафика мобильной ПД [11] и сети Интернет в Российской Федерации [16]. При этом отмечается экспоненциальный характер роста трафика M2M [17], что характерно для развития новых технологий телекоммуникаций [18].

С помощью хорошо зарекомендовавшего себя метода ассоциативного прогнозирования [19] получен прогноз роста суммарного трафика M2M в сетях фиксированной и подвижной связи и беспроводного доступа (рис. 1).

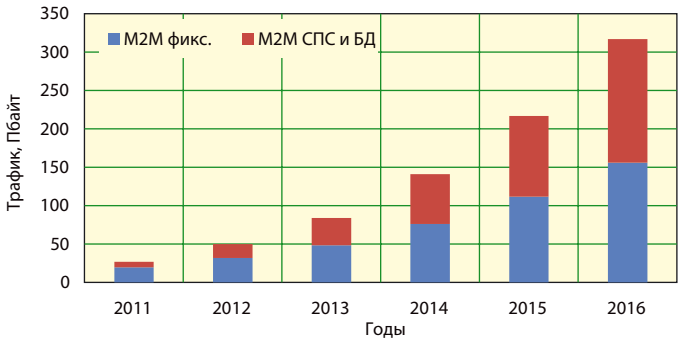

Рис. 1. **Прогноз роста суммарного трафика M2M в сетях фиксированной и подвижной связи и беспроводного доступа**

Как видно из приведенного прогноза, оценки M2M трафика в сетях фиксированной и подвижной связи, а также беспроводного доступа близки по значению, что объясняется близкими значениями общей величины трафика в этих сетях. Следует отметить, что при прогнозировании учитывался тот факт, что по данным [20] 33% трафика ПД сетей подвижной связи переносятся в сеть фиксированной связи, увеличивая ее общий трафик.

Как видим, суммарный объем прогнозируемого трафика M2M на 2016 г. превышает 300 Пбайт, что требует проведения детальных исследований его характеристик. Отметим, что доля трафика M2M составит при этом около 5% от суммарного трафика сетей связи РФ. Кроме того, следует ожидать, что трафик M2M может иметь существенно иные характеристики, чем трафик традиционных сетей связи.

Особенности трафика M2M. Для описания трафика в современных сетях связи существуют различные теоретические модели, как правило, построенные на основе теории массового обслуживания [21]. Задачей построения модели является описание свойств трафика (потока) и параметров его обслуживания сетью связи.

Трафик M2M представляет собой поток данных (пакетов в сети ПД или сеансов в сети с коммутацией каналов). Основным его отличием от абонентского трафика человек-человек H2H (Human-to-Human) является то, что инициатором передачи информации является автоматическое устройство. В зависимости от реализации системы обмена данными (протокола взаимодействия) событие передачи может наступить при следующих условиях:

- воздействие внешних факторов, приводящих к ПД (изменение физических параметров, контролируемых датчиком);
- истечение определенного интервала времени (в общем случае продолжительность интервала может быть любой постоянной или вычисляемой в соответствие с каким-либо законом, строго говоря, не случайной величиной);

● технические причины — передача служебных данных (инициализация устройства, вызванная включением, перезапуском устройства и т.д.), не связанные с приведенными выше факторами.

В соответствие с перечисленными условиями, приводящими к ПД, в системах M2M можно условно выделить три основных типа трафика.

Первый тип — опосредованный трафик; производится автоматическими системами с использованием активных устройств (устройство может быть инициатором ПД). Этот трафик можно рассматривать как реакцию на различные случайные события (например, попадание измеряемой величины в некоторый интервал, срабатывание аварийной или иной сигнализации и т.п.). В данном случае свойства трафика зависят от свойств контролируемых процессов. Но если такая система предназначена для контроля относительно редких случайных событий (системы аварийной сигнализации, контроля доступа и др.), то зачастую интенсивность наблюдаемых событий может быть соизмерима или даже меньше интенсивности отказов самого устройства наблюдения. Для обеспечения необходимой надежности обнаружения наблюдаемых событий необходимо контролировать техническое состояние датчиков. Для этого требуется передача служебных данных, объем которых может существенно превышать объем полезной информации, а свойства трафика определятся особенностями процессов диагностики состояния датчиков.

Второй тип — псевдодетерминированный трафик; производится автоматическими системами с использованием пассивных датчиков. В настоящее время получили распространение системы диспетчерского управления и сбора данных (SCADA — Supervisory Control And Data Acquisition), построенные по принципу главный — подчиненный (Master-Slave). В этих системах датчики являются подчиненными (пассивными устройствами) и производят ПД по запросу главного (Master) устройства. В этом случае свойства трафика определяются алгоритмом выбора интервала времени между моментами передачи запросов данных. Как правило, в существующих системах интервалы между моментами опроса не случайны. Опрос датчиков происходит в соответствие с некоторым расписанием или просто с заданным постоянным периодом. К данному типу трафика относится также трафик, производимый различными автоматическими системами в детерминированные моменты времени (обновление данных, программного обеспечения по расписанию и др.).

Третий тип — служебный трафик; характерен для систем с активными датчиками. Он осуществляется при наступлении некоторых внешних (как правило, случайных) событий, приводящих к необходимости выполнения служебных операций по поддержанию работоспособности системы, а также диагностики состояния датчиков. Это служебный трафик, производимый в результате различного рода сбоев работы аппаратных или программных средств, в целях устранения которых выполняются необходимые процедуры установления соединения, передачи параметров для настройки датчиков и т.п. Как правило, служебный трафик приводит к генерации трафика сигнализации, который достаточно хорошо исследован для сетей USN в [5]. Поэтому его характеристики далее не анализируются.

Модели трафика M2M. Опосредованный трафик. Такой трафик возникает в системах с активными устройствами под влиянием внешних процессов. В зависимости от конкретного приложения системы мониторинга характер этих процессов может быть различен. Имеет смысл рассмотреть лишь те процессы, которые могут иметь место в наиболее массовых приложениях:

● аварийная сигнализация (противопожарная, сигнализация целостности конструкций зданий и сооружений, отказов технических систем жизнеобеспечения, сигнализация незаконного проникновения на охраняемые объекты), реализуемая, например, в ЖКХ;

● контроль угроз среде обитания человека (загрязнения окружающей среды, погодных условий, сейсмических и климатических угроз), организуемый структурами Министерства по чрезвычайным ситуациям;

● контроль опасных состояний здоровья человека (сердечного ритма, артериального давления, состава крови и других показателей), реализуемый в медицинских учреждениях в лечебных и профилактических целях.

Каждый из упомянутых выше процессов может иметь свои характерные особенности, что будет отражаться на трафике, производимом соответствующей системой. Однако общей характерной особенностью приложений является то, что события, приводящие к возникновению трафика, относительно редки. Интенсивность этих событий соизмерима с интенсивностью отказов технических устройств, следовательно, для эксплуатации данных систем необходимо контролировать состояние устройств, что приводит к необходимости передачи служебных сообщений. Свойства трафика служебных сообщений зависят от метода контроля состояния технического состояния. Например, для контроля состояния может быть использован периодический опрос устройств сервером. В этом случае период опроса может выбираться, исходя из требований к надежности (коэффициенту готовности) системы [21]. Коэффициент готовности определяется следующим образом:

$$K_{\Gamma} = \frac{T_{\text{И}}}{T_{\text{И}} + T_{\text{О}} + T_{\text{В}}}, \qquad (1)$$

где $T_{\text{И}}$ — время исправного состояния (наработка на отказ), ч; $T_{\text{О}}$ — время обнаружения неисправности, ч; $T_{\text{В}}$ — время восстановления, ч.

Предположим, что отказы устройства случайны и равновероятны на протяжении периода опроса. Тогда необходимый период опроса может быть получен из (1):

$$t_o = \frac{2}{K_{\Gamma}}\left(T_{\text{И}} - K_{\Gamma}\left(T_{\text{И}} + T_{\text{В}}\right)\right). \qquad (2)$$

Например, при требовании $K_{\Gamma} = 0{,}9999$, времени восстановления $T_{\text{В}} = 2$ ч и наработке на отказ 50 000 ч необходимый период опроса составит 6 ч. Таким образом, при реальных значениях надежности технических систем интенсивность служебного трафика относительно мала и имеет существенное значение только при обслуживании достаточно большого числа подобных систем.

Сложность обслуживания трафика, создаваемого подобными системами, состоит в том, что «поведение» данного типа устройств может быть зависимым. Например, некоторое количество устройств контролирует состояние объекта или технологического процесса, которое изменяется таким образом, что все или большая часть данных устройств контроля должны передать информацию о состоянии (аварийная ситуация и все параметры вышли за допустимые границы). Такая ситуация может привести к массовым сообщениям (вызовам). В этом случае интенсивность трафика будет определяться числом устройств контроля,

объемом передаваемых сообщений, вероятностью активизации устройств и интенсивностью событий, приводящих к активизации устройств.

Для анализа подобного трафика построена имитационная модель, в которой принят ряд допущений.

1. Каждое из n устройств может находиться в пассивном и активном состояниях.

2. В пассивном состоянии устройство производит только технологический трафик (контроль состояния), представляющий собой периодический детерминированный процесс с периодом T_i. Величина T_i выбирается случайно при инициализации модели как равномерно распределенная случайная величина в границах от $T_{\min}$ до $T_{\max}$.

3. В активное состояние устройство переходит при наступлении некоторого события и находится в нем короткое время, в течение которого производит случайный объем трафика, затем снова переходит в пассивное состояние. Объем трафика, производимый устройством в активном состоянии, случаен и имеет равномерное распределение от $v_{\min}$ до $v_{\max}$ со средним значением $\bar{v}$.

4. Событие наступает в случайные независимые моменты времени. Допускаем, что интервал времени между целевыми событиями случаен и имеет экспоненциальное распределение вероятности со средним значением $\bar{t}_E$.

При моделировании были приняты следующие значения: $n = 10$, $T_{\min} = 0$, $T_{\max} = 1$, $v_{\min} = 0$, $v_{\max} = 1000$ (сообщений), $\bar{t}_E = 100$. На рис. 2 приведен пример реализации потока пакетов в системе, полученный имитационным моделированием. Видно, что в процессе поступления имеют место существенные пики трафика, значительно превосходящие среднее значение.

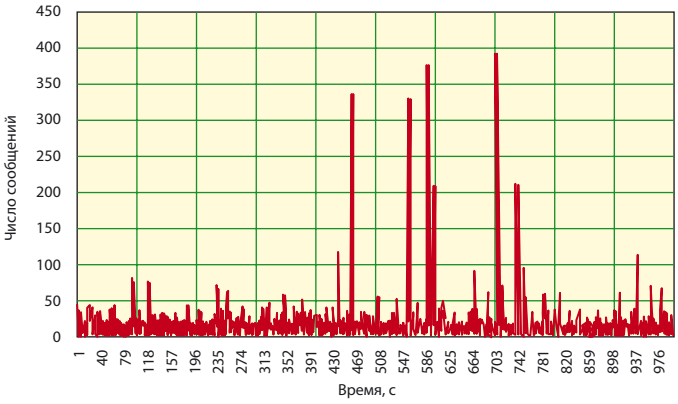

Рис. 2. **Реализация потока опосредованного трафика**

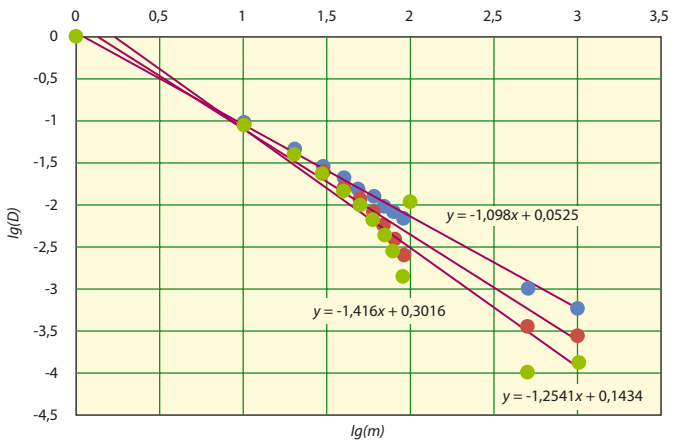

Рис. 3. **Оценка коэффициента Херста с помощью графика изменения дисперсии**

На рис. 3 представлена зависимость оценки изменения дисперсии для проведения оценки коэффициента Херста. На графике приведены три прямые для значений вероятности $p = 0{,}1;\ 0{,}5;\ 1{,}0$. Коэффициент Херста для этих значений составляет $H = 0{,}451;\ 0{,}375;\ 0{,}292$, соответственно.

Таким образом, производимый системой трафик в зависимости от параметров может иметь свойства антиперсистентного ($H < 0{,}5$) или простейшего ($H \approx 0{,}5$) потока. Ранее антиперсистентные свойства наблюдались для потока потерь пакетов UDP [22].

Модели трафика M2M. Псевдодетерминированный трафик. Сегодня широкое распространение получили системы мониторинга и диспетчерского управления (SCADA). Подобная система представляет собой систему мастер-подчиненный, в которой роль мастера выполняет сервер сбора данных, а подчиненного — контроллер или датчик (сенсор), установленный на контролируемом объекте. ПД осуществляется через сеть связи. В общем случае в сети может функционировать множество таких систем (рис. 4).

Рис. 4. **Общая структура системы мониторинга и диспетчерского управления**

Как правило, трафик в направлении между i сервером и j устройством представляет собой детерминированный поток данных (пакетов): запросов сервера и ответов контроллера (датчика). В общем случае переменные параметры потока системы могут быть определены расписанием и имеют определенный период повторения T_i.

Если в сети функционирует n систем мониторинга, то при неизменных фазовых сдвигах между моментами поступления запросов (ответов) $\varphi_i\ i = 1 \ldots n$, общий трафик также будет представлять собой детерминированный периодический процесс с периодом, равным наименьшему общему кратному всех периодов опроса $T_S = lcm\{T_i\} \quad i = 1 \ldots n$.

Если фазовые сдвиги не постоянны и случайны (вследствие асинхронного включения и перезапусков отдельных систем), то общий трафик также приобретает свойства случайного процесса (псевдодетерминированный трафик).

С помощью системы имитационного моделирования была построена модель трафика от нескольких ($n = 10$) систем мониторинга, производящих детерминированные (в установившемся режиме) периодические потоки. Период $T_i \quad i = 1 \ldots n$, выбирается случайно в пределах от 1 до 60 с (значение периода подчиняется равномерному закону распределения). Каждая из систем мониторинга может перезапускаться в случайный момент времени, т.е. случай-

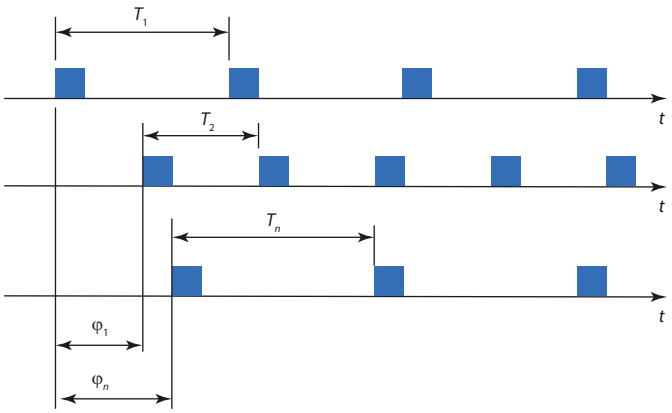

Рис. 5. **Модель трафика систем мониторинга**

ным образом может изменяться фазовый сдвиг φ_i $i = 1 \ldots n$. Интервал времени между рестартами системы случаен и подчинен экспоненциальному закону распределения

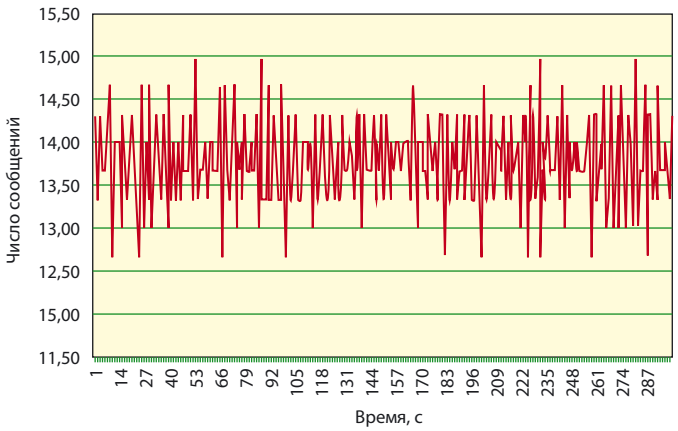

Рис. 6. **Реализация потока детерминированного трафика**

вероятности со средним значением 0,6 рестартов в час. Пример реализации трафика приведен на рис. 6.

Полученный поток $X(t)$ был проверен на свойства самоподобия. На рис. 7 *а*—*г* приведены реализации потока

$$X_i^{(m)} = \frac{1}{m} \sum_{t=m(i-1)+1}^{mi} X(t),$$

агрегированные за различные интервалы времени m.

Для потока получена оценка коэффициента Херста методом аппроксимации графика изменения дисперсии потока

$$\left(\sigma^2\left(X_t^{(m)}\right)\right) \sim -\beta \log(m) + \log(a).$$

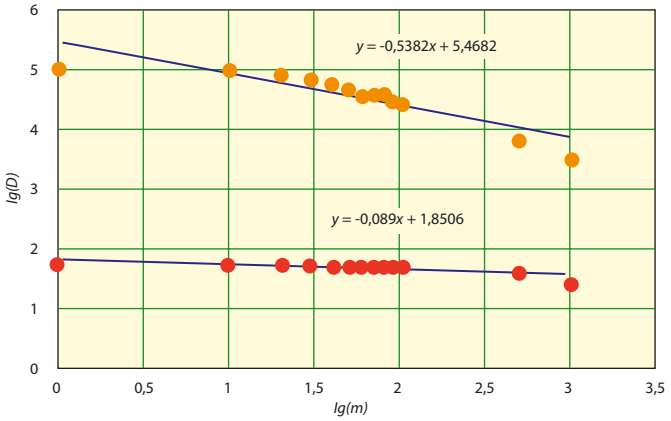

Рис.8. **Оценка коэффициента Херста графиком изменения дисперсии (для различных интенсивностей перезапуска систем)**

Аппроксимация приведена на рис.8.

Таким образом, производимый системой трафик имеет свойства самоподобного потока $(H > 0{,}5)$. Коэффициент Херста потока изменяется в зависимости от интенсивно-

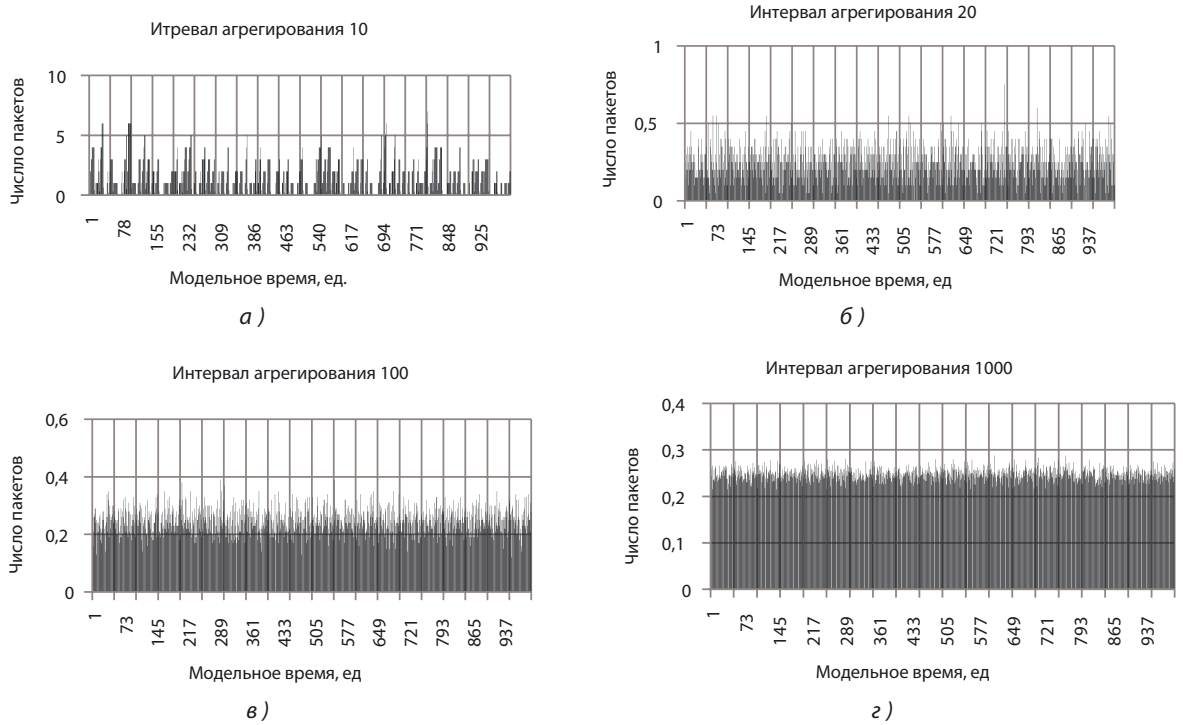

Рис. 7. **Реализации потока с разными интервалами агрегирования**

сти перезапуска. При $p = 0{,}1$ значение $H = 0{,}73$, при $p = 1$ $H = 0{,}96$.

Выводы. 1. Системы M2M являются одними из наиболее перспективных и активно развивающихся направлений в области телекоммуникаций. Прогноз, выполненный ассоциативным методом, показывает, что к 2016 г. доля трафика сетей M2M составит около 5% от общего объема трафика сетей связи или более Пбайт в абсолютном выражении.

2. Одними из наиболее значимых источников трафика M2M являются системы мониторинга и диспетчерского управления. Предложено выделить три типа трафика, производимого такими системами: опосредованный, псевдодетерминированный и служебный.

3. Статистические свойства потока опосредованного трафика определяются такой его особенностью как зависимость источников трафика: при наступлении некоторых событий она приводит к массовой активности устройств и, как следствие, случайным пикам трафика. Анализ статистических свойств данного потока доказывает, что он антиперсистентный.

4. Статистические свойства псевдодетерминированного трафика определяются числом и периодами последовательностей опроса устройств, а также интенсивностью рестартов. Анализ статистических свойств данного потока доказывает, что он самоподобен с высокой степенью самоподобия.

ЛИТЕРАТУРЫ

1. **Кучерявый А.Е., Прокопьев А.В., Кучерявый Е.А.** Самоорганизующиеся сети.— С. Петербург: Изд–во «Любавич», 2011.
2. **Vinel A., Campolo C., Petit J., Koucheryavy Y.** Trustworthy broadcasting in IEEE 802.11p/WAVE vehicular networks: Delay analysis // IEEE Communications Letters.— 2011.— 15 (9).
3. **Andreev S., Galinina O., Koucheryavy Y.** Energy-efficient client relay scheme for machine-to-machine communication / Proceedings Global Telecommunications Conference (GLOBECOM 2011), Houston, Texas, USA.— 5—9 December 2011.
4. **Кучерявый А.Е., Парамонов А.И.** Модели трафика для сенсорных сетей в u-России // Электросвязь.— 2006.— № 6.
5. **Koucheryavy A., Prokopiev A.** Ubiquitous Sensor Networks Traffic Models for Telemetry Applications / in The 11th International Conference on Next Generation Wired/Wireless Networking NEW2AN 2011, Saint-Petersburg. Springer LNCS 6869.— Aug. 2011.
6. **Koucheryavy A., Vybornova A.** Ubiquitous Sensor Networks Traffic Models for Medical and Tracking Applications / in The 12th International Conference on Next Generation Wired/Wireless Networking NEW2AN 2012, Saint-Petersburg. Springer LNCS 7469.— Aug. 2012.
7. **Koucheryavy A., Muthanna A., Prokopiev A.** Ubiquitous Sensor Networks Traffic Models for Image Applications. Internet of Things and its Enablers (INTHITEN) / Proceedings. Conference, State University of Telecommunication, St. Petersburg, Russia.— 3—4 June 2013.
8. **Schneps-Schneppe M., Namiot D.** M2M Applications and Open API: What Could Be Next? / in The 12th International Conference on Next Generation Wired/Wireless Networking NEW2AN 2012, Saint-Petersburg. Springer LNCS 7469.— Aug. 2012.
9. **Schneps-Schneppe M., Maximenko A., Namiot D.** On M2M communications standards for smart metering. Internet of Things and its Enablers (INTHITEN) / Proceedings. Conference, State University of Telecommunication, St. Petersburg, Russia.— 3—4 June 2013.
10. **Dr. Wahle S.** Competence Center NGNI. Open MTC Platform M2M Solutions for Smart Cities and the Internet of Things. 6th KUVS NG SDP Workshop Berlin.— April 4, 2012. (http://www.kuvs-ngsdp.org/_slides/05_OpenMTC-Platform_Wahle.pdf).
11. Обзор российского рынка мобильного интернет-доступа 22.01.2013, Мобильные телекоммуникации. http://www.mobilecomm.ru/obzor-rossiyskogo-rinka-mobilnogo-internet-dostupa.
12. **Кучерявый А.Е.** Интернет Вещей // Электросвязь.— 2013.— № 1.
13. **Drajic D. et al.** Traffic Generation Application for Simulating Online Games and M2M applications via Wireless Networks. 9th Conference on Wireless On-demand Network Systems and Services WONS 2012, Courmayeur, Italy.— 9—11 January 2012.
14. **Shafig M.Z. et al.** A First Look at Cellular Machine-to-Machine Traffic: Large Scale Measurement and Characterization. 12th ACM Sigmetrics / Performance International Conference. London, England, UK.— 11—15 June 2012.
15. **Potsch T., Marwat S.N.K., Zaki Y., Gorg C.** Influence of Future M2M Communication on the LTE System / Wireless and Mobile Networking Conference. Dubai, United Arab Emirates.— 23—25 April 2013.
16. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012—2017, CISCO white paper.— 6 February 2013.
17. Обзор российского рынка мобильного интернет-доступа 22.01.2013, Мобильные телекоммуникации. http://www.mobilecomm.ru/obzor-rossiyskogo-rinka-mobilnogo-internet-dostupa.
18. Минкомсвязь. Статистика отрасли. http://minsvyaz.ru/ru/directions/stat/stat/.
19. **Кучерявый А.Е., Ревелова З.Б., Парамонов А.И.** Реструктуризация трафика сетей связи и новые подходы к прогнозированию их развития // Электросвязь.— 2003.— № 2.
20. Прогноз Cisco. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11—520862.pdf.
21. **Кучерявый А.Е., Парамонов А.И., Кучерявый Е.А.** Сети связи общего пользования. Тенденции развития и методы расчёта.— М.: ФГУП ЦНИИС, 2008.
22. **Бельков Д.В., Едемская Е.Н., Незамова Л.В., Едемская Т.А.** Анализ потерь пакетов при передаче UDP-трафика / Зб. матеріалів Всеукраінськоі науково-технічноі конференціі «Інформаційні системи та комп'ютерний мониторінг», Том 1.— 11—13 квітня 2011 р., Донецьк: ДонНТУ.— 2011.

Получено 12.02.14