

6. ETSI TS 188 001: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN management; OSS Architecture Release 1. July, 2005. V.0.2.9. // Режим доступа [<http://pda.etsi.org/pda/AQuery.asp>]
7. ETSI TR 188 004: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Management; OSS vision. May, 2005. V.1.1.1. // Режим доступа [<http://pda.etsi.org/pda/AQuery.asp>]
8. ITU-T Recommendation M.3050.2 Enhanced Telecom Operations Map (eTOM). Process decompositions and descriptions (06/2004). Geneva, 2005. – 104 p.
9. ITU-T Recommendation M.3050 Enhanced Telecom Operations Map (eTOM). Supplement 1: ITIL application note (05/2004). Geneva, 2005. – 29 p.
10. Старыгин А. ЦОД нового поколения: особенности, модель зрелости, технологии, архитектура // Adaptive world (Инфраструктурные решения компании НР). 2007. №3 – с. 12-23.
11. Брукс П. Метрики для управления ИТ-услугами. Пер. с англ. М.: Альпина Бизнес Букс, 2008. – 283 с.
12. Саати Т., Кернс К. Аналитическое планирование. Организация систем. Пер. с англ. М.: Радио и связь, 1991. – 224 с.
13. Гребешков А.Ю. Разработка метода эффективного использования канального ресурса при развитии междугородной телефонной сети / Автореф. дисс. к.т.н. МТУСИ, 1996. – 18 с.

УДК 004.7:004.94

МОДЕЛИРОВАНИЕ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ НАУЧНО-ПРОИЗВОДСТВЕННОГО ОБЪЕДИНЕНИЯ НА УРОВНЕ ПРИЛОЖЕНИЙ

Тронин В.Г.

Описан программный продукт, моделирующий вычислительную сеть на прикладном уровне (ПП МВСПУ). Данный программный продукт реализует раскрашенные сети Петри, собственные математические модели загрузки узлов.

Введение

Научно-производственное объединение (НПО) характеризуется уникальностью процессов управления при реализации производственного цикла от замысла, проектирования до изготовления, испытаний опытного образца и до организации мелкосерийного производства наукоемкой продукции. Большой объем доработок, изменений и разнотипность обрабатываемой информации – типичные черты НПО, которые делают неизбежной высокую сложность информационной системы и сопряжение различных форматов данных и автоматизированных систем.

Для моделирования вычислительной сети НПО была использована теория сетей Петри, несомненным достоинством которых является математически строгое описание модели. Это позволяет проводить анализ с помощью современной вычислительной техники [1-2].

1. Функции информационной системы моделирования вычислительных сетей на основе сетей Петри

На основе математического аппарата сетей Петри был реализован ПП МВСПУ с применением пользовательского графического интерфейса.

ПП МВСПУ в своем составе имеет два основных инструментария: инструментарий моделирования вычислительных сетей и инструментарий сетей Петри.

Функциями инструментария сетей Петри являются:

- представление моделей узлов вычислительной сети на основе сетей Петри;
- дискретное моделирование работы отдельных узлов вычислительной сети и отображение результатов в виде графиков.

Функциями инструментария моделирования вычислительных сетей являются:

- представление топологии вычислительной сети;
- ведение библиотек элементов сети, моделей, программных продуктов;
- экспорт и импорт узлов вычислительной сети через формат XML;
- экспорт топологии вычислительной сети в формат Visio;

- дискретное моделирование работы вычислительной сети и отображение результатов в виде графиков.

2. Инструментарий сетей Петри

Одно из основных достоинств аппарата сетей Петри заключается в том, что они могут быть представлены как в графической форме (что обеспечивает наглядность), так и в аналитической (что позволяет автоматизировать процесс их анализа) [3].

Цвет в раскрашенной сети Петри описывает тип передаваемой или хранимой информации [4]. В реализованном ПП МВСПУ используются три простых цвета: *mac*, *data*, *load* и один составной – *frame*. Цвет *mac* – адрес узла сети, цвет *data* – элемент данных, передаваемый по сети.

Фрейм (*frame*) содержит:

- адрес источника, адрес-получателя (*mac*),
- данные запроса, данные ответа (*data*),
- коэффициенты загрузки запросом процессора, оперативной памяти, жесткого диска, видеопамяти (*load*),
- коэффициенты загрузки ответом процессора, оперативной памяти, жесткого диска, видеопамяти (*load*).

Ограничения для позиции могут задаваться определением максимального числа фишек в позиции и определением максимального объема информации, передаваемой через определенную переменную.

Порты в описываемом инструментарии сетей Петри служат для организации связи между элементами моделируемой вычислительной сети, линиями связи могут быть соединены только с переходом. В каждой модели элемента вычислительной сети должен присутствовать хотя бы один порт.

Линии связи в рассматриваемом инструментарии могут быть двух видов: однонаправленные и двунаправленные. На рис. 1 представлен фрагмент сети Петри, состоящий из двух позиций (*LAN* и *Buffer*) и одного перехода (*Receive*), однонаправленных линий связи. При срабатывании перехода фишка из позиции *LAN* переходит в позицию *Buffer*.

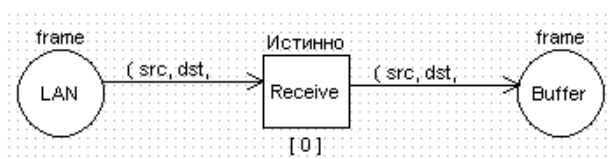


Рис. 1. Вариант применения однонаправленной линии связи

Для каждой линии связи необходимо определить переменную или набор переменных (со-

ответственно для фишек простого цвета и составного цвета). Поскольку для каждой позиции определяется тип фишек, то при редактировании переменных, относящихся к линии связи, перечень типов соответствует структуре типов для фишек в позиции, из которой исходит данная линия связи.

На рис. 2 представлен фрагмент сети Петри, в котором одна из линий связи является двунаправленной.

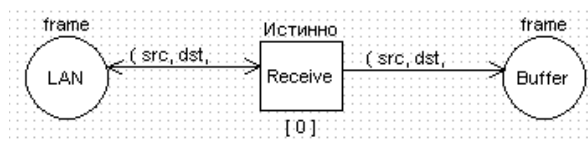


Рис. 2. Вариант применения двунаправленной линии связи

В примере, представленном на рис. 2, при срабатывании перехода *Receive* фишка попадает в позицию *Buffer*, при этом в позиции *LAN* фишка остается (в отличие от варианта с однонаправленной линией связи).

3. Примеры работы сети Петри

Рассмотрим более подробно процесс срабатывания перехода на примере фрагмента сети Петри, представленного на рис. 3.

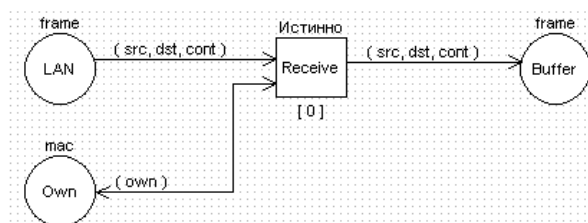


Рис. 3. Примерный фрагмент сети Петри

Данный фрагмент сети позволяет моделировать процесс выборки фреймов из локальной сети сервером. Локальная сеть представлена позицией *LAN*. В позиции *Own* хранится локальный адрес сервера, а в позицию *Buffer* помещается выбранный фрейм. Переход *Receive* на рис. 3 сработает в том случае, если во входных позициях *LAN* и *Own* будут размещаться хотя бы по одной фишке.

Пусть на первом шаге моделирования в позиции *LAN* будет находиться одна фишка *frame* = (3,5,100), в позиции *Own* – одна фишка *mac* = 5. Содержимое позиций на соответствует заданному начальному значению фишек и представлено на рис. 4.

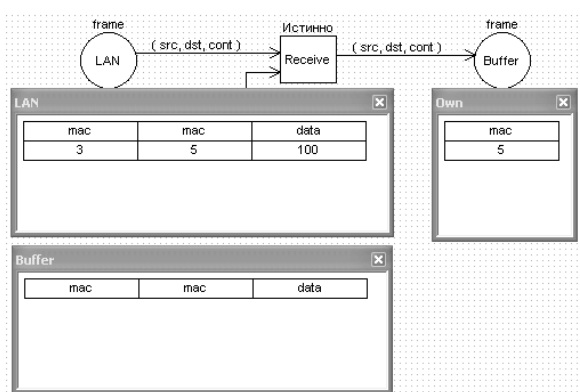


Рис. 4. Разметка сети на первом шаге моделирования

Разметка сети на втором шаге представлена на рис. 5.

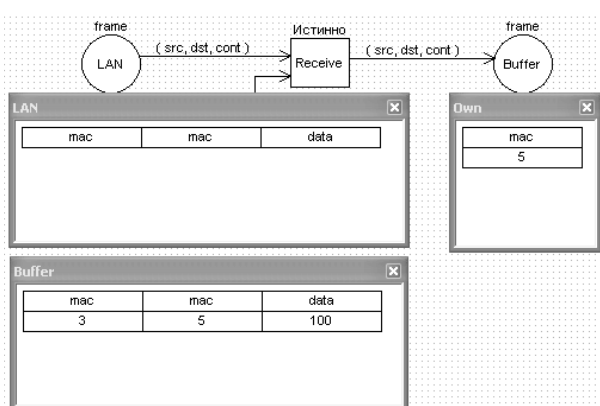


Рис. 5. Разметка сети на втором шаге моделирования

Из рис. 5 видно, что фрейм переместился из позиции LAN в позицию Buffer, а фишка в позиции Own осталась на прежнем месте.

Таким образом, если на определенном шаге моделирования фишка появляется в позиции LAN, то на следующем шаге она переходит в позицию Buffer. Для того чтобы усложнить задачу и выбирать из позиции LAN только фишки, адресованные моделируемому устройству, необходимо соответствующим образом настроить условие срабатывания перехода.

Величину задержки можно задавать двумя способами: как постоянную (не изменяется во время моделирования) и как функциональную. При выборе функциональной задержки у пользователя есть возможность определить функцию изменения величины задержки и определить параметры выбранной функции.

4. Инструментарий моделирования вычислительных сетей

Инструментарий моделирования вычислительных сетей позволяет создавать модель реальной или гипотетической вычислительной сети, применяя модели устройств, созданные на уровне инструментария сети Петри.

Информационную систему предприятия можно представить как соединенные в одно целое через компьютерную сеть технические средства с функционирующими приложениями (программные продукты, автоматизированные системы), позволяющие автоматизировать производственные процессы организации и являющиеся генераторами трафика [5-6].

Пакет, генерируемый приложением (например, CAD под операционной системой Linux) по определенному расписанию характеризуется следующими параметрами:

- размер запроса, разброс запроса, частота запроса;
- размер ответа, разброс ответа;
- коэффициенты загрузки у клиента оперативной памяти, процессора, жесткого диска, видеопамяти.

Для сервера приложения характеризуются следующими параметрами:

- тип сервера (FTP, приложений, и т.д.);
- базовая операционная система (Windows Server 2003, Linux и т.д.);
- коэффициент загрузки памяти, жесткого диска, процессора, видеопамяти.

В реальной вычислительной сети на одном аппаратном сервере могут функционировать несколько программных серверов (например, FTP-сервер и web-сервер), а ПЭВМ пользуется услугами, которые предоставляются разными автоматизированными системами.

В ПП МВСПУ с помощью раскрашенных сетей Петри для каждого типа вычислительной техники создается отдельная модель и заносится в библиотеку. Библиотека содержит набор следующих элементов вычислительной сети: серверы, рабочие станции, коммутаторы, концентраторы, маршрутизаторы, модемы, конверторы и линии связи. Сетевой трафик представлен в виде фреймов, которые генерируются клиентами сетевых автоматизированных систем.

Реализованная схема позволяет учитывать различные варианты устройств (например, ПЭВМ с несколькими сетевыми картами, несколькими процессорами, коммутатор с различным количеством портов), дополнять библиотеку вновь появляющимися типами устройств.

Для вычислительных систем (сервер, рабочая станция) создана библиотека, позволяющая для каждого типа ПЭВМ (сервера) сохранять следующие параметры: производительность, процессора, жесткого диска, оперативной памяти, видеопамяти, размер оперативной памяти.

Для проведения моделирования на уровне приложений проводится первоначальное заполнение баз

данных: клиентских сетевых приложений, программных серверов, вычислительных систем.

В базу данных серверов заносятся данные о программных серверах с коэффициентами загрузки для процессора, памяти, жесткого диска, видеопамяти сервера.

В базу данных приложений заносятся все приложения, с которыми работают пользователи на рабочих станциях с коэффициентами загрузки для процессора, памяти, жесткого диска, видеопамяти клиента, средний размер, разброс, частота запроса, средний размер и разброс ответа.

Разработанный программный комплекс на основе раскрашенных сетей Петри позволяет выполнить моделирование с использованием естественных для восприятия пользователя объектов - программных приложений и технических средств вычислительной сети.

4. Математическая модель загрузки узлов вычислительной сети на основе сетей Петри

Рассмотрим реализованные в программном продукте модели загрузки.

Условные обозначения:

- время моделирования t ;
- дискретный шаг моделирования τ_M (мс);
- величина запроса/ответа R_t (кБ);
- интервал усреднения: $\Delta t = 1$ с;
- производительность узла (эталонная): \bar{v}_g (Мбт/с);
- объем узла (эталонный) \bar{V}_g (кБ);
- коэффициент загрузки узла k_u (уровень приложений);
- коэффициент перерасчета узла k_p (технические средства).

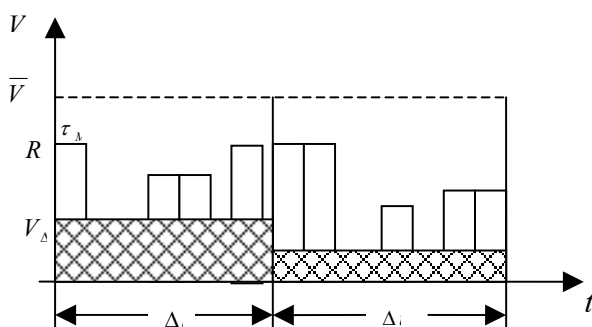


Рис. 6. Загрузка памяти эталонного узла

4.1. Модель загрузки памяти узла

Усредненное значение загрузки памяти эталонного узла (рис. 6) вычисляется по следующей формуле:

$$V_{\Delta t} = \frac{\sum_{t \in \Delta t} R_t \cdot \tau_M \cdot 10^{-3}}{\Delta t}.$$

Следовательно, загрузка памяти эталонного узла в процентах будет выглядеть следующим образом:

$$Z_{V_g} = \frac{V_{\Delta t}}{\bar{V}_g} \cdot 100\% = \frac{\sum_{t \in \Delta t} R_t \cdot \tau_M \cdot 10^{-3}}{\Delta t \cdot \bar{V}_g} \cdot 100\%.$$

Загрузка памяти неэталонного узла

$$Z_V = \frac{V_{\Delta t}}{\bar{V}_g \cdot k_p} \cdot 100\% = \frac{\sum_{t \in \Delta t} R_t \cdot \tau_M \cdot 10^{-3}}{\Delta t \cdot \bar{V}_g \cdot k_p} \cdot 100\%.$$

4.2. Загрузка узла по производительности

Время задержки перехода эталонного узла определяется следующим образом:

$$T_g = \frac{R_t}{v_g \cdot 976,5625},$$

где числовой коэффициент определяет разные единицы измерения (кБ и Мбт/с).

Из этого следует, что количество тактов

$$N_g = \frac{1,024 \cdot R_t}{v_g \cdot \tau_M}.$$

Далее определяем количество тактов задержки реального узла с реальным приложением:

$$N = \frac{1,024 \cdot R_t \cdot k_u}{v_g \cdot \tau_M \cdot k_p}.$$

Загрузка узла по производительности на основе полученной задержки

$$Z_v = \frac{\sum_{t \in \Delta t} \alpha_t \cdot \tau_M \cdot 10^{-3}}{\Delta t} \cdot 100\%,$$

где $\alpha_t = \{0,1\}$, 0 переход не активен в момент t , 1 – переход активен в момент t .

Литература

1. Бенькович Е.С., Колесов Ю.Б., Сениченков Ю.Б. Практическое моделирование динамических систем. СПб.: БХВ-Петербург, 2002. – С. 43-57.
2. Нечепуренко М.И., Попков В.К., Майнагашев С.М. и др. Алгоритмы и программы решения задач на графах и сетях. Новосибирск: Наука, 1990. – С.12-40.

3. Питерсон Дж. Теория сетей Петри и моделирования систем. Пер. с англ. М.: Мир, 1984. – С. 67-72.
4. Макаров И.М., Назаретов В.М., Кульба А.В., Швецов А.Р. Сети Петри с разноцветными маркерами // Техническая кибернетика. № 6, 1987. – С. 101-107.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2001. – С. 56-84.
6. Закер К. Компьютерные сети. Модернизация и поиск неисправностей. Пер. с англ. СПб.: БХВ-Петербург, 2003. – С. 430-478.

УДК 004.056.52

АНАЛИЗ МОДЕЛЕЙ РАЗГРАНИЧЕНИЯ ДОСТУПА, РЕАЛИЗОВАННЫХ В СОВРЕМЕННЫХ СОЦИОТЕХНИЧЕСКИХ СИСТЕМАХ

Лепешкин О. М., Харечкин П. В.

В статье рассматриваются особенности применения моделей разграничения доступа в социотехнических системах. Выполнен анализ достоинств и недостатков классических моделей и их непосредственного влияния на функциональную безопасность социотехнических систем. Предложен подход к повышению функциональной безопасности социотехнических систем, основанный на разработке новой функционально-ролевой модели разграничения доступа.

Внедрение информационных технологий в процессы производства и управления современных организаций стало объективной реальностью. Масштабы применения информационных технологий таковы, что наряду с проблемами производительности, надежности и устойчивости функционирования социотехнических систем (СТС) остро стоят проблемы обеспечения информационной безопасности (ИБ) в отношении защиты циркулирующей в системах информации от несанкционированного доступа (НСД).

Обеспечение информационной безопасности СТС осуществляется на основе систем управления доступом. Управление доступом - это определение возможности субъекта оперировать над объектом, которая в общем виде описывается рис. 1.

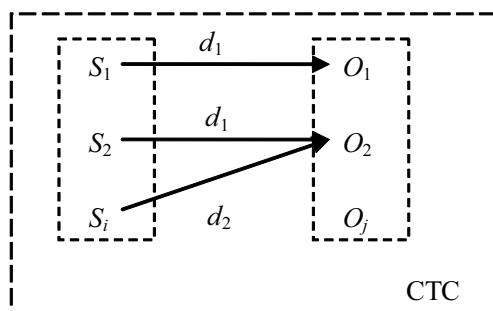


Рис. 1. Схема доступа субъектов S_i к объектам O_j СТС

Классические модели, такие как дискреционная (доверительная) и мандатная (принудительная) являются наиболее известными и распространенными на данный момент [1]. Дискреционный контроль доступа позволяет субъектам определять права доступа к объектам при условии наличия прав собственности на данные объекты. Данный подход обеспечивает гибкость и динамичность в изменении полномочий.

При всей наглядности и гибкости возможных настроек разграничительной политики доступа к ресурсам, матричным моделям присущи серьезные недостатки. Основной из них – это излишне детализированный уровень описания отношений субъектов и объектов. Из-за этого усложняется процедура администрирования системы защиты. Причем это происходит как при задании настроек, так и при поддержании их в актуальном состоянии при включении в схему разграничения доступа новых субъектов и объектов. Как следствие, усложнение администрирования может приводить к возникновению ошибок, росту количества уязвимостей и увеличению возможностей доступа к информации со стороны внешних и внутренних нарушителей.

Существенным недостатком дискреционных моделей, реализованных в СТС, следует указать и то, что в ходе функционирования структура СТС изменяется таким образом, что субъекты и объекты могут меняться местами. Так, информационные системы рассматривались ранее как объект управления, в то время как человек-пользователь являлся субъектом управления. Но при включении человека в информационную систему его роли разделились на исполнительную и управляющую. Человек-исполнитель теперь является объектом управления, а человек с ролью управления является субъектом управления СТС.