УДК 621.39, 004.7
Т. Р. ШМЕЛЁВА, канд. техн. наук, доцент,
Одесская национальная академия связи им. А. С. Попова

Анализ эффективности вычислительных решеток реентерабельными раскрашенными сетями Петри

Разработан метод моделирования вычислительных решеток реентерабельными раскрашенными сетями Петри, что позволило получить модели с инвариантной структурой и исследовать решетки большого размера под воздействием злонамеренного трафика. Результаты исследования совпадают с ранее полученными для малых размеров решеток с помощью традиционных моделей. Выявленная уязвимость вычислительных решеток стимулирует дальнейшие исследования по разработке средств противодействия атакам.

Ключевые слова: вычислительные решетки; реентерабельность; раскрашенные сети Петри; злонамеренный трафик.

Введение и постановка задачи

Раскрашенная сеть Петри (РСП) является универсальной алгоритмической системой и удобным средством моделирования телекоммуникационных сетей. РСП имеет ряд существенных преимуществ даже по сравнению с такими специализированными системами, как ns и OpNet. Преимуществами РСП, которые отмечены в [2], являются наглядность графического представления, лаконичность конструкций языка функционального программирования ML (рекурсивные функции), возможность комбинирования аналитических и имитационных методов исследования модели. Традиционный метод построения моделей предполагает прямое отображение топологии сети в структурных элементах РСП. Недостаток этого метода — необходимость перекомпоновки модели для каждой новой топологической схемы сети.

Вычислительные решетки играют ключевую роль в решении «неподдающихся» задач в различных прикладных областях, таких как ядерная физика, молекулярная генетика, структурная биология. Объединение большого количества вычислительных узлов в виртуальную структуру куба (гиперкуба), тора, шара позволяет получить решение задачи за приемлемое время. Выполнено моделирование вычислительных решеток РСП [6] и дана оценка влияния злонамеренного трафика на функционирование решетки. Однако метод прямого отображения структуры решетки в РСП позволяет исследовать сравнительно небольшие решетки, например 8×8.

Таким образом, возникает актуальная задача моделирования вычислительных решеток произвольного размера РСП, структура которых незначительно зависит или совсем не зависит от топологии сети.

Анализ литературных данных

Обзор современных вычислительных решеток представлен в [1]. Методы моделирования телекоммуникационных систем разработаны в монографии [2]. Особенности моделирования вычислительных решеток раскрашенными сетями Петри [5] представлены в [6]. Кроме того, принципы объектного моделирования излагаются в [3], основы программирования на языке ML изложены в [4]. Однако методы построения моделей вычислительных решеток с инвариантной структурой ранее не обсуждались в литературе.

Цель и задачи исследования

Целью настоящей работы является построение методов исследования вычислительных решеток произвольного размера за счет использования моделей с инвариантной структурой на основе свертки топологии при помощи переключения тегов. Для достижения данной цели решались следующие задачи:

- свертка топологии сети в массиве параметров, представленных в виде маркировки позиции РСП;
- формирование множества и структуры тегов, ассоциированных с динамическими объектами модели;
- разработка процедур переключения тегов;
- модификация и адаптация базовых элементов моделей решеток: коммуникационный узел, терминальный (абонентский) узел, генератор (пушка) злонамеренного трафика.

Модель вычислительной решетки в виде реентерабельной раскрашенной сети Петри

Модель вычислительной решетки, построенная в форме РСП, представлена в [6]. Для построения модели применен принцип прямого отображения, когда для каждого элемента решетки построена подмодель, т. е. количество подмоделей соответствует количеству элементов решетки. При этом объем модели увеличивался пропорционально размеру изучаемой решетки. Так, объем модели квадратной решетки размера 8×8 составил 4,5 Мбит, что затрудняло загрузку, тестирование и исследование свойств модели. Объем предлагаемой в этой статье модели прямоугольной вычислительной решетки [8] в виде

реентерабельной раскрашенной сети Петри (РРСП) не зависит от размерности решетки, имеет неизменное значение и составляет 750 Кбит. Термин «реентерабельность» (буквально «повторная входимость») означает способность каждого фрагмента моделировать одновременно несколько работающих устройств соответствующего типа. Модель вычислительной решетки в виде РРСП представлена на рис. 1.

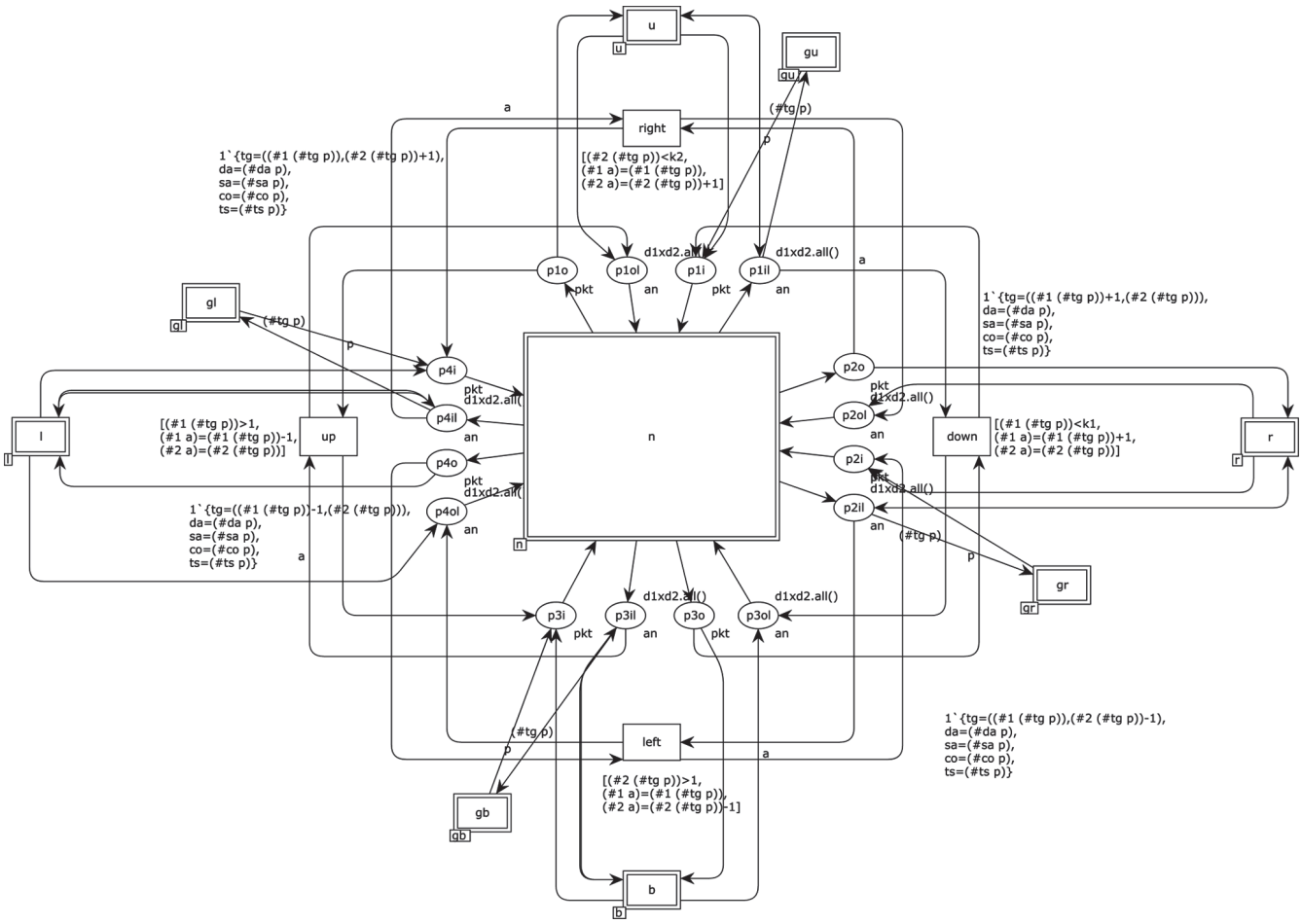

Рис. 1. Модель прямоугольной вычислительной решетки

Для создания модели применялся принцип иерархической композиции, используемой для построения сложных моделей. Подмодели решетки были представлены переходами сети Петри. Модель состоит из двух главных подмоделей: модели коммуникационного узла (*data communication equipment* — DCE) и терминального оборудования (*data terminal equipment* — DTE), а также вспомогательной подмодели, с помощью которой генерируется вредоносный трафик в сети.

Модель 4-портового коммуникационного узла представлена единичной подмоделью, описывающей все узлы решетки любой размерности. Например, на рис. 1 — переходом *n* и 16-тью совмещенными позициями, расположенными на сторонах перехода (четыре полнодуплексных порта, каждый моделируется четырьмя позициями). Так, четвертый порт представлен позициями *p4i* и *p4il*, моделирующими входной порт, а позиции *p4o* и *p4ol* моделируют соответственно выходной порт. Для решетки 8 × 8 начальная маркировка позиций ограничителей портов *p4il*, *p4ol* равна 64.

Модель терминального оборудования представлена четырьмя подмоделями, названия которых выбраны в соответствии с их краевым расположением. На рис. 1 — переходами *u* («upper» верхний), *b*, *l*, *r* и 16-тью совмещенными позициями, описанными ранее. Вспомогательные подмодели, которые используются для генерации злонамеренного трафика, показаны переходами *gu*, *gb*, *gl*, *gr*. Передачу пакетов в сети между узлами DCE и DTE моделируют переходы *up*, *down*, *left*, *right*.

Модель коммуникационного узла DCE

Рассмотрим детальнее модель 4-портового коммуникационного узла, которая описывает все узлы решетки любой размерности. Количество описываемых коммутационных узлов для решетки размерности *k1* × *k2* равно *k1*k2*, например, для решетки 8 × 8 равно 64. Модель приведена на рис. 2.

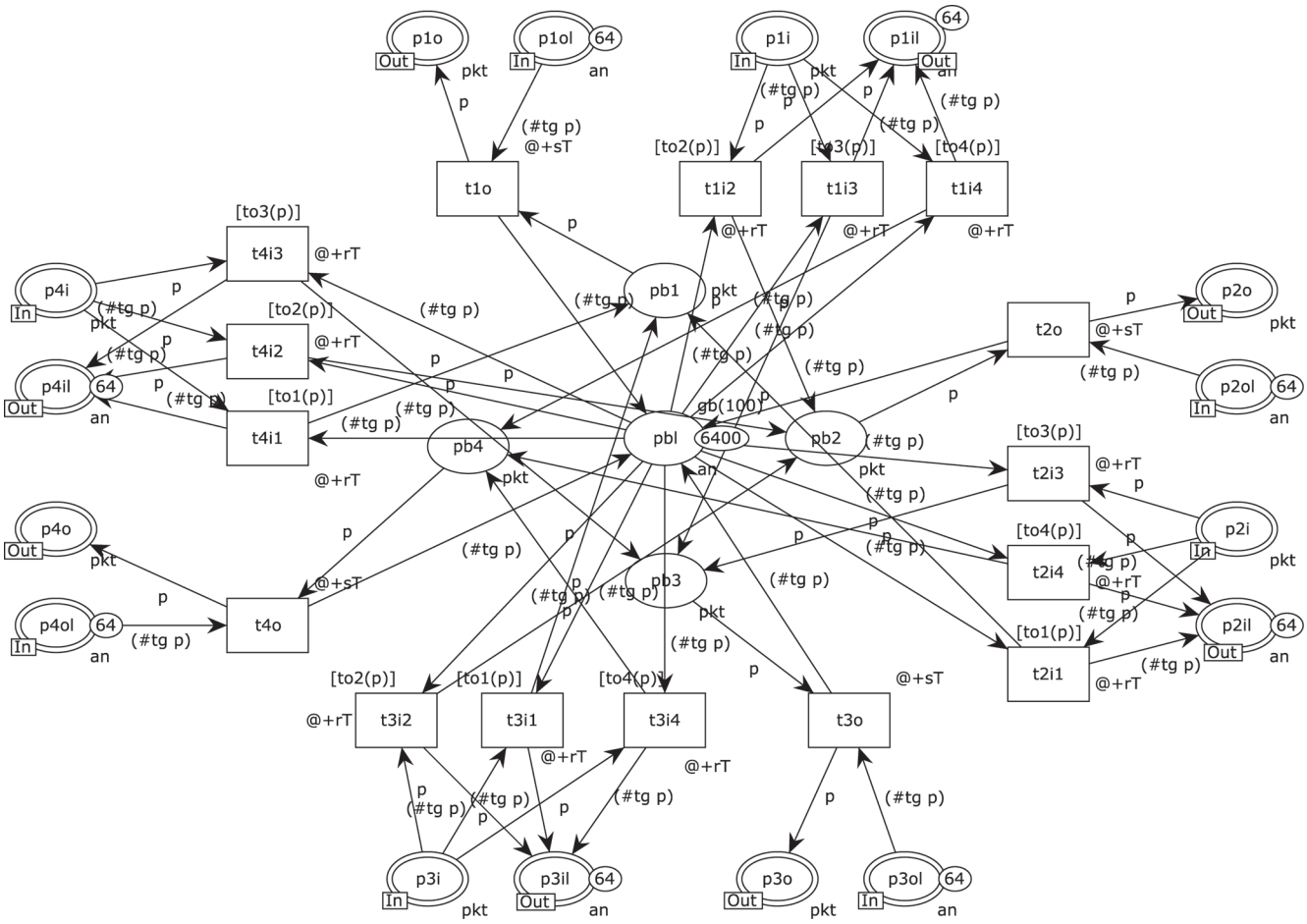

Рис. 2. Модель коммуникационного узла

Для проведения вычислительных экспериментов и оценки эффективности работы вычислительной решетки для каждого перехода модели заданы временные параметры *sT* и *rT*, представляющие временные задержки отправки и получения пакета. Для реализации алгоритма коммутации пакетов используются основные *to1(p)*, *to2(p)*, *to3(p)*, *to4(p)* и вспомогательные предикаты переадресации *fun_v1*, *fun_db4*, *fun_cb4*, *fun_nb4* и т. д., описанные в [6].

Количество контактных позиций портов, расположенных на сторонах квадрата, правила композиции решетки, которые определяют соединение каналов противоположных типов, т. е. выходной канал соединяется с входным каналом соседнего узла и наоборот, а также правила приема и отправки сообщения соответствуют описанным в [6]. Модель решетки размерности $k1 \times k2$ оптимизируется заменой всех моделей коммутационных узлов решетки, а именно *k1*k2*, одной моделью, содержащей в соответствующих позициях маркировку, равную размерности решетки. Для примера решетки 8 × 8: 64 модели коммутационных узлов заменяются одной моделью узла, в которой выполнена свертка топологии с помощью коммутации тегов, где параметром является размерность решетки, представленная маркировкой в соответствующих позициях буфера узла, входных и выходных портов.

Размер внутреннего буфера узла, или иначе маркировка позиции *pbl* рассчитывается как произведение количества узлов решетки на размер одного буфера. Например, для решетки 8 × 8 и размера внутреннего буфера одного узла 100 сообщений маркировка позиции *pbl* равна 6400.

Модель терминального оборудования DTE

В прямоугольной решетке два числа *(i, j)* используются для адресации коммуникационных узлов и терминального оборудования (*i* — номер строки; *j* — номер столбца). Таким образом, все коммуникационные узлы пронумерованы от 1 до $k1$ по вертикали, от 1 до $k2$ по горизонтали, а адрес терминального оборудования содержит только один изменяемый индекс, второй индекс одинаков для всех моделей одного типа. Например, у DTE верхнего уровня первый индекс $i = 0$, а второй j изменяется от 1 до $k2$, у DTE правого уровня первый индекс i изменяется от 1 до $k1$, второй $j = k2 + 1$. Модель DTE узла верхней краевой стороны границы представлена на рис. 3.

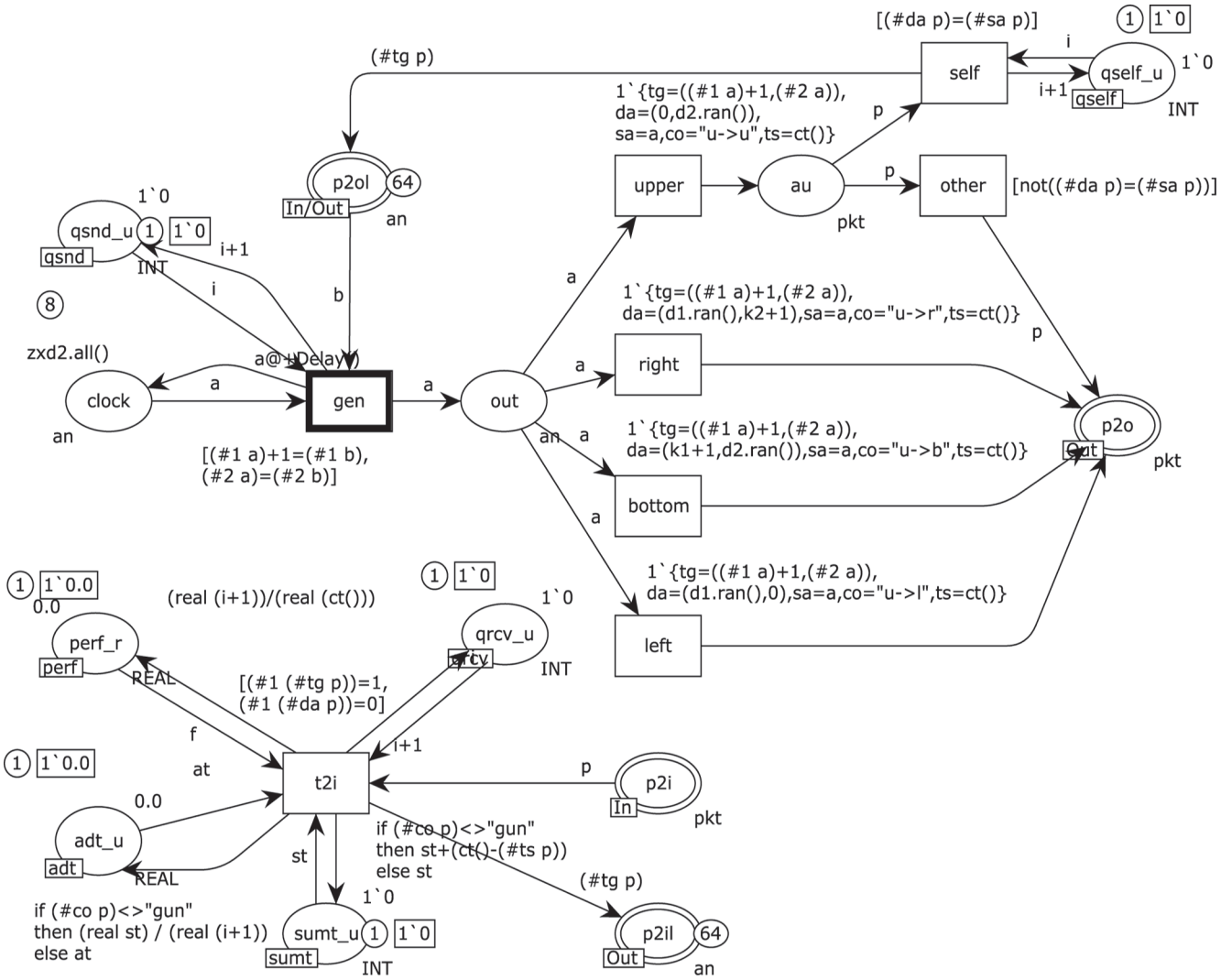

Рис. 3. Модель верхнего краевого терминального оборудования

Модель терминального оборудования состоит из двух основных частей в соответствии с простейшими функциями узла DTE — генерации и получения сообщений. Рассмотрим подробнее моделирование базовых функций терминального оборудования. Периодичность формирования пакетов описывается позицией *clock* при помощи функции *Delay( )*, которая является функцией распределения случайной переменной, в данной модели — закон распределения генерации пакетов узлом DTE. Оценка эффективности функционирования решетки зависит от функции распределения генерации трафика. В моделирующей системе CPN Tools [5] для описания пользовательских случайных функций представлен широкий диапазон известных законов распределения.

Вторым условием генерации пакета и запуска перехода *gen* является наличие фишки в позиции *p*ol*, которая обозначает, что выходной порт свободен. При срабатывании перехода *gen* счетчик количества отправленных пакетов увеличивается на единицу. Описывается этот счетчик маркировкой позиции *qsnd_**, а фишка, которая совпадает с адресом текущего узла *a*, попадает в позицию *out*. Для генерации адреса получателя при помощи функции *ran( )* выбирается случайно один из переходов *left*, *upper*, *right*, *bottom*. Например, к правой границе пакет и адрес получателя формируются следующим выражением: 1`{tg = ((#1 a) + 1, (#2 a)), da = (d1.ran(), k2 + 1), sa = a, co = "u- > r", ts = ct()}, которое содержит время отправки сообщения, описанное выражением ts = ct(). Тип *tg* описывает тег, задающий текущее положение пакета внутри решетки и представлен парой координат текущего узла. Для фильтрации пакетов с собственным адресом назначения используется переход *upper*, поскольку на рис. 3 представлена модель верхнего узла.

Переход *t*i* моделирует прием сообщений, которые не обрабатываются, а поглощаются; подсчет количества принятых сообщений (значение хранится в позиции *qrcv_**); вычисление среднего времени доставки пакета в единицах модельного времени MTU (значение находится в позиции adt_*).

Оценка эффективности решетки при разных видах нагрузки

В традиционной модели [6] исследование параметров качества обслуживания проводилось с учетом размера внутреннего буфера и производительности узла DCE, интенсивности рабочей нагрузки, описываемой распределением Пуассона. Было показано, что при малых значениях размера внутреннего буфера решетка попадает в тупик даже при трафике, который равняется 10% пропускной способности решетки. Достаточно большой буфер, например размером 10 000 и более, не позволяет наблюдать тупики даже при пиковой нагрузке. Поэтому для вычислительных экспериментов с моделью коммутации тегов выбран размер буфера, равный 100.

Результаты эксперимента для рабочей нагрузки разной интенсивности представлены в табл. 1. В качестве исследуемых параметров качества обслуживания выбраны производительность решетки и среднее время доставки пакета.

Таблица 1

Результаты вычислительного эксперимента для решетки 8 × 8 при разной рабочей нагрузке

Интенсивность рабочей нагрузки решетки 8 × 8	Шаг (Step)	Время (Time)	Производительность решетки (packets/MTU)	Среднее время доставки пакета (MTU)
90,0	10000000	1131590	0,34	78
30,0	10000000	377553	1,03	79
20,0	10000000	251396	1,54	81
10,0	10000000	126200	3,09	97
9,0	10000000	114209	3,41	121
8,0	976995*	13440	2,65	253
7,0	457478*	7550	2,07	266
6,0	333540*	5165	2,17	271
5,0	273547*	3521	2,57	264
4,0	212391*	2343	2,98	249

Результаты вычислительного эксперимента полностью совпадают с результатами, полученными в [6; 7] в пределах погрешности, что подтверждает адекватность предлагаемой реентерабельной модели, основанной на переключении тегов. Однако размерность решетки 8 × 8 является предельной для традиционной модели. При увеличении размерности решетки любая корректировка модели: добавление нового или удаление элемента, изменение значения переменных, констант или маркировки, — влечет за собой длительную (порядка 3 мин и более) синтаксическую проверку, что делает неэффективным процесс исследования решетки на оборудовании средней мощности. Время корректировки в предложенной модели не превышает нескольких секунд для решетки любой размерности. Результаты эксперимента для решетки 64 × 64 при разной рабочей нагрузке приведены в табл. 2.

Таблица 2

Результаты вычислительного эксперимента для решетки 64 × 64 при разной рабочей нагрузке

Интенсивность рабочей нагрузки решетки 64 × 64	Шаг (Step)	Время (Time)	Количество отправленных пакетов	Количество принятых пакетов	Производительность решетки (packets/MTU)	Среднее время доставки пакета (MTU)
30,0	1000000	1052	9112	3498	3,32	417
10,0	10000000	7299	62444	49485	6,78	920
4,0	1000000	325	22702	1566	4,81	165

Моделирование злонамеренного трафика, описание моделей пушек пакетов, присоединенных к границам решетки, основные характеристики пушек, которые влияют на поведение модели, а также конфигурации, для которых получены существенные результаты, — все эти вопросы изучены в [7]. Для исследования влияния злонамеренного трафика на QoS решетки остановимся на одной разновидности — на «дуэли» трафика. Выбор обусловлен тем, что данный вид трафика, создавая дополнительную нагрузку менее чем 10%, имеет меньшее влияние на качество обслуживания, маскируясь под рабочую нагрузку, однако при этом мгновенно приводит решетку в тупик. Результаты эксперимента для решетки 8 × 8 с добавлением разновидности злонамеренного трафика «дуэли» приведены в табл. 3. Решетка приходит в полный тупик при интенсивности рабочей нагрузки, в которой ранее тупик не наблюдался. Интенсивность трафика пушки $gl = 4{,}0$.

Таблица 3

Результаты вычислительного эксперимента для решетки 8 × 8 при «дуэли» трафика

Интенсивность рабочей нагрузки решетки 8 × 8	Шаг (Step)	Время (Time)	Количество отправленных пакетов	Количество принятых пакетов	Производительность решетки (packets/MTU)	Среднее время доставки пакета (MTU)
20,0	4972657	116736	192854	173260	1,48	97
10,0	995686	17470	41991	37003	2,12	132
90	782410	14192	34049	28393	2,01	143

Таким образом, результаты имитационного моделирования подтверждают возможность блокировки вычислительной решетки в условиях рабочей нагрузки при наличии злоумышленного трафика, который не превышает 10% общей нагрузки решетки, а в некоторых случаях 5% пиковой нагрузки решетки.

Выводы

Свертка топологии и построение моделей с переключением тегов позволили исследовать проблемы блокирования решеток посредством рабочего и злонамеренного трафика в среде моделирующей системы CPN Tools для решеток достаточно большого (реалистичного) размера. Было показано, что решетка, даже при низкой (около 30%) ее рабочей нагрузке, может быть блокирована с полным тупиком узлов DCE при помощи «дуэли» трафика с дополнительной нагрузкой менее чем 5%. Для малых размеров сетей результаты совпадают с ранее полученными для традиционных моделей. Таким образом, подтверждена уязвимость структур решетки к атакам злонамеренным трафиком.

Реентерабельные модели, основанные на переключении тегов, являются перспективным направлением исследования эффективности и безопасности современных технологий вычислительных решеток и облаков.

Литература

1. ***Preve, N. P.*** *Grid Computing: Towards a Global Interconnected Infrastructure / N. P. Preve.— Springer, 2011.— 312 p.*

2. ***Zaitsev, D. A.*** *Clans of Petri Nets: Verification of protocols and performance evaluation of networks / D. A. Zaitsev.— LAP LAMBERT Academic Publishing, 2013.— 292 p.*

3. ***Труб, И. И.*** *Объектно-ориентированное моделирование на языке С++ / И. И. Труб.— СПб.: Питер, 2005.— 411 с.*

4. ***Jeffrey, D.*** *Ullman. Elements of ML Programming / D. Ullman Jeffrey.— Publisher New Jersey: Prentice Hall PTR, 1997.— 383 p.*

5. ***Zaitsev, D. A.*** *Simulating Telecommunication Systems with CPN Tools: Students'book / D. A. Zaitsev, T. R. Shmeleva.— Odessa: ONAT, 2006.— 60 p.*

6. ***Оценка*** *влияния злонамеренного трафика на функционирование вычислительных решеток / [Д. А. Зайцев, Т. Р. Шмелёва, В. Ретсчитзеггер, Б. Пролл] // Радиотехника.— 2014.— Вып. 176.— С. 164–171.*

7. ***Blocking*** *Communication Grid via Ill-Intentioned Traffic / [D. A. Zaitsev, T. R. Shmeleva, W. Retschitzegger, B. Proll] // 14th Middle Eastern Simulation & Modelling Multiconference, February 3-5, 2014, Muscat, Oman.— P. 63–71.*

8. ***Shmeleva, T. R.*** *Parametric Colored Petri net model of Computing Grids / T. R. Shmeleva // 69 НТ конференция ОНАС, декабрь 3–5, 2014, Одесса.— С. 41–43.*

Рецензент: доктор техн. наук, профессор **Н. В. Захарченко,** Одесская национальная академия связи им. А. С. Попова.

Т. Р. Шмельова

АНАЛІЗ ЕФЕКТИВНОСТІ ОБЧИСЛЮВАЛЬНИХ ҐРАТ ЗА ДОПОМОГОЮ РЕЄНТЕРАБЕЛЬНИХ РОЗФАРБОВАНИХ МЕРЕЖ ПЕТРІ

Розроблено метод моделювання обчислювальних ґрат реєнтерабельними розфарбованими мережами Петрі, що дозволило отримати моделі з інваріантною структурою і досліджувати ґрати великого розміру під впливом зловмисного трафіку. Результати дослідження збігаються з раніше отриманими для малих розмірів ґрат за допомогою традиційних моделей. Виявлена уразливість обчислювальних ґрат стимулює подальші дослідження з розробки засобів протидії атакам.

Ключові слова: обчислювальні ґрати; реєнтерабельність; розфарбовані мережі Петрі; зловмисний трафік.

T. R. Shmeleva

ANALYSIS OF EFFICIENCY OF COMPUTING GRIDS BY REENTERABLE COLOURED PETRI NETS

The method for modeling computing grids by reenterable coloured Petri nets was developed, which allowed obtaining models with invariant structure and investigating the big sizegrids under the influence of ill-intentioned traffic. The research results coincide with ones obtained for the small size of arrays using traditional models. Revealed vulnerabilities of computing grids stimulate further research to develop means to counter attacks.

Keywords: computing grids; reenterablity; coloured Petri nets; ill-intentioned traffic.