УДК 519.6

С. Д. Белов [1], С. В. Ломакин [2], В. А. Огородников [3], С. М. Пригарин [4], А. С. Родионов [5], Л. Б. Чубаров [6]

[1] Институт ядерной физики СО РАН
пр. Акад. Лаврентьева, 11, Новосибирск, 630090, Россия

[2, 3, 4, 5] Институт вычислительной математики и математической геофизики СО РАН
пр. Акад. Лаврентьева, 6, Новосибирск, 630090, Россия

[1, 6] Институт вычислительных технологий СО РАН
пр. Акад. Лаврентьева, 6, Новосибирск, 630090, Россия

[3, 4, 5] Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия
E-mail: [3] ova@osmf.sscc.ru; [4] smp@osmf.sscc.ru;
[5] alrod@sscc.ru; [6] chubarov@ict.nsc.ru

АНАЛИЗ И МОДЕЛИРОВАНИЕ ТРАФИКА В ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ *

В работе представлены некоторые результаты анализа реального трафика IP-сетей и на его основе предлагается метод численного моделирования соответствующих временных рядов. Метод основан на нелинейных преобразованиях гауссовских случайных процессов. Анализируется фрактальная размерность как исходных, так и моделируемых временных рядов. Показано, что предлагаемый метод позволяет с достаточной точностью воспроизводить одномерные распределения, корреляции и фрактальную размерность временных рядов исследуемого трафика.

Ключевые слова: сетевой трафик, статистический анализ, численное моделирование временных рядов, нелинейные преобразования гауссовских процессов, фрактальная размерность.

Введение

Задача моделирования трафика в телекоммуникационных и компьютерных сетях различного назначения является одной из основных при создании их моделей. При рассмотрении коротких периодов, как правило, используются модели пуассоновских процессов, однако при моделировании трафика на длинных временных отрезках подобные модели неадекватны в силу квазипериодичности и существенной автокорреляционной зависимости трафика, что будет показано ниже. В частности, хорошо зарекомендовавший себя метод моделирования одномерных стационарных процессов с заданными распределением и автокорреляционной функцией (АКФ), использовавшийся нами при моделировании отказов в работе вычислительного оборудования [1], здесь невозможно применить в силу чрезвычайно медленно затухающей АКФ (рис. 1). По этой причине многими авторами рассматриваются другие модели, прежде всего модели самоподобных процессов [2–6]. Однако предложенные ими модели также не вполне воспроизводят сложный дважды квазипериодический характер IP-трафика, наблюдаемый в научно-образовательных сетях, к которым принадлежат и сети институтов Сибирского отделения РАН. Нами накоплены уникальные статистические данные по входящему / исходящему IP-трафику Института вычислительной математики и математической геофизики (ИВМиМГ) СО РАН более чем за полтора года наблюдений (с интеграцией по 5-минутным интервалам), которые позволили с высокой степенью точности

* Работа выполнена при финансовой поддержке президентской программы «Ведущие научные школы» (НШ-4774.2006.1, НШ-931.2008.9), РФФИ (проект № 06-07-89038-а), комплексного интеграционного проекта СО РАН 1.7 и проекта Минобрнауки РФ 2007-4-1.4-15-04-004.

оценить разнообразные параметры трафика и предложить новую модель, воспроизводящую их с высокой степенью достоверности. При построении моделей использовались также данные по трафику Института ядерной физики (ИЯФ) СО РАН за более короткий период (2 месяца). Одновременно решалась задача оценки качества мониторинга трафика СО РАН с помощью создаваемого в рамках проектов СО РАН и Минобрнауки РФ специального сервера сбора статистики (ССС) сети передачи данных (СПД) СО РАН.

Задачи и структура ССС СПД СО РАН

Решение задач мониторинга телекоммуникационной инфраструктуры СПД СО РАН необходимо для поддержки эффективного управления сетью, обеспечения надежности ее функционирования, гарантированного качества обслуживания абонентов и безопасности, а также для сбора статистики и детального контроля выполнения абонентами сети установленного регламента работы.

Одним из первых вопросов, возникающих при формализации задач мониторинга сетевой инфраструктуры, является вопрос об определении списка или набора этих задач. Как указано в работе [7], в такой набор с необходимостью входят:

- поддержка эффективного управления сетью;
- обеспечение надежности функционирования сети;
- гарантия необходимого уровня качества обслуживания абонентов;
- обеспечение безопасности функционирования сети;
- обеспечение сбора статистики;
- решение вопросов биллинга в сети;
- решение фискальных задач, связанных с соблюдением регламента работы абонентов в сети.

Из перечня ясна обязательность непосредственной привязки задач мониторинга к конкретным задачам управления сетью.

Следующим шагом в постановке задачи сетевого мониторинга является определение набора параметров, описывающих состояние исследуемой сети и обеспечивающих возможности управления сетью как объектом. Множество этих параметров в целом согласуется со стандартными параметрами, регистрируемыми в базах данных устройств, однако их общее количество избыточно для оперативного управления. В такой ситуации становится необходимым определение совокупности параметров, влияющих на методы решения *практических* задач мониторинга.

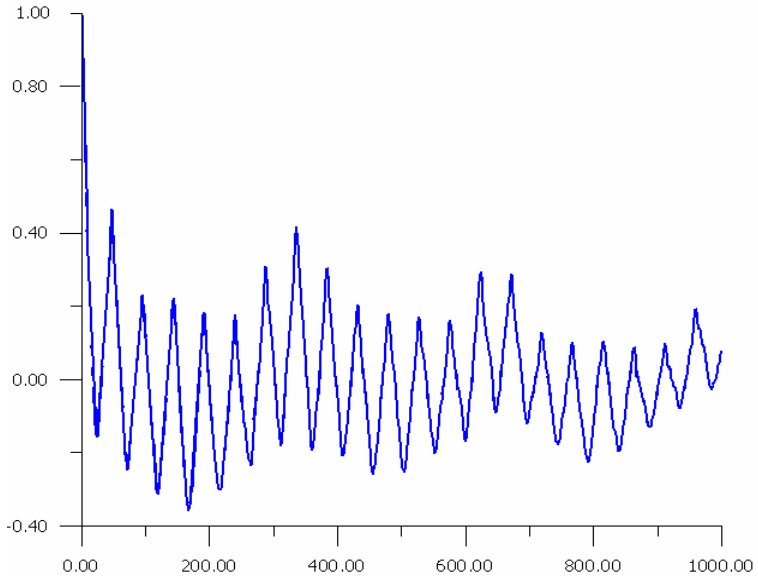


Рис. 1. Двухдневный фрагмент АКФ, рассчитанной по двухмесячным данным исходящего трафика ИЯФ, интегрированных по 30-минутным интервалам

Приведем некоторые количественные оценки масштабов и качественного состава сети Новосибирского научного центра (ННЦ) СО РАН:

- количество активных коммутирующих устройств – более трех десятков (включая такие устройства, как Cisco 2950, Cisco 4507, Cisco 7206NPE, различные сервера технологических баз данных, например сервера видеоконференцсвязи, VoIP-шлюзы и т. п.);
- количество «пассивных» устройств – более 200 (мультиплексоры, модемы, конверторы и т. п.);
- количество магистральных сегментов кабельных линий связи – более 50, общей протяженностью более 150 км;
- количество точек соединений – более 4 000;
- количество систем энергоснабжения, аварийного питания с разными уровнями мощности – более 30;
- системы климат-контроля.

Таким образом, общее число параметров, влияющих на решение тех или иных конкретных задач мониторинга, может быть оценено в 4–5 тысяч. Необходимо заметить, что эти параметры характеризуют только физический и канальный уровни сети. В приведенных выше цифрах отсутствуют данные, определяющие региональные структуры СПД СО РАН и интегрирующие их канальные структуры. Эти объекты обладают относительной автономностью и, как следствие, оказывают малое влияние на работу остальных сетевых структур, в то время как сегмент, расположенный в ННЦ, в полной мере определяет работу всех абонентов СПД СО РАН.

Необходимость учета характеристик сетевого уровня при решении задач мониторинга приводит, в свою очередь, к необходимости увеличения общего количества параметров, определяющих работу сети, до 5–10 тысяч. Это число может быть увеличено, если исходить из необходимости привлечения информации уровня приложений. Для оценки, например, количества сессий, одновременно существующих в исследуемом сетевом сегменте, приходится учитывать число пользователей этой сети, которое в отдельные временные интервалы достигает 20–40 тысяч.

Для решения всего комплекса задач мониторинга необходимо учитывать и временные масштабы процессов в сети, а также временные масштабы, характеризующие актуальность тех или иных задач. С достаточной определенностью можно говорить о наличии в сети процессов продолжительностью от единиц секунд до единиц и десятков минут; от десятков минут до часов и более; от часов до суток, недель и месяцев. Эти масштабы, очевидно, зависят от специфики решаемых задач мониторинга.

Установленный и запущенный в опытную эксплуатацию в марте 2007 г. первый сервер разрабатываемой системы мониторинга и сбора статистики был собран на основе современного двухпроцессорного компьютера (Xeon 3.20GHz), оснащенного 4 Гб оперативной памяти, тремя сетевыми Ethernet-интерфейсами: 100 Мбит/с в качестве системного интерфейса и двумя гигабитными в качестве мониторирующих.

Исследуемый поток передается с центрального коммутатора СПД СО РАН с использованием технологии мониторирующих span-портов. При этом на один из интерфейсов коммутатора / маршрутизатора копируется весь трафик некоторых выделенных интерфейсов. Данное решение обладает рядом недостатков, таких как недостаточная масштабируемость, повышенная нагрузка на активное оборудование инфраструктуры сети и искажение временных характеристик исследуемого трафика, которые будут преодолены в ходе последующей модернизации аппаратной базы ССС.

Для определения адекватности установленной на сервере операционной системы OpenBSD задачам считывания и анализа потоков данных значительной интенсивности была проведена ее калибровка, в ходе которой генерировался тестовый поток, направленный с одного из внутренних хостов СПД во внешнюю по отношению к СПД сеть, затем этот поток сопоставлялся с принятым системой мониторинга. Результаты испытаний показали, что поведение системы вполне соответствует ожиданиям при существующих значениях загрузки мониторируемых подключений.

В реализуемой архитектуре системы предусмотрена возможность одновременной работы множества автономных программ, ведущих обработку анализируемого потока. По результа-

там испытаний была выбрана программа CNUPM, обеспечивающая минимальную загрузку процессора и, следовательно, максимальную производительность, что позволяет дополнительно задействовать другие специализированные коллекторы, которые могут анализировать не только сетевые атрибуты пакета, но и содержащиеся в пакетах данные (payloads). В качестве программ-коллекторов, анализирующих передаваемые данные, применялись программа URLSNARF, являющаяся компонентой пакета DSNIFF, и система SNORT. Поскольку система SNORT в основном ориентирована на распознавание вторжений, вирусных атак и прочих угроз, а не на анализ трафика и идентификацию прикладных протоколов, ее библиотека сигнатур должна быть существенно пересмотрена и сокращена. На начальном этапе работы рассматривался существенно ограниченный набор сигнатур, необходимых для идентификации только двух сетевых приложений: E-Donkey и BitTorrent, относящихся к категории наиболее важных в наших условиях Peer-To-Peer приложений, ответственных, по предварительным оценкам, за генерацию до 20–30 % нелегитимного трафика.

Отметим, что CNUPM собирает интегральную статистику трафика, программа URLSNARF выделяет из анализируемого потока лишь характерные запросы «http GET», используемые программами, которые работают в протоколе BitTorrent, а программа SNORT с примененной библиотекой фиксирует только сигнатуры, характерные для протокола EDonkey.

Сбор исходных данных для моделирования трафика

Как отмечалось ранее, для построения адекватных моделей необходимо учитывать суточную и недельную периодичность, что требует наличия данных за возможно более длительный период. Вместе с тем прототип системы сетевого мониторинга заработал в штатном режиме лишь с середины 2007 г. По этой причине был организован сбор данных по трафику в двух отдельно взятых институтах: ИВМиМГ и ИЯФ СО РАН, при этом в ИВМиМГ СО РАН данные собирались специально для выполнения обсуждаемого здесь исследования.

Была собрана статистика по трафику на внешнем канале ИВМиМГ СО РАН за период с апреля 2006 по май 2008 г. Статистика представлена данными на интервалах продолжительностью пять минут и содержит информацию об адресах и используемых портах источников и назначения. Данные представлены для всех активных хостов сети, включая как пользовательские системы, так и публичные ресурсы института (web, ftp, почтовый сервер и пр.). Таким образом, оказались доступны подробные данные внешнего трафика академического института по пятиминутным интервалам, собранные более чем за годичный период. Для сбора статистики использовался пакет trafd, установленный на маршрутизаторе, работающем под управлением операционной системы FreeBSD. Пакет включает в себя инструменты сбора данных о трафике, сохранения данных на диск и инструменты для оперативного контроля за проходящим трафиком. Для обработки полученных статистических данных написан набор скриптов на языке Perl.

В результате статистического и содержательного анализа данных получена информация о структуре трафика и о распределении потребителей и источников трафика внутри сети института. В идеале такая информация должна составить основу для выработки предложений по модернизации сети института-абонента. Была получена также информация о наборе и распределении используемых портов, что, в свою очередь, позволяет делать выводы о протоколах, использующихся для взаимодействия с сетью Интернет и об их соответствии RFC 4340, устанавливающим зависимости между протоколами и используемыми ими портами. Например, оказалось, что доли входящего / исходящего трафиков имеют соотношение 75/25 % от общего объема внешнего трафика института. Летом происходит заметное снижение объемов трафика – до 75 % от весеннего периода; 5 % хостов суммарно потребляют 80 % трафика, 60 % хостов суммарно потребляют менее 1 %. По источникам трафика ситуация существенно не меняется. На 4 % хостов приходится 80 % исходящего трафика, 70 % хостов суммарно производят менее одного процента исходящего трафика.

Основу внешнего трафика института составляют web-протоколы: http (порт 80), http-alt (порт 591), https (порт 443) и proxy (порты 3128, 8008, 8080 и др.). Причем доля протокола http (порт 80) в этом семействе составляет порядка 95 %. Результаты анализа трафика, прове-

денного по временным интервалам, показали суточные, недельные и даже сезонные зависимости суммарного внешнего трафика. Также можно говорить о его взрывном периодическом характере. Подобный характер случайного процесса делает затруднительным его моделирование обычными моделями временных рядов. Собранные данные являются основой для построенных статистических моделей.

В целом, системы сбора статистики трафика, использованные в сетях ИЯФ и ИВМиМГ СО РАН во многом подобны, с той разницей, что в качестве отчетного периода в ИЯФ использовался интервал в 30 минут, тогда как в ИВМиМГ – 5 минут. Это приводит к некоторому загрублению результатов анализа трафика ИЯФ в сопоставлении с трафиком ИВМиМГ. Данные, собираемые коллектором CNUPM на точках мониторирования СПД СО РАН, во многом подобны данным, собираемым в сетях ИЯФ и ИВМиМГ, – существенным отличием является отсутствие в периодической статистике записи о количестве пакетов за отчетный период. При необходимости эти данные могут быть добавлены.

Алгоритм моделирования сетевого трафика

Предположим, что наблюдается выборка $X = (x_1, ..., x_N)$ и целью является разработка алгоритмов численного моделирования случайных последовательностей y_n произвольной длины, статистические свойства которых «подобны» статистическим свойствам выборки *X*. В нашем случае выборка *X* описывает процесс передачи информации в компьютерной сети, и, таким образом, речь идет о построении имитационной модели трафика, позволяющей многократно воспроизводить случайные последовательности аналогичные тем, которые наблюдаются в реальных компьютерных сетях. В отношении наблюдаемой выборки *X* делается важное предположение о том, что $x_1, ..., x_N$ представляют собой выборочные значения *стационарной* (и эргодической) случайной последовательности с конечной дисперсией. Это предположение, естественно, может вызвать множество возражений, однако отказ от стационарности значительно усложняет проблему. Таким образом, задача состоит в конструировании численной модели стационарной случайной последовательности y_n.

Методы численного моделирования стационарных случайных процессов хорошо изучены (см., например, [8–10]), что обусловлено множеством прикладных стохастических задач в самых различных областях. Для имитации временных рядов сетевого трафика было решено использовать известный метод *обратной функции распределения*:

$$y_t = F^{-1}\Phi(u_t), \tag{1}$$

где u_t – гауссовская стационарная последовательность с нулевым средним, единичной дисперсией и некоторой корреляционной функцией $\rho(t) = Eu_{s+t}u_s$. Случайные процессы (1) называют иногда *квазигауссовскими* [11]. Ниже представлено краткое описание алгоритма моделирования сетевого трафика, построенного на основе этого метода.

1. Используя предположение о стационарности, по выборке *X* оценивается одномерное распределение и корреляционная функция стационарной последовательности. Функцию одномерного распределения будем обозначать далее через *F*, а ковариационную функцию – через *r*(*t*).

2. Формула (1) гарантирует необходимое одномерное распределение *F* моделируемой последовательности y_n. Для того чтобы обеспечить требуемую ковариационную функцию *r*(*t*), корреляционная функция ρ(*t*) гауссовской последовательности вычисляется на основе соотношений

$$r(t) = R_f(\rho(t)),$$

$$R_f(r) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(u)f(v)j_r(u,v)dudv, \tag{2}$$

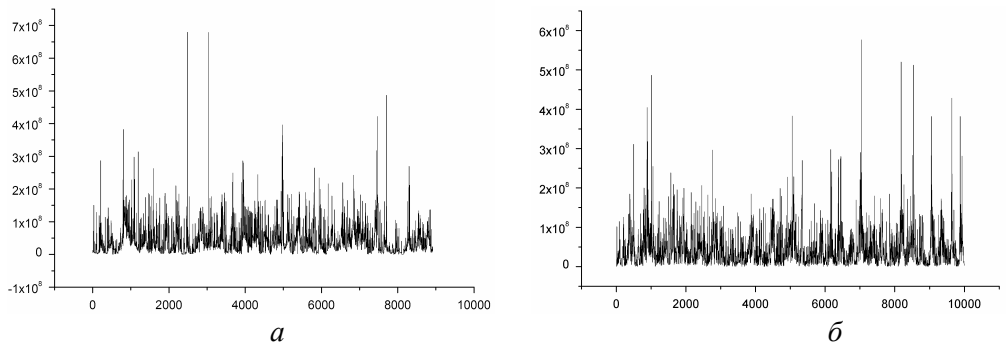
где $\varphi_\rho(u,v) = [2\pi\sqrt{1-\rho^2}\exp(\frac{u^2+v^2-2\rho uv}{2(1-\rho^2)})]^{-1}$ является плотностью двумерного гауссовского вектора с нулевым математическим ожиданием, единичной дисперсией компонент и коэффициентом корреляции между компонентами ρ. Здесь мы сталкиваемся с проблемами, связанными с численным обращением (2) и возможным отсутствием свойства положительной определенности вычисленной функции ρ (эти проблемы подробно обсуждаются в [10]). Поэтому при решении многих прикладных задач воспроизвести ковариационную структуру моделируемого негауссовского процесса удается лишь приближенно.

3. Моделируется стационарная гауссовская случайная последовательность u_t с нулевым средним, единичной дисперсией и корреляционной функцией ρ(t). Для моделирования были использованы авторегрессионные и спектральные модели (см. [8–10; 18; 21]).

4. Случайная последовательность y_t моделируется по формуле (1).

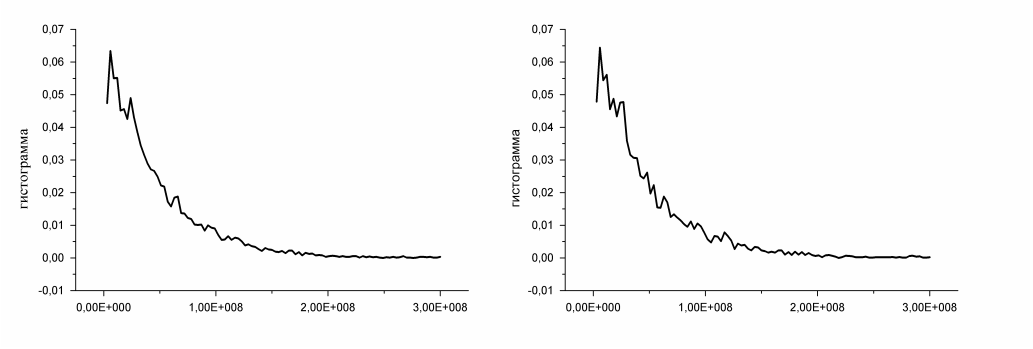
Результаты численного моделирования сетевого трафика

В качестве наблюдаемой выборки $X = (x_1, ..., x_N)$ использовался ряд входного трафика ИВМиМГ СО РАН за июнь 2006 г.: x_n – это интегральные значения трафика за 5 минут, N = 8 921. На рис. 2–5 представлены наблюдаемый временной ряд, гистограмма его одномерного распределения и оценка корреляционной функции. На этих же рисунках представлены реализация y_n, n = 1, …, 10 000, квазигауссовской модели сетевого трафика, построенной по наблюдаемой выборке, и соответствующие статистические характеристики модельного ряда. Видно, что квазигауссовская модель достаточно хорошо передает одномерное распределение и корреляционную структуру временного ряда.



а *б*

Рис. 2. Реализация сетевого трафика в байтах: наблюдаемая (*а*) и смоделированная (*б*). Фрактальные размерности для наблюдаемого и смоделированного процессов равны соответственно 1.79 и 1.8



а *б*

Рис. 3. Гистограммы смоделированного (*а*) и наблюдаемого (*б*) временных рядов

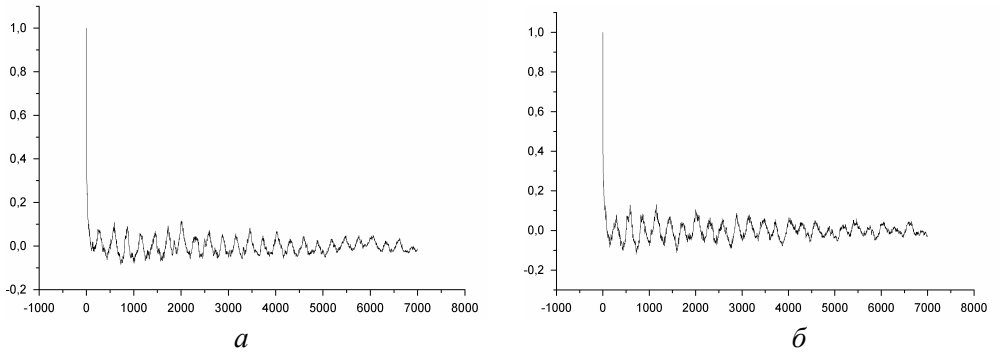


Рис. 4. Автокорреляционные функции наблюдаемого (*а*) и смоделированного (*б*) временных рядов

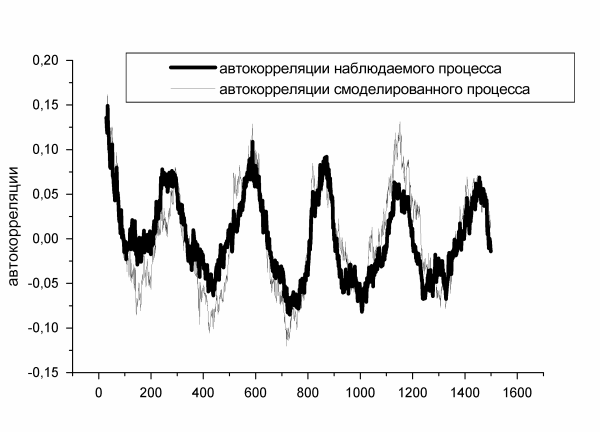


Рис. 5. Участки автокорреляционных функций наблюдаемого и смоделированного временных рядов

Одним из существенных показателей сетевого трафика считается его фрактальная размерность (см., например, [4–6], а также проект «Self-Similarity h.u.», представленный по адресу http://www.teletraffic.ru/). Для оценки фрактальной размерности наблюдаемых рядов был использован так называемый дисперсионный метод, обоснованный для случайных процессов со стационарными приращениями в работе [14]. Значения фрактальной размерности наблюдаемого ряда и нескольких реализаций квазигауссовской модели представлены ниже.

Статистика наблюдаемой и модельных реализаций сетевого трафика

Статистика	Наблюдаемый ряд	Четыре модельных ряда
Среднее	$4{,}649 \cdot 10^7$	$4{,}730 \cdot 10^7$; $4{,}556 \cdot 10^7$; $4{,}654 \cdot 10^7$; $4{,}856 \cdot 10^7$
Дисперсия	$2{,}4731 \cdot 10^{15}$	$2{,}682 \cdot 10^{15}$; $2{,}252 \cdot 10^{15}$; $2{,}405 \cdot 10^{15}$; $2{,}617 \cdot 10^{15}$
Фрактальная размерность	1,79	1,80; 1,80; 1,81; 1,77

В заключение следует еще раз отметить, что принятое в данной работе предположение о стационарности и эргодичности процесса использовалось нами для упрощения задачи. В дальнейшем в модели целесообразно учитывать более сложные временные зависимости параметров распределений и корреляционных связей реального трафика, например их суточную и недельную периодичность.

Список литературы

1. *Rodionov A. S.*, *Choo H.*, *Youn H. Y.* Process Simulation Using Randomized Markov Chain and Truncated Marginal Distribution // Supercomputing. 2002. No. 1. P. 69–85.

2. *Gallardo J. R.*, *Makrakis D.*, *Orozco-Barbosa L.* Fast Simulation of Broadband Telecommunications Networks Carrying Long-Range Dependent Bursty Traffic // Proc. of the 1999 Winter Simulation Conference. N. Y.: Pergamon Press, 1999. P. 374–381.

3. *Harmantzis F. C.*, *Hatzinakos D.*, *Lambadaris I.* Effective Bandwidths and Tail Probabilities for Gaussian and Stable Self-Similar Traffic // Proc. of the IEEE International Conference on Communications, 11–15 May 2003. Anchorage, USA, 2003. Vol. 3. P. 1515–1520.

4. *Self-Similar* Network Traffic and Performance Evaluation / Eds. K. Park, W. Willinger. N. Y.: John Wiley and Sons, 2000.

5. *Leland W. E.*, *Taqqu M. S.*, *Willinger W.*, *Wilson D. V.* On the Self-Similar Nature of Ethernet Traffic (Extended Version) // IEEE/ACM Transactions of Networking. 1994. Vol. 2 (1). P. 1–15.

6. *Городецкий А. Я.*, *Заборовский В. С.* Информатика. Фрактальные процессы в компьютерных сетях. СПб.: Изд-во СПбГТУ, 2000.

7. *Шокин Ю. И.*, *Никульцев В. С.*, *Стубарев В. М.*, *Шабальников И. В.*, *Белов С. Д.* Изучение связности потоков данных между сетевыми абонентами в целях обеспечения безопасности корпоративной СПД СО РАН // Вычислительные технологии. 2008. Т. 13, спец. вып. 2. С. 100–107.

8. *Михайлов Г. А.*, *Войтишек А. В.* Численное статистическое моделирование. Методы Монте-Карло. М.: Изд. центр «Академия», 2006. 368 с.

9. *Ogorodnikov V. A.*, *Prigarin S. M.* Numerical Modelling of Random Processes and Fields: Algorithms and Applications. VSP, Utrecht, 1996. 240 p.

10. *Пригарин С. М.* Методы численного моделирования случайных процессов и полей. Новосибирск: Изд-во ИВМиМГ СО РАН, 2005. 259 с.

11. *Пригарин С. М.*, *Маршак А. Л.* Численное моделирование векторных полубинарных однородных случайных полей и имитация разорванной облачности // Сибирский журнал вычислительной математики. 2008. Т. 11, № 3. С. 347–356.

12. *Михайлов Г. А.* Приближенные модели случайных процессов и полей // Журн. вычисл. математики и мат. физики. 1983. Т. 23, № 3. С. 558–566.

13. *Prigarin S.M.* Spectral Models of Random Fields in Monte Carlo Methods. VSP, Utrecht, 2001. 198 p.

14. *Пригарин С. М.*, *Хан К.*, *Винклер Г.* Сравнительный анализ двух численных методов для оценки хаусдорфовой размерности дробного броуновского движения // Сибирский журнал вычислительной математики. 2008. Т. 11, № 2. С. 202–218.

Материал поступил в редколлегию 13.08.2008

S. D. Belov, S. V. Lomakin, V. A. Ogorodnikov, S. M. Prigarin, A. S. Rodionov, L. B. Chubarov

Analysis and Simulation of the Traffic in High Performance Computer Networks

The paper deals with numerical methods to simulate time series of the network traffic on the basis of nonlinear transformations of Gaussian random processes. Fractal dimension of the real and simulated time series was analyzed. It was shown that the proposed methods enable to reproduce one-dimensional distributions, correlations, and fractal dimension of the observed time series.

Keywords: network traffic, numerical modeling of time series, nonlinear transformations of Gaussian processes, fractal dimension.