Моделирование и анализ информационных систем. Т. 25, № 2 (2018), с. 193–206
Modeling and Analysis of Information Systems. Vol. 25, No 2 (2018), pp. 193–206

DOI: 10.18255/1818-1015-2018-2-193-206

УДК 004.94, 004.724.4

Сравнительный анализ устойчивости вычислительных решеток с различной архитектурой узла к индуцированным тупикам

Шмелёва Т. Р.

получена 3 сентября 2017

Аннотация. Рассматриваются классификация и области применения методов коммутации, их достоинства и недостатки. Построена модель вычислительной решетки в форме раскрашенной сети Петри с узлом, реализующим сквозную коммутацию пакетов. Модель состоит из узлов коммутации пакетов, генераторов трафика и пушек, которые формируют злонамеренный трафик, замаскированный под обычный пользовательский трафик. Исследованы характеристики модели решетки в условиях рабочей нагрузки с различной интенсивностью. Оценено влияние злонамеренного трафика типа «дуэль трафика» на параметры качества обслуживания решетки. Проведен сравнительный анализ устойчивости вычислительных решеток с узлами, реализующими технологию передачи пакетов с обязательной буферизацией, и сквозной коммутации. Показано, что производительности решеток примерно одинаковы в условиях рабочей нагрузки; а в условиях пиковой нагрузки решетка с узлом, реализующим технологию передачи пакетов с принудительной буферизацией, более устойчива. Решетка с узлами, реализующими технологию SAF, приходит к полному тупику через дополнительную нагрузку менее чем 10 процентов. После детального исследования показано, что конфигурация «дуэль трафика» не оказывает влияния на решетку с узлами cut-through при увеличении рабочей нагрузки до пиковой, при которой решетка приходит к полному тупику. Периодичность запуска пушек, генерирующих злонамеренный трафик, определена случайной функцией с пуассоновским распределением. Для построения моделей и измерений характеристик используется моделирующая система CPN Tools. Производительность решетки и среднее время доставки пакета оценивается при различных вариантах нагрузки на решетку.

Ключевые слова: безопасность вычисления на решетках, сквозная коммутация, защита против атак трафика, оценка производительности, раскрашенная сеть Петри, тупик

Для цитирования: Шмелёва Т. Р., "Сравнительный анализ устойчивости вычислительных решеток с различной архитектурой узла к индуцированным тупикам", *Моделирование и анализ информационных систем*, **25**:2 (2018), 193–206.

Об авторах:
Шмелёва Татьяна Рудольфовна, orcid.org/0000-0002-4799-3842, канд. техн. наук, доцент,
Одесская национальная академия связи им. А.С. Попова,
ул. Кузнечная, 1, г. Одесса, 65029 Украина, e-mail: tishtri@rambler.ru

Благодарности: Автор благодарит программный комитет и участников PSSV-2017 за обсуждение результатов, представленных в статье.

Введение

Сети вычислительных ресурсов [1] или вычислительные решетки (Grid Computing) решают проблемы, связанные с интенсивными вычислениями, обработкой супербольших массивов данных, что требует использования разнородных и сверхскоростных ресурсов. Не последнее место в этой системе занимают устройства передачи данных [2]: коммутаторы и маршрутизаторы. Для повышения производительности решетки и стабильности функционирования становится актуальным выбор метода коммутации пакетов [2, 3] в устройствах передачи данных.

Ранее были изучены параметры качества обслуживания и эффективность телекоммуникационных сетей [4–6] и вычислительных решеток с узлами, реализующими метод обязательной буферизации [7]. Модели были построены в форме раскрашенных сетей Петри [8]. Проведены исследования влияния злонамеренного трафика на поведение и характеристики вычислительной решетки [9], с коммуникационными устройствами типа store-and-forward. Оценка производительности решетки и среднего времени доставки пакета проведена в [10], для решеток с коммутационным устройством, реализующим сквозную коммутацию пакетов.

Целью настоящей статьи является сравнительный анализ устойчивости вычислительных решеток [7, 10] с различной архитектурой узла к индуцированным тупикам; дальнейшее развитие методов анализа прямоугольных коммуникационных решеток для узлов, реализующих сквозную коммутацию пакетов. Методы предназначены для применения при проектировании вычислительных решеток, в разработке новых телекоммуникационных устройств и в интеллектуальных системах защиты.

1. Классификация и области применения методов коммутации

В современных телекоммуникационных системах доминируют два основных метода [2, 3] пакетной коммутации: первый с обязательной буферизацией пакета, или store-and-forward (SAF); второй без буферизации, или cut-through, другое популярное название метода сквозной коммутации – «на лету» (on the fly). Применяются в сетях и гибридные коммутаторы, которые могут автоматически менять режим работы с cut-through на SAF и наоборот. Переключение между режимами основано на определении производительности узла и целостности пакета.

Технология коммутации с обязательной буферизацией является традиционной для большинства современных сетей [2, 5, 6]. Она обеспечивает передачу пакета отправителю только после приема пакета и проверки контрольной суммы (FCS). Пакет удаляется, если он короче 64 байтов или длиннее 1518 байтов, или контрольная сумма ошибочна. Для метода SAF время доставки пакета увеличивается пропорционально размеру пакета: чем больше размер пакета, тем больше времени требуется на прием и проверку. Однако коммутаторы, реализующие метод обязательной буферизации, обладают существенными преимуществами: устройство может быть оснащено портами, поддерживающими разные технологии и скорости передачи, поэтому задержка, вносимая коммутацией store-and-forward при передаче кадров, оказывает-

ся незначительной; и второе, проверка целостности пакета позволяет не нагружать сеть поврежденными пакетами.

Технология сквозной коммутации буферизует только заголовок сообщения [2]. Коммутаторы cut-through не выполняют селекцию пакетов [3], благодаря этому они самые быстрые в своем классе. Недостаток этого метода коммутации заключается в том, что он передает любые пакеты, в том числе содержащие неправильную контрольную сумму, однако современная сетевая инфраструктура позволяет свести вероятность возникновения ошибочных пакетов к минимуму. В некоторых устройствах со сквозной коммутацией используется метод ICS (interim cut-through switching), который фильтрует пакеты длиной менее 64 байтов. Коммутаторы без обязательной буферизации [3] в основном используются в центрах обработки данных, где необходимо обеспечить непрерывную передачу большого объема трафика с минимальными задержками.

2. Модель вычислительной решетки со сквозной коммутацией пакетов

В телекоммуникационных сетях одной из основных компонент является активное оборудование, такое как коммутаторы или маршрутизаторы. Модели коммуникационных прямоугольных решеток [1] с основным элементом, представленным моделью коммуникационного устройства, реализующий технологию SAF, изучены в [7, 9]. Рассмотрим модель узла со сквозной коммутацией пакетов [10], или, иначе, с прямой передачей пакета из порта в порт без принудительной буферизации. Используемые типы, функции, переменные и константы описаны в [9]. Для построения модели решетки используются две основные модели: модель узла со сквозной коммутацией пакетов как коммуникационное устройство и модель генератора трафика как терминальное устройство. Для исследования влияния злонамеренного трафика на функционирование решетки построены модели пушек пакетов. Все модели построены в моделирующей системе CPN Tools [8].

2.1. Модель узла со сквозной коммутацией пакетов

Модель узла основана на стандартных процедурах передачи пакетов [3] в современных сетях и решетках. На рисунке 1 представлена базовая модель узла сетевого устройства со сквозной коммутацией пакетов [10], которая будет использована для построения модели прямоугольной решетки. Модель узла содержит четыре порта, обеспечивающие полнодуплексный режим работы для одновременной передачи и приема пакетов. Каждый порт состоит из четырех позиций, которые моделируют входной и выходной каналы: буфер выходного канала порта описывается позицией *po* и позицией-ограничителем *pol*; буфер входного канала порта представлен позицией *pi* и ее ограничителем – позицией *pil*. Позиции портов описаны как тип *pkt*, ограничитель порта равен единице, которая соответствует пропускной способности канала порта – одному пакету. Для спецификации всех портов к имени порта добавляется индекс порта, равный от одного до четырех. Для построения модели решетки узлы портов узлов располагаются по сторонам квадрата в следующем по-

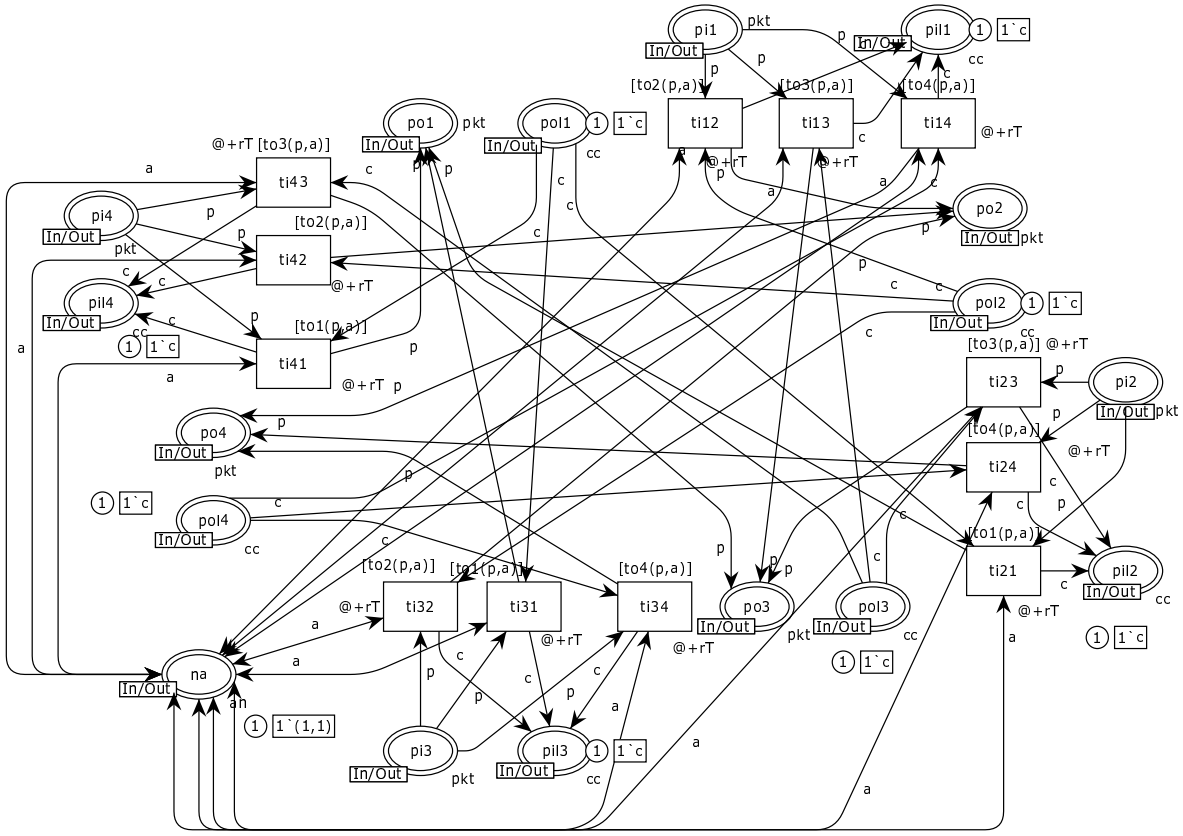

Рис. 1. Модель коммуникационного узла

Fig. 1. Model of a communication node

рядке: верхний порт – это первый порт, описывается позициями $po1, pol1, pi1, pil1$; правый порт – это второй порт с позициями $po2, pol2, pi2, pil2$; нижний порт является третьим портом с позициями $pi3, pil3, po3, pol3$; и левый порт – это четвертый порт с позициями $pi4, pil4, po4, pol4$. Позиции портов и их ограничителей являются контактными позициями для композиции решетки любого размера.

Для адресации узлов решетки используются индексы (i, j), где первый индекс описывает номер строки, а второй – номер столбца. Каждый узел имеет уникальный адрес, который хранится в контактной позиции na. Выходной канал порта моделируется только двумя позициями: po, pol, а входной канал порта моделируется двумя позициями pi, pil и тремя переходами. Для описания перенаправления пакета с входного порта на выходной порт к имени перехода ti добавляются два индекса для каждого возможного направления передачи (верхний, нижний, левый или правый). Например, переход $ti43$ передает пакет из входного порта $pi4$ в выходной порт $po3$.

Временные характеристики модели узла, представленной в [9], заданы двумя параметрами sT и rT, которые представляют собой временную задержку отправки и получения пакета соответственно. В рассматриваемой модели для описания сквозной коммутации пакетов каждый переход наделен временным атрибутом rT, который описывает время получения и перенаправления пакета из входного порта в выходной порт. Напомним, что в соответствии с алгоритмом сквозной коммутации [3] пакет перенаправляется из входного порта в выходной порт, если выходной

порт свободен. Для определения выходного порта назначения [7] в модели узла используются специальные предикаты, они представлены как атрибуты переходов. Например, предикат $to4(p, a)$ определяет передачу пакета в четвертый выходной порт, где переменная p содержит информацию о пакете (адрес назначения, адрес отправителя) и a адрес текущего узла.

В начальной маркировке все позиции ограничителей портов $pil*$ и $pol*$ содержат маркировку 1'c; все входные $pi*$ и выходные $po*$ позиции пустые, т.е. не содержат фишек. Модели узла решетки присваивается имя в соответствии с номером строки и столбца решетки, например, устройство $n6-4$ является четвертым элементом в шестой строке прямоугольной решетки.

2.2. Модель генератора трафика

Для формирования нагрузки и исследования параметров качества обслуживания решетки построена модель генератора трафика (терминального устройства), которая подробно описана в [9]. Терминальным устройствам присваиваются имена в соответствии с первой буквой имени границы, к которой они присоединены, к букве добавляется пара индексов – номера строки и столбца. Например, в имени «правого» терминального устройства первая буква r, терминальное устройство $r5-9$ пятое в девятом столбце сетки. Модель состоит из трех основных частей: генерация и отправка пакета [4]; получение пакета; обработка сообщения [6] и вычисление параметров качества обслуживания решетки [5, 10].

Первая часть описывает процесс генерации трафика, интенсивность и функцию распределения трафика, правила отправки пакетов. Каждый пакет состоит из адреса получателя, адреса отправителя, информационного поля и временного штампа, равного времени отправки сообщения. Адрес получателя выбирается из всего множества адресов с помощью случайной функции. Счетчик отправленных пакетов в начальной маркировке равен нулю и при формировании сообщения увеличивается на единицу. Обязательным условием генерации пакета является доступность выходного канала порта. Получение пакета моделируется двумя позициями входного канала порта принимающего узла, далее все пакеты используются для нахождения параметров QoS решетки в процессе вычислительного эксперимента. Третья часть модели содержит счетчик полученных пакетов, накапливает сумму времен доставки пакетов, рассчитывает среднее время доставки пакета, производительность решетки.

2.3. Модель пушки пакетов

Для исследования поведения решетки и оценки параметров качества обслуживания в условиях влияния злонамеренного трафика построены и присоединены к границам решетки модели пушек пакетов [7]. Модель пакетной пушки, которая является упрощенной моделью генератора трафика, представлена на рисунке 2. Формирование пакетов, передача их в сеть и увеличение счетчика отправленных пакетов выполняется переходом $GunGenP$. Периодичность запуска определена случайной функцией $gDelay()$ и переменной tic, которая хранится в позиции $GunClock$, количество сгенерированных пушкой пакетов вычисляется в позиции $N - sndg$. Адрес

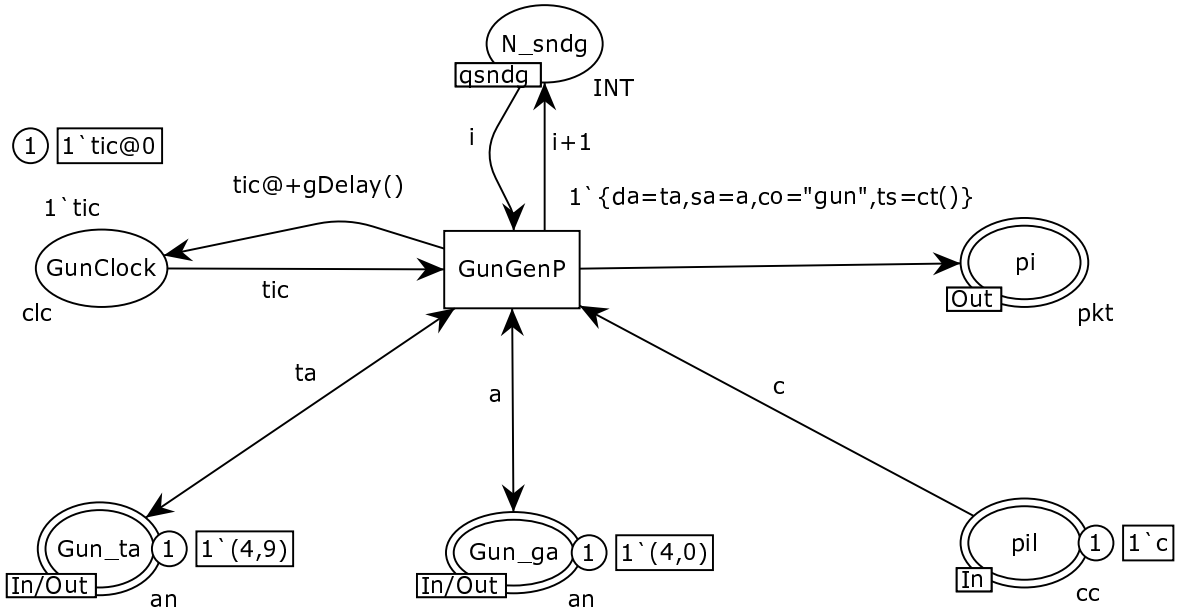

Рис. 2. Модель пушки пакетов

Fig. 2. Model of a packet gun

отправителя задан в позиции $Gun-ga$; адрес получателя назначается в зависимости от типа злонамеренного трафика в позиции $Gun-ta$; позиции pi и pil моделируют канал передачи пакета. Получение и обработку пакетов пушек выполняют терминальные устройства, для идентификации пакета пушки информационное поле содержит слово gun. Основные характеристики пушек, которые влияют на поведение модели решетки, такие как: интенсивность работы, количество пушек и мишеней, их расположение – изучены в [9].

2.4. Модель вычислительной решетки с узлом, реализующим сквозную коммутацию пакетов

Модель вычислительной решетки [1] представляет собой объединение моделей узлов, реализующих сквозную коммутацию пакетов, и моделей генераторов трафика [7]. В соответствии с иерархической структурой моделей, построенных в CPN Tools [8], модели всех устройств представлены как подмодели в виде переходов на главной странице модели. К переходам добавлены позиции, моделирующие порты устройств, и позиция, которая содержит уникальный адрес устройства. Модель вычислительной решетки размера 8x8 с узлом, реализующим сквозную коммутацию пакетов, и с текущей маркировкой, полученной в процессе моделирования, представлена на рисунке 3. К модели решетки добавлены две пушки, образующие конфигурацию «дуэль трафика», это пара пушек с взаимными мишенями, которые присоединены к терминальным устройствам с индексами (4,0) слева и (4,9) справа.

Композиция модели решетки производится согласно правилам, представленным в [7, 9]. Модель решетки является главной страницей модели, имеет вид прямоугольной матрицы, состоящей из подмоделей коммуникационных узлов, реализу-

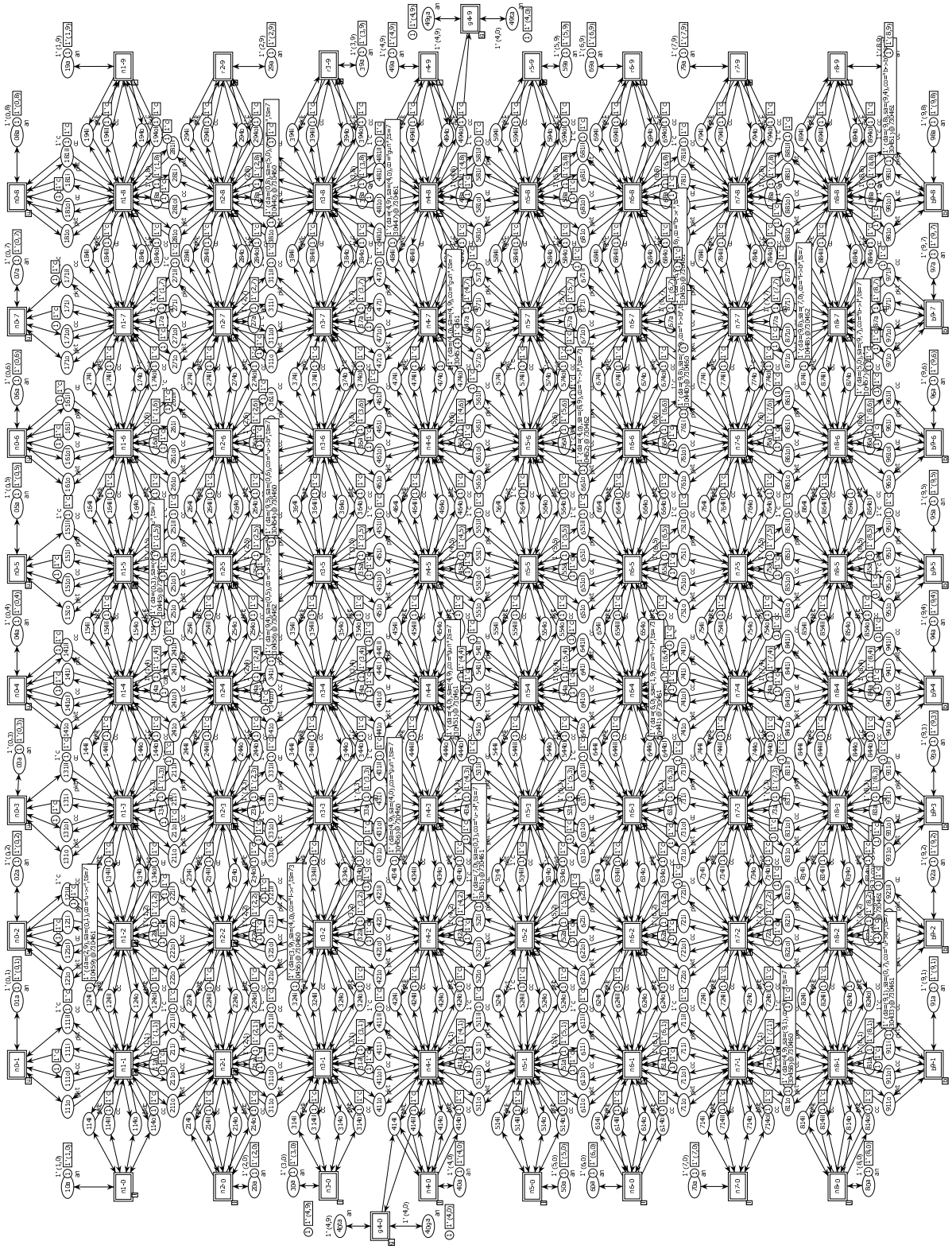

Рис. 3. Модель вычислительной решетки 8x8

Fig. 3. Model of an 8x8 computing grid

ющих метод сквозной коммутации. Модели генераторов трафика и модели пушек присоединены к границам модели решетки. Коммуникационные и терминальные устройства представлены переходами сети Петри, позиции с индексами (* – i, j, p: i – номер строки, j – номер столбца, p – номер порта) и суффиксами $*o, *ol, *i, *il$ являются контактными позициями, которые описывают выходные и входные порты узлов сетки и терминальных устройств.

Первый и четвертый порты каждого узла представлены индексом этого узла; второй и третий порты объединяются с первым и четвертым портами следующих узлов и имеют индексы следующих узлов. Например, позиция $361i$ является первым входным портом узла $n3-6$ и третьим выходным портом узла $n2-6$. Контактные позиции последней строки и правого столбца решетки описывают первый и четвертый порты узлов, которых нет в модели, эти позиции используются для присоединения нижних и правых терминальных устройств, генерирующих пользовательский трафик. Например, позиция $494o$ является четвертым выходным портом узла $n4-9$, но узла с таким индексом (4,9) нет в решетке, эта позиция объединяется с входным портом терминального устройства $r4-9$. Далее все исследования будут проводиться на модели вычислительной решетки размера 8x8.

3. Сравнительный анализ устойчивости вычислительных решеток с различной архитектурой узла

3.1. Масштабирование времени

После построения и отладки модели имитационное моделирование предусматривает специальную организацию экспериментов с моделью. Наличие стационарного режима функционирования модели позволяет провести оценку средних характеристик и других статистических моментов. Моделирующая система CPN Tools [8] используется как обычная система имитационного моделирования, которая позволяет моделировать на больших интервалах времени поведение сети любой сложности [4, 9]. Больший интерес представляют модели, которые используют случайные функции [4–6], в этом случае исследуются такие особенности сети, как среднее время доставки пакета, производительность, количество отправленных и принятых пакетов т.д.

В CPN Tools нет инструментов для управления временем, но предоставляется возможность выбрать достаточно большое количество шагов, чтобы обеспечить длительность процесса моделирования, соответствующую реальному времени. Также не вычисляется первичная статистическая информация: максимальное, минимальное и среднее количество фишек в позициях, частоты срабатывания переходов и т.д. Но система предоставляет язык для описания процессов накопления и вычисления характеристик, который используется в измерительных фрагментах сети [4–6].

Эксперименты с моделью предполагают: масштабирование времени, существование стационарного режима поведения модели, оценку характеристик. Масштабирование времени представляет большой интерес, чтобы сделать модель реалистичной. Время в CPN Tools измеряется в единицах модельного времени (MTU), которые не имеют размерности, и представляется натуральным числом. Поэтому для исследуе-

мой сети сначала определяются времена в реальных единицах (мс, нс) из описания технологии, аппаратных средств и программного обеспечения. Затем выбирается MTU как наименьший интервал времени. Затем все времена модели пересчитываются в MTU, после получения результатов моделирования время пересчитывается обратно в реальные единицы времени.

Для определения временных характеристик модели вычислительной решетки и расчета параметров качества обслуживания рассмотрим масштабирование времени для технологии 10 Гбит/с. Временные характеристики узла решетки заданы двумя параметрами sT и rT, которые представляют собой временную задержку отправки и получения пакета соответственно. Скорость передачи полезной информации в рассматриваемой технологии составляет 8 Гбит/с, или, иначе 1 Гбайт/с. Примем длину пакета равной максимальной длине кадра Ethernet, 1518 байтов, и длину заголовка кадра 18 байтов. Тогда весь пакет передается за $1,518 \cdot 10^{-6}$ секунды, пакет без адресной информации за $1,5 \cdot 10^{-6}$, заголовок пакета за $0,018 \cdot 10^{-6}$. Значение $0,018 \cdot 10^{-6}$, как минимальное, примем за 1 MTU. Пересчитаем остальные значения: $1,5 \cdot 10^{-6}$ равно 83 MTU, $1,518 \cdot 10^{-6}$ равно 84 MTU.

Тогда для метода коммутации с обязательной буферизацией временная задержка получения пакета rT равна 84 MTU, временная задержка отправки пакета sT равна 1 MTU, общее время задержки 85 MTU. Для метода сквозной коммутации временные задержки получения пакета и отправки пакета являются объединенной величиной (rT), в соответствии с характеристикой технологии [2,3].

Для решетки 8x8 идеальное время доставки пакета при методе сквозной коммутации (передача через 8 устройств-хопов) равно 84 MTU. Идеальное время предполагает, что заголовок пакета находится в 8 узле, а хвост пакета еще передается в первом узле. Тогда временная задержка на одном узле примерно равна 11 MTU. Для того чтобы упростить оценку средних и сделать модель более реалистичной, примем следующие значения временных характеристик: для метода коммутации с обязательной буферизацией общая временная задержка 100 MTU, для метода сквозной коммутации 20 MTU. Разделим значения на 10, для узлов SAF временные характеристики на переходах модели узла назначим равными $sT = rT = 5$, для узлов cut-through $rT = 2$.

3.2. Исследование характеристик моделей решеток в условиях рабочей нагрузки

Модель вычислительной решетки отлажена в условиях рабочей нагрузки, которую формируют модели генераторов трафика [10]. Выполнена оценка параметров качества обслуживания и поведения решетки в условиях рабочей и пиковой нагрузки. Исследования производительности решетки и среднего времени доставки пакета выполнены для распределения Пуассона с различной интенсивностью.

В таблице 1 представлены результаты исследования характеристик решетки в условиях рабочей нагрузки для узлов без обязательной буферизации. Аббревиатура MTU (Model Time Unit) обозначает единицу измерения модельного времени; символ $*$ показывает, что решетка приходит к полному тупику, то есть в модели отсутствуют активные переходы. Производительность решетки измеряется в количестве

Таблица 1. Характеристики модели решетки 8x8 при рабочей нагрузке

Table 1. Characteristics of an 8x8 grid model under a workload

Интенсивн. рабочей нагрузки Workload intensity	Шаг Step	Время Time	Кол-во отправлн. пакетов N sent packets	Кол-во принятых пакетов N received packets	Производит. решетки Grid performance	Ср.время доставки пакета Average packetDT
90.0	10000000	2615179	930023	901051	0.34	15
50.0	10000000	1453296	930061	900918	0.61	15
40.0	10000000	1163360	930316	901580	0.77	15
30.0	10000000	872079	930017	900635	1.03	15
20.0	10000000	581430	930397	901152	1.54	15
15.0*	9080431	396103	844938	818415	2.06	15
10.0*	8339863	242597	775968	751454	3.09	16
9.0*	2182011	57315	203181	196658	3.44	16
8.0*	2164592	50464	201381	194996	3.86	16
7.0*	7488036	152909	696902	674855	4.41	16
6.0*	1366960	26111	127387	123307	5.11	17
5.0*	381924	5950	35588	34339	5.81	19
4.0*	49317	842	4729	4397	5.62	24

пакетов в единицу модельного времени ($packets/MTU$), среднее время доставки пакета в MTU.

Полученные результаты (таблица 1) показывают, что решетка приходит в тупик даже при рабочей нагрузке, в большинстве случаев тупик означает, что порты назначения узлов заняты. Максимальная производительность решетки, или пиковая нагрузка, достигается при интенсивности рабочей нагрузки wl=15.0 и заданной интенсивности обслуживания rT=2, и равна gp=2 пакета за единицу модельного времени.

Проведен сравнительный анализ устойчивости вычислительных решеток с различной архитектурой узла. В таблице 2 представлены результаты исследования решеток посредством рабочей нагрузки для узлов, реализующих технологию передачи пакетов с принудительной буферизацией SAF [9], и сквозной коммутации. Размер буфера в модели узла, реализующего SAF, равен 100 пакетам.

Производительности решеток примерно одинаковы в условиях рабочей нагрузки. В условиях пиковой нагрузки решетка с узлом, реализующим технологию передачи пакетов с принудительной буферизацией, более устойчива, в отличие от сквозной коммутации, у которой производительность падает в 1,5 раза и более. Среднее время доставки пакета значительно ухудшается, примерно в 2 раза, у решетки с узлом SAF; при этом у решетки с узлом cut-through в 1,5 раза. Решетка с узлами cut-through приходит к полному тупику при интенсивности пиковой нагрузки wl=10.0 (характеристики решетки в таблице 2 отмечены символом $*$), решетка с узлами SAF – при интенсивности пиковой нагрузки, равной wl=8.0.

Таблица 2. Характеристики моделей решетки 8x8 с различной архитектурой узла при рабочей нагрузке

Table 2. Characteristics of 8x8 grid models with different node architecture under a workload

Интенсивность рабоч.нагрузки Workload intensity	Производ-ть решетки Grid perform. SAF	Средн.время доставки пак. Average packet delivery time	Производ-ть решетки Grid perform. $Cut-through$	Средн.время доставки пак. Average packet delivery time
90.0	0.34	78	0.34	15
50.0	0.62	78	0.61	15
40.0	0.78	79	0.77	15
30.0	1.03	79	1.03	15
20.0	1.55	81	1.54	15
10.0	3.1	97	3.09*	16*
9.0	3.44	130	3.44*	16*
8.0*	2.51	236	3.86	16
7.0*	2.16	301	4.41	16
6.0*	2.22	288	5.11	17
5.0*	3.41	231	5.81	19
4.0*	3.25	189	5.62	24

3.3. Оценка влияния злонамеренного трафика на параметры качества обслуживания решеток

Исследуем производительность решетки и среднее время доставки пакета в условиях злонамеренного трафика, с различной интенсивностью и пуассоновской функцией распределения. В таблице 3 представлены результаты исследования характеристик решетки для узлов без обязательной буферизации, интенсивность рабочей нагрузки wl=30.0. Значение интенсивности рабочей нагрузки выбрано для дальнейшего сравнения с результатами, полученными для SAF [7,9]. К параметрам таблицы, представленным в предыдущем подразделе, добавлено значение $gsnd$ – количество пакетов (выстрелов), отправленных пушками; количество операций (шагов), выполняемых моделью, осталось равным $Step$=10000000.

Результаты вычислительного эксперимента, представленные в таблице 3, показывают, что среднее время доставки пакета в решетке при интенсивности злонамеренного трафика в диапазоне 4.0–9.0 практически не изменяется, равно 15–16 MTU и равно среднему времени доставки в условиях рабочей нагрузки (таблица 1). Производительность решетки увеличивается, при максимальной интенсивности пушки gl=4.0 производительность решетки в 1.5 раза больше, чем при рабочей нагрузке, и равна gp=1.54 пакета за единицу модельного времени. Решетка не приходит в тупик, т.е. конфигурация «дуэль» не оказывает влияние на решетку при интенсивности рабочей нагрузки wl=30.0.

Таблица 3. Характеристики модели решетки 8x8 при разной интенсивности злонамеренного трафика

Table 3. Characteristics of an 8x8 grid model under ill-intentioned traffic with different intensity

Интенсивн. трафика пушки Traffic gun intensity	Время Time	Кол-во отправл-х пакетов Number of packets sent	Кол-во принятых пакетов Number of packets received	Кол-во пакетов выстрел-х из пушек N fired packets	Производи-тельность решетки Grid performance	Среднее время доставки пакета Average packetDT
4.0	607791	648331	931033	302864	1.54	16
5.0	646515	689875	926856	258690	1.43	16
5.5	662607	706690	925542	241035	1.39	16
6.0	675425	720558	923412	225116	1.36	16
8.0	715934	763637	918985	179083	1.28	15
9.0	730551	778991	916985	162344	1.28	15

Проведем сравнительный анализ устойчивости вычислительных решеток с различной архитектурой узла в условиях злонамеренного трафика, типа «дуэль трафика». Пушки присоединены к узлам решетки (рис. 3) с индексами (4,0) и (4,9). В таблице 4 представлены результаты исследования решеток с узлами, реализующими технологию передачи пакетов с обязательной буферизацией [9], и сквозной коммутации.

Таблица 4. Характеристики моделей решетки 8x8 с различной архитектурой узла в условиях злонамеренного трафика

Table 4. Characteristics of 8x8 grid models with different node architecture under an ill-intentioned traffic

Интенсивность трафика пушки Traffic gun intensity	Производит-ть решетки Grid performance SAF	Средн.время доставки пак. Average packet delivery time	Производит-ть решетки Grid performance $Cut-through$	Средн.время доставки пак. Average packet delivery time
4.0	0.34*	76	1.54	16
5.0	0.43*	73	1.43	16
5.5	0.67*	78	1.39	16
6.0	1.37	67	1.36	16
8.0	1.28	64	1.28	15
9.0	1.26	66	1.28	15

При интенсивности рабочей нагрузки wl=30.0 дуэль трафика приводит решетку с узлами, реализующими технологию SAF, к полному тупику через дополнительную нагрузку менее чем 10 процентов. Решетка с узлами, реализующими cut-through, работает в штатном режиме. Дальнейшие исследования показали, что конфигурация «дуэль трафика» не оказывает влияние на решетку с узлами cut-through при увеличении рабочей нагрузки до пиковой wl=15.0, при которой решетка приходит к полному тупику.

Построена модель вычислительной решетки с узлами, реализующими технологию сквозной коммутации пакетов, в форме раскрашенной сети Петри. Исследована безопасность решеток и возможность взаимоблокировок узлов решетки в условиях рабочей нагрузки. Для оценки параметров качества обслуживания в условиях злонамеренного трафика к модели решетки добавлены модели пушки пакетов, имитирующие «вредный» трафик. Проведен сравнительный анализ устойчивости вычислительных решеток с различной архитектурой узла в условиях рабочей нагрузки и злонамеренного трафика.

Таким образом, результаты имитационного моделирования подтвердили ранее полученные результаты, что современная архитектура коммутационных устройств не гарантирует безопасность решетки. Должны быть разработаны специальные протоколы для обнаружения и предотвращения взаимоблокировок, которые предполагают взаимодействие нескольких узлов.

Направлением дальнейших исследований является оценка эффективности и характеристик QoS решетки при произвольных функциях распределения генераторов трафика, типов тупиков, конфигураций устройств, формирующих скрытые атаки, построение рентерабельной модели для исследования структур решеток любого размера.

Список литературы / References

[1] Preve N. P., *Grid Computing: Towards a Global Interconnected Infrastructure*, Springer, 2011, 312 pp.

[2] Зайцев Д. А., Шмелёва Т. Р., Гуляев К. Д., *Отчет о научно-исследовательской работе «Разработка новых систем адресации глобальных сетей»*, номер госрегистрации 0108U008900, ОНАС, Одесса, 2009, 124 pp., (на украинском языке); [Zaitsev D. A., Shmeleva T. R., Guliaiev K. D., *Report on scientific-research work "Development of New World-wide Networks Addressing Systems"*, state registration number 0108U008900, ONAT, Odessa, 2009, 124 pp., (in Ukrainian).]

[3] Liberzon D., *Switching in Systems and Control*, Birkhauser, Boston, 2003, 230 pp.

[4] Sakun A. L., Zaitsev D. A., "An Evaluation of MPLS Efficacy using Colored Petri Net Models", *Proceedings of International Middle Eastern Multiconference on Simulation and Modelling (MESM'2008)*, Amman (Jordan), August 26–28, 2008, 31–36

[5] Shmeleva T. R., Zaitsev D. A., "Switched Ethernet Response Time Evaluation via Colored Petri Net Model", *Proccedings of International Middle Eastern Multiconference on Simulation and Modelling*, August 28–30, 2006, Alexandria (Egypt), 68–77

[6] Zaitsev D. A., Shmeleva T. R., "Parametric Petri Net Model for Ethernet Performance and Qos Evaluation", *Proceedings of 16th Workshop on Algorithms and Tools for Petri Nets*, September 25–26, 2009, University of Karlsruhe, Germany, 15–28

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

[8] Jensen K., Kristensen L.M., *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*, Springer, 2009, 384 pp.

[9] Retschitzegger W., Proll B., Zaitsev D. A., Shmeleva T. R., "Security of grid structures under disguised traffic attacks", *Cluster Computing*, **19**:3 (2016), 1183–1200

[10] Shmeleva T. R., "Security of Grid Structures with Cut-through Switching Nodes", *System Informatics*, 2017, № 10, 23–32

Shmeleva T. R., "Comparative Analysis of Stability to Induced Deadlocks for Computing Grids with Various Node Architectures", *Modeling and Analysis of Information Systems*, **25**:2 (2018), 193–206.

DOI: 10.18255/1818-1015-2018-2-193-206

Abstract. In this paper, we consider the classification and applications of switching methods, their advantages and disadvantages. A model of a computing grid was constructed in the form of a colored Petri net with a node which implements cut-through packet switching. The model consists of packet switching nodes, traffic generators and guns that form malicious traffic disguised as usual user traffic. The characteristics of the grid model were investigated under a working load with different intensities. The influence of malicious traffic such as ≪traffic duel≫ was estimated on the quality of service parameters of the grid. A comparative analysis of the computing grids stability was carried out with nodes which implement the store-and-forward and cut-through switching technologies. It is shown that the grids performance is approximately the same under work load conditions, and under peak load conditions the grid with the node implementing the store-and-forward technology is more stable. The grid with nodes implementing SAF technology comes to a complete deadlock through an additional load which is less than 10 percent. After a detailed study, it is shown that the ≪traffic duel≫ configuration does not affect the grid with cut-through nodes if the workload is increases to the peak load, at which the grid comes to a complete deadlock. The execution intensity of guns which generate a malicious traffic is determined by a random function with the Poisson distribution. The modeling system CPN Tools is used for constructing models and measuring parameters. Grid performance and average package delivery time are estimated in the grid on various load options.

Keywords: computing grid security, cut-through switching, traffic attack defence, performance evaluation, colored Petri net, deadlock

On the authors:
Tatiana R. Shmeleva, orcid.org/0000-0002-4799-3842, PhD,
A.S. Popov Odessa National Academy of Telecommunications,
1 Kuznechnaya str., Odessa 65029, Ukraine, e-mail: tishtri@rambler.ru

Acknowledgments: The author would like to thank Program Committee and the participants of PSSV-2017 workshop for discussion of some results presented in this paper.