

ПРИМЕНЕНИЕ МОДЕЛЕЙ ТРАФИКА ДАННЫХ ДЛЯ МОНИТОРИНГА КОМПЬЮТЕРНЫХ СЕТЕЙ СИСТЕМЫ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ

В работе рассмотрены характеристики трафика данных в вычислительных сетях современных автоматизированных и компьютеризованных систем УВД. Проанализированы статистические модели трафика данных, даны рекомендации по выбору характеристик и структуры сетей.

Введение

В данной работе рассматриваются принципы построения и особенности методов передачи разнородных данных в информационно-управляющих системах критичного применения (ИУС КП). Такие системы работают в экстремальных условиях, в агрессивных средах, непрерывно в течение всего периода эксплуатации управляемого объекта. Как правило, информационный обмен в ИУС КП должен осуществляться в реальном времени. Поэтому требования к надежности, живучести и производительности сетей передачи данных в ИУС КП значительно выше, чем в обычных производственных или коммерческих системах. К ИУС КП относят специальные авиационные и ракетно-космические, транспортные, энергетические и некоторые другие системы. Безусловно, и системы управления воздушным движением являются системами критичного применения.

Основной задачей оптимизации вычислительных сетей является поддержание на требуемом уровне характеристик производительности и пропускной способности сети в условиях колебаний нагрузки на сеть. В настоящее время интенсивность трафика может изменяться в десятки раз, поэтому задачи оптимизации необходимо решать в реальном масштабе времени.

Прежде всего, необходимо сформулировать *критерии эффективности* работы сети. Чаще всего такими критериями служат производительность и надежность, для которых в свою очередь требуется выбрать конкретные показатели оценки, например, время реакции и коэффициент готовности соответственно.

Кроме того, необходимо определить множество *варьируемых параметров* сети, прямо или косвенно влияющих на критерии эффективности. Все варьируемые параметры долж-

ны быть сгруппированы в однородные подмножества. Параметрами настройки могут быть как устройства, так и протоколы или технологии передачи данных.

Необходимо также определить *пороги чувствительности* и наборы ограничений для критериев эффективности. Так, производительность сети можно оценивать на логическом уровне: "Работает"/ "Не работает", и тогда оптимизация сводится к диагностике неисправностей и приведению сети в любое работоспособное состояние. Другим крайним случаем является тонкая настройка сети, при которой параметры работающей сети (например, размер кадра или величина окна неподтвержденных пакетов) могут варьироваться с целью повышения производительности (например, среднего значения времени реакции) хотя бы на несколько процентов. Как правило, под оптимизацией сети понимают некоторый компромиссный подход. Требуется выбирать такие значения параметров сети, чтобы показатели ее эффективности, как минимум, были не ниже предельно допустимых, задаваемых при выборе глобального уровня качества сервиса *QoS*.

Таким образом, можно предложить три последовательных этапа управления сетью.

1. Приведение сети в работоспособное состояние, что обычно включает:

- поиск неисправных элементов сети - кабелей, разъемов, адаптеров, компьютеров;
- проверку совместимости оборудования и программного обеспечения;
- выбор корректных значений ключевых параметров программ и устройств, при которых обеспечивается передача данных между узлами сети - адресов сетей и узлов, используемых протоколов, типов кадров, пакетов и т.п.

2. Грубая настройка - выбор параметров, заметно влияющих на характеристики сети. Если сеть работоспособна, но обмен данными происходит очень медленно (время ожидания неприемлемо) или же сеансы связи часто прерываю то необходимо искать некие ключевые факторы ухудшения работы сети. Обычно причины заметного снижения производительности сети или неустойчивой работы сети кроются в неверно работающем элементе или некорректно установленном параметре, но из-за большого количества возможных виновников может потребоваться длительное наблюдение за работой сети, сбор статистики и перебор вариантов. Здесь также обычно задается некоторое пороговое значение показателя эффективности и требуется найти такой вариант сети, у которого это значение было бы не хуже порогового.

3. Точная настройка параметров сети – собственно оптимизация. В случае нормально работающей сети дальнейшее повышение ее качества обычно требует нахождения некоторого оптимального сочетания значений большого количества параметров. Ясно, что в реальных условиях достаточно найти решение, близкое к оптимальному, т.е. некоторый рациональный вариант структуры и параметров сети.

Роль моделирования в решении задачи выбора параметров и структуры сети

Поиск рационального варианта сети – процедура чаще всего неформальная, так как она связана с выбором слишком большого и очень разнородного множества параметров сети – типов применяемого коммутационного оборудования, серверов, терминальных узлов, типов операционных систем, параметров этих операционных систем, стеков коммуникационных протоколов, их параметров и т.д. и т.п. Очень часто мотивы, влияющие на выбор "в целом", то есть выбор типа или модели оборудования, стека протоколов или операционной системы, не носят технического характера, а принимаются из других соображений – коммерческих, "политических" и т.п. Поэтому формализовать постановку задачи оптимизации в таких случаях затруднительно. Здесь основное внимание уделяется этапам мониторинга и анализа сети, как более формальным и автоматизируемым процедурам.

На сегодняшний день как эффективное управление работой существующей сети, так

и создание проекта новой невозможно без детального моделирования ее работы. Целью моделирования является определение оптимальной топологии, адекватный выбор сетевого оборудования, определение рабочих характеристик сети и возможных этапов ее развития.

При исследованиях сетей применяют как аналитические модели, так и имитационное моделирование. При имитационном моделировании используются либо готовые специализированные программные системы, в которых процесс создания модели упрощен, либо составляются программы на универсальных языках программирования. В первом случае программные системы сами генерируют модель сети на основе исходных данных о ее топологии и используемых протоколах, об интенсивностях потоков запросов между компьютерами сети, протяженности линий связи, о типах используемого оборудования и приложений. Программные системы моделирования могут быть узко специализированными и достаточно универсальными, позволяющие имитировать сети самых различных типов.

Системы имитационного моделирования обычно включают также набор средств для подготовки исходных данных об исследуемой сети - предварительной обработки данных о топологии сети и измеренном трафике. Кроме того, система снабжается средствами для статистической обработки полученных результатов моделирования. Последний этап моделирования должен включать в себя сравнение расчетных результатов с экспериментальными данными, полученными для реальной сети. Качество результатов моделирования в значительной степени зависит от точности исходных данных о сети, переданных в систему имитационного моделирования. Однако следует заметить, что применение средств имитационного моделирования может быть полезно в основном для прогнозирования работы уже существующей сети. Определение характеристик сети еще на стадии проектирования можно осуществить при помощи аналитического моделирования.

При построении аналитических моделей сеть и все протекающие в ней процессы представляются совокупностью математических соотношений. При выводе таких соотношений приходится пренебрегать некоторыми деталями или факторами.

Адекватными моделями сетей передачи цифровых данных принято считать системы

массового обслуживания [1]. Такие модели являются достаточно универсальным математическим аппаратом, позволяющим осуществлять выбор альтернативных вариантов, расчет и оптимизацию характеристик на этапе проектирования сети. При разработке модели учитывается закон распределения потоков заявок, процесса обслуживания, число серверов, максимальный размер очереди, число клиентов в сети, схема работы буфера и другие характеристики. Основными искомыми характеристиками обычно являются производительность сети и средняя задержка пакетов.

Большое значение имеет и широко используется при анализе и проектировании компьютерных сетей классическое выражение для нахождения среднего времени пребывания пакета в сети, выведенное Клейнроком. При нахождении этой величины предполагается, что длина пакета выбирается независимо в соответствии с плотностью распределения:

$$f(x) = b \exp(-bx),$$

где $l_{\text{пб}} = 1/b$ – средняя длина пакета, измеряемая в битах (байтах); процесс поступления пакетов в сеть является пуассоновским с параметром Λ_r (пакетов/с), где r – номер пары “узел-источник – узел-адресат”; объемы буферных накопителей не ограничены и подтверждение об успешной доставке передается мгновенно. Тогда среднее время пребывания пакета в сети равно:

$$\bar{D} = \frac{\lambda[\bar{S}^2 + (4e + 2)\tau\bar{S} + 5\tau^2 + 4e(2e - 1)\tau^2]}{2(1 - \lambda[\bar{S} + \tau + 2e\tau])} - \frac{(1 - e^{-2\lambda\tau})(e + \lambda\tau - 2\lambda\tau e)}{\lambda e[F(\lambda)e^{-(1+\lambda\tau)} + e^{-2\lambda\tau} - 1]} + 2\tau e + \bar{S} + \tau/3,$$

где e – основание натурального логарифма; τ – задержка распространения сигнала в сети; \bar{S} и \bar{S}^2 – соответственно первый и второй моменты распределения передачи или обслуживания сообщения;

$f(\lambda)$ – преобразование Лапласа для распределения времени передачи сообщения.

$$\text{Следовательно } F(\lambda) = \int_0^{\infty} f(t)e^{-\lambda t} dt, \text{ а}$$

для сообщений постоянной длины $f(\lambda) = e^{-p}$

$$T = \sum_{i=1}^M \frac{\lambda_i}{bC_i - \lambda_i},$$

где:

λ_i – общий поток пакетов, поступающих в i -й канал;

$1/b$ – средняя длина пакета, измеряемая в битах(байтах);

C_i – пропускная способность i -го канала, измеряемая в бит/с.

При этом необходимо учитывать следующее принципиальное ограничение на применимость данной формулы. При ее выводе предполагалось, что процесс поступления заявок считается стационарным и эргодическим. Естественно, для реального трафика, циркулирующего в сетях систем критичного применения, справедливость такого допущения должна проверяться и уточняться, иначе получаемые оценки могут быть неоправданно оптимистичными.

Примером аналитической модели, разработанной для конкретной топологии сети, может быть модель для сетей *Ethernet* [2]. При ее разработке предполагается, что сеть состоит из бесконечного числа станций, соединенных каналами с доменным доступом. То есть станция может начать передачу только в начале какого-то временного домена. Распределение сообщений подчиняется закону Пуассона с интенсивностью λ . Тогда среднее значение времени ожидания для таких сетей составляет:

$\bar{S}^2 = \bar{S}^2$, где $\pi = \lambda\bar{S}$. Для экспоненциального распределения длин сообщений:

$$F(\lambda) = \frac{1}{1 + \rho}, \quad \bar{S}^2 = 2\bar{S}^2.$$

Однако использование классических аналитических моделей также не может считаться идеальным решением проблемы, поскольку такие модели полностью не в состоянии отобразить сложные процессы, протекающие в компьютерных сетях, а также основываются на ряде предположений и допущений.

Математические модели сетевого трафика систем критичного применения

Особое внимание, на наш взгляд, следует уделить анализу и моделированию трафика сети. Классическими моделями информационных потоков принято считать: пуассоновский (простейший) входящий поток, поток Эрланга порядка r , модели потока Эрланга для дробных r , описываемые гамма-распределением. Однако, основываясь на результатах многочисленных экспериментальных исследований, проведенных в последнее время, можно утверждать, что трафик современных цифровых телекоммуникационных и компьютерных сетей обладает особой структурой [3]. Особенности, о которых идет речь, принято называть проявлением эффекта самоподобия трафика. Это свойство проявляется на практике в том, что статистические характеристики трафика как бы «масштабируются» при усреднении за разные отрезки времени. Физически это объясняется эффектами группирования трафика: пакеты, принадлежащие одному и тому же набору данных большой длительности, поступают на узел коммутации или на терминальный узел не случайным образом, а целой пачкой. Описанное явление значительно ухудшает характеристики при прохождении самоподобного трафика через сеть даже в случаях, когда средняя интенсивность трафика намного ниже потенциально достижимой скорости передачи в данном канале, поскольку приводит к потерям пакетов из-за ограниченности буфера, рассчитанного по классическим методикам и, соответственно, увеличиваются задержка в сети, джиттер.

Для учета свойств самоподобия трафика предлагается, например, метод, суть которого заключается во введении коэффициента самоподобия (так называемого параметра Херста) и некоторых функций масштаба $f(H)$. Подставляя в выражения выходных характеристик системы вместо интенсивности λ простейшего потока $\lambda f(H)$ с подходящим подбором $f(H)$, можно обеспечить приемлемую точность описания системы, и, соответственно, возможность использования традиционных методов моделирования трафика.

Самоподобный трафик моделируется с помощью статистически самоподобных процессов. В роли таких процессов могут быть предложены два основных класса моделей [4]. Пе-

рвый – фрактальные точечные процессы (*FSNDP*, *ON/OFF*), которые оперируют с потоками единичных пакетов и непрерывным временем. Во втором случае агрегированный трафик рассматривается как случайный процесс дискретного времени $\{X_t\}$, значениями (отсчетами) X_t которого является число либо суммарный объем пакетов, поступивших от источника на t -м единичном интервале времени.

Фрактальный точечный процесс, называемый также процессом *FSNDP*, относится к классу дважды стохастических пуассоновских процессов. Переменная во времени интенсивность этого процесса задается непрерывным случайным процессом – фрактальным дробовым шумом, который получается путем фильтрации классического пуассоновского процесса.

Процесс *FSNDP* полностью определяется набором из пяти параметров: (μ , β , K , A , B), имеющих следующий смысл.

Первичный пуассоновский поток $\{t_i\}$ с постоянной интенсивностью μ служит входом для линейного фильтра с импульсной функцией

$$h(t) = \begin{cases} Kt^{-\beta}, & t \in (A, B) \\ 0, & t \notin (A, B) \end{cases},$$

где β определяется степенью самоподобия процесса, A , B – неотрицательные ограничивающие параметры, K – положительная константа, определяющая амплитуду результирующего процесса. Фильтр порождает фрактальный дробовой шум:

$$I(t) = \sum_{i=-\infty}^{\infty} h(t - t_i),$$

рассматриваемый как переменная интенсивность для второго пуассоновского точечного процесса, выходом которого является поток *FSNDP* (рис.1).

Параметр β определяется степенью самоподобия процесса и связан с параметром Херста H :

$$H = 3/2 - \beta.$$

Процесс обладает устойчиво самоподобными свойствами при условии $A \ll B$ и A , достаточно близком к нулю. В практических моделях обычно принимается, что $A=0 \dots 0,1$, а $B \leq 10$.

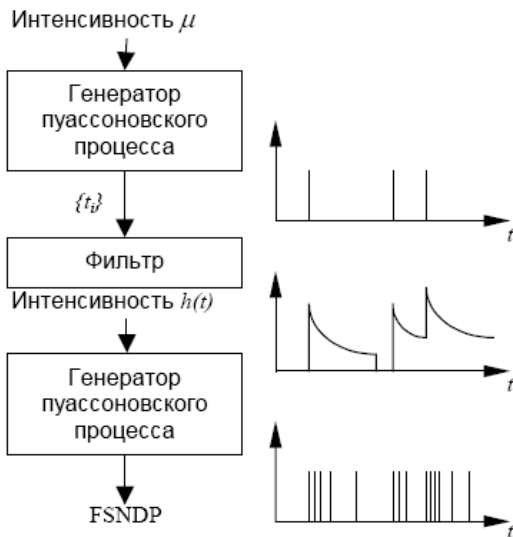


Рис.1. Составляющие процесса FSNDP

Как отмечалось выше, для моделирования трафика используется также режим *ON/OFF*. В этом случае трафик моделируется с помощью комбинации источников, которые его генерируют. Каждый источник в течение некоторого периода времени генерирует пакеты данных (так называемые *ON*-периоды), при этом внутри одного периода пакеты приходят с одинаковыми интервалами между ними. После *ON*-периода следует *OFF*-период, когда источник не генерирует пакеты. В это время подключается другой источник. Размер *ON*- и *OFF*-периодов является случайной величиной, которая должна иметь конечное математичес-

кое ожидание и бесконечную дисперсию. Например, длительность *ON*- и *OFF*-периодов является случайной величиной, и может быть распределённой по закону Парето: $W(x) = cx^{-c-1}$. Здесь c – параметр формы, обычно лежащий в пределах от 1 до 2.

Второй метод основывается на моделировании фрактального гауссовского шума ФГШ (или, как вариант, фрактального броуновского движения ФБД) [5].

При моделировании сетевого трафика с долговременной зависимостью может использоваться классическое распределение Парето. Такие модели достаточно адекватно описывают, например, пульсации данных, отличительной особенностью которых при исследовании долговременной зависимости является наличие так называемых «тяжелых хвостов» кривой распределения, для которых функция распределения при больших значениях случайной величины эквивалентна $cx^{-\alpha}$, $0 < \alpha < 2$ – индекс «хвоста» (хвост распределения затухает не по экспоненциальному, а по гиперболическому закону).

Результаты моделирования

Графики были построены для различных параметров Херста. На рис. 2 представлен график последовательности с параметром Херста $H = 0,7$.

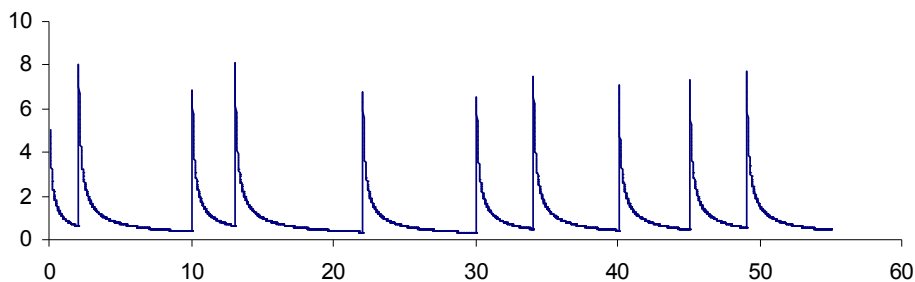
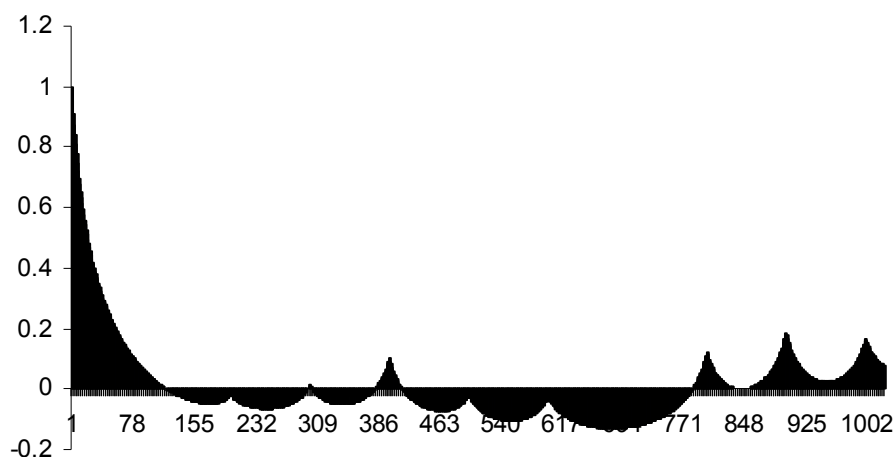
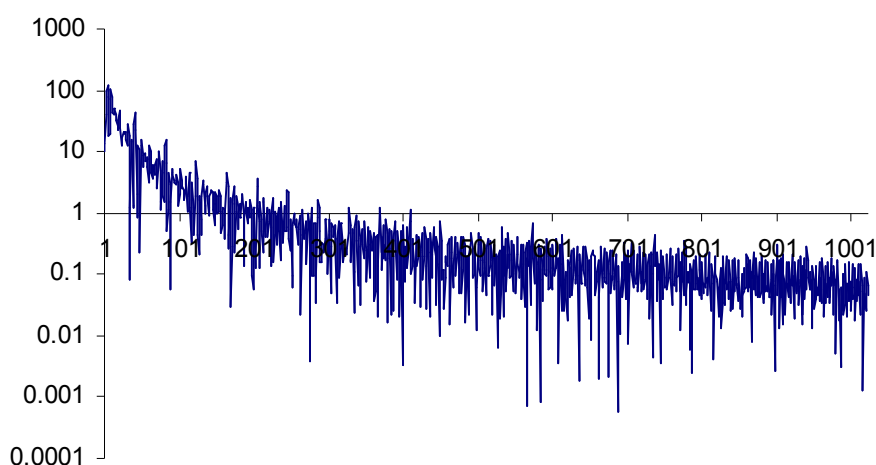


Рис 2. Модель процесса FSNDP

Графики нормированной автокорреляционной функции и спектральной плотности процесса изображены на рис. 3 и 4 соответственно.

Полученная путем моделирования спектральная плотность (рис. 4) имеет сходный вид с экспериментально полученными спектрами реализаций трафика [6].

Используя такие модели трафика, можно получать репрезентативные сравнительные характеристики производительности сетей при различном характере данных (например, оцифрованная речь, компьютерные данные, цифровое видео и т.д.) и обоснованно выбирать параметры сетевого оборудования систем критичного применения, в том числе систем УВД.

Рис 3. График автокорреляционной функции процесса *FSNDP*.Рис 6. Спектральная плотность процесса *FSNDP*.

Список литературы

1. Вишнеvский В.М. Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003. – 512 с.
2. S.S. Lam: "A Carrier Sense Multiple Access Protocol for Local Networks," Computer Networks, vol. 4, n. 1, January 1980. – P. 21–32.
3. Столлингс В. Современные компьютерные сети. 2-е издание. – СПб.: Питер, 2003. – 783 с.
4. Городецкий А.Я., Заборовский В.С. Информатика. Фрактальные процессы в компьютерных сетях / СПб.: СПбГТУ, 2000. – 102 с.
5. О.И. Шелухин, А.В. Осин. Исследование самоподобной структуры трафика Ethernet // Вестник МГУ С. Серия: Радиоэлектроника и информатика. Тематический выпуск "Современные технологии в радио и телекоммуникациях". Сб. науч. тр. – М.: МГУ, 2002. – С. 12–27.
6. W. Leland, M. Taqqu, W. Willinger, and D. Wilson. On the Self-Similar Nature of Ethernet Traffic (Extended Version), IEEE/ACM Transactions on Networking, 2(1), February 1994. – P. 1–15.