Проектирование компьютерных сетей

DOI 10.66032/2221-2574-2025-1-3-54-64 УДК 004.7+004.9

МЕТОДИКА ВЫБОРА АДАПТИВНОГО УПРАВЛЕНИЯ ПОТОКАМИ ДЛЯ СЕТЕВЫХ УЗЛОВ SPACEFIBRE

Суворова Елена Александровна
кандидат технических наук, доцент, ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения».
E-mail: wildcat15@yandex.ru

Поляков Вадим Борисович
доктор технических наук, доцент, ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения».

Адрес: 190000, Российская Федерация, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А.

Аннотация: В большинстве высокопроизводительных распределённых вычислительных систем, используемых в радиотехнических системах, отдельных их подсистемах, существует необходимость передачи большого количества независимых потоков данных. В стандарте SpaceFibre независимая передача потоков данных обеспечивается за счёт использования виртуальных сетей (виртуальных каналов). В стандарте обеспечивается поддержка 64 виртуальных сетей, что на порядки меньше, чем количество потоков данных в современных вычислительных системах. Вследствие этого, необходимо обеспечивать независимость потоков данных, передаваемых и в пределах одной виртуальной сети. В стандарте существует два механизма — механизм потоковой передачи (Streaming mode) и механизм таймаутов, которые потенциально могут использоваться для исключения незапланированного взаимовлияния потоков. В статье предлагаются дополнительные механизмы адаптивного управления потоками, позволяющие управлять достижимыми характеристиками. Выполняется оценка, сравнение возможностей этих механизмов, оценка достижимых характеристик в зависимости от различных сценариев событий, которые могут провоцировать незапланированное взаимовлияние потоков. Для реализации данных механизмов требуются дополнительные аппаратные затраты. В статье предлагается методика оценки эффективности существующих в стандарте и предлагаемых механизмов на основе Data Envelopment Analysis. Она позволяет разработчику выбрать механизмы с учётом допустимых аппаратных затрат и вероятности различных сценариев, приводящих к незапланированному влиянию, характерных для разрабатываемой системы.

Ключевые слова: SpaceFibre, динамическая реконфигурация, сети с требованиями реального времени, DEA, адаптивное управление потоками данных, высокопроизводительные вычислительные системы.

Введение

Большинство современных радиотехнических систем и входящих в их состав подсистем является сложными многозадачными системами. К части решаемых в них задач предъявляются требования жёсткого реального времени, для других задач могут применяться требования мягкого реального времени, к некоторым задачам требования реального времени могут не применяться. Для обмена данными между задачами, функционирующими в пределах одной подсистемы, как правило, используется одно и тоже (общее) сетевое оборудование, поскольку существуют ограничения по массе и энергопотреблению. Характеристики потоков данных могут значительно меняться во времени. В условиях ограниченных сетевых ресурсов требуется возможность адаптации к этим изменениям — перераспределения сетевых ресурсов между потоками. При этом особенно важным становится обеспечение независимости потоков данных, обеспечение требуемых характеристик передачи потоков данных в условиях таких изменений.

В сети SpaceFibre [1] для передачи потоков данных, которые не должны влиять друг на

друга, используются различные виртуальные сети. Использование физических каналов передачи данных в сети различными виртуальными сетями осуществляется в режиме разделения времени. В соответствии со стандартом SpaceFibre в одной сети может поддерживаться до 64 виртуальных сетей, в одном звене передачи данных может поддерживаться до 32 виртуальных каналов (через него может проходить до 32 виртуальных сетей). Очерёдность передачи в физический канал фреймов, относящихся к разным виртуальным сетям (разным виртуальным каналам), определяется параметрами, заданными для них системным администратором.

Одна виртуальная сеть потенциально может использоваться для передачи одного потока данных. Но в современных распределённых вычислительных системах существует необходимость передавать сотни и тысячи потоков данных [2, 3, 4, 5, 6, 7]. Вследствие этого в стандарте SpaceFibre рекомендуется одну (каждую) виртуальную сеть использовать для передачи нескольких потоков данных, для которых требуется обеспечить сходные характеристики доставки объектов данных. В стандарте SpaceFibre определено, что виртуальная сеть с номером 0 должна использоваться для передачи служебной информации, необходимой для управления сетью [1]. Для каждой из виртуальных сетей разработчик распределённой вычислительной системы может задавать любые параметры в рамках допустимых по стандарту: уровень приоритета, долю пропускной способности физического канала, перечень таймслотов, в которых разрешена передача данных. Физический канал используется для передачи фреймов из разных виртуальных каналов в режиме разделения времени в соответствии с этими параметрами.

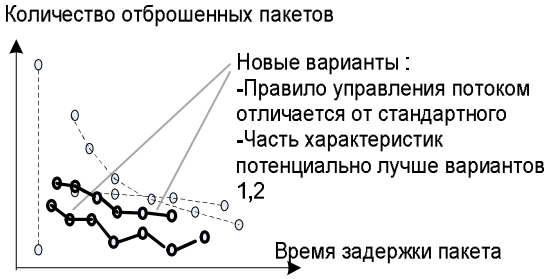
Для каждого виртуального канала может быть задано правило управления потоком. В рамках стандарта определено два возможных варианта управления потоком в звене передачи данных. При использовании обоих вариантов приёмная сторона отправляет передающей стороне информацию о количестве слов данных (количество кредитов FCT), которые она может принять в соответствии с имеющимся свободным местом в приёмном буфере. При использовании первого варианта передающая сторона осуществляет передачу данных в соответствии с полученным количеством кредитов. При отсутствии кредитов передача данных останавливается до тех пор, пока не будут получены новые кредиты. Соответственно такая остановка может привести к блокировке дальнейшей передачи не только этого потока данных, но и других потоков данных в этой виртуальной сети. Для борьбы с блокировками предусмотрены таймауты передачи данных. По истечении таймаута текущий пакет данных отбрасывается. Значение таймаута настраивается разработчиком сети в соответствии с ожидаемыми характеристиками корректной передачи [1].

При использовании второго варианта если на передающей стороне имеются данные на передачу и отсутствуют кредиты, то данные отбрасываются (стираются), чтобы не блокировать передачу других потоков данных (если пакет данных начал отбрасываться, то он отбрасывается до конца, даже в том случае, когда новые кредиты уже были получены).

Таким образом, выбор одного из вариантов и значений параметров позволяет либо исключить отбрасывание данных, но при этом могут возникать блокировки передачи, либо исключить блокировки за счёт того, что данные будут отбрасываться сразу же (при этом может отбрасываться много данных), либо за счёт выбора размера таймаута управлять временем ожидания передачи данных (рис. 1, *а*).

В современных сетях, используемых для высокопроизводительных вычислительных систем, применяются различные стратегии адаптивного управления потоками данных [7, 8, 9, 10]. Потенциально в сетевых узлах могут использоваться более сложные схемы поведения, чем определенные в стандарте, позволяющие адаптировать управление потоками данных в пределах виртуальной сети к ситуациям,

а) правила управления потоком SpaceFibre



б) дополнительные правила управления потоком

Рис. 1. Иллюстрация зависимости времени задержки пакета, количества отброшенных пакетов от выбранного варианта и размера таймаута

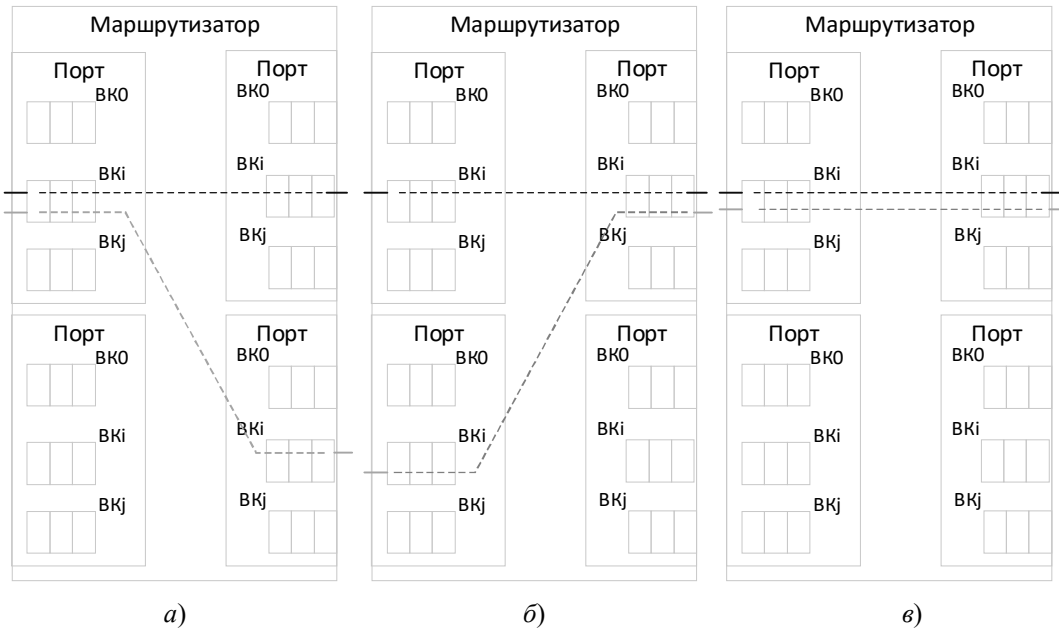
которые могут в ней возникать. Данные схемы потенциально могут сократить количество отбрасываемых пакетов, сократить взаимовлияние между потоками. Но для их реализации требуются дополнительные аппаратные затраты (рис. 1, *б*).

В статье предлагается методика, позволяющая разработчику оценивать эффективность схем адаптивного управления потоками, основанная на Data Envelopment Analysis (DEA) [11, 12, 13], приводится пример использования этой методики

Типовые причины взаимовлияния потоков данных в пределах одной виртуальной сети

Под взаимовлиянием потоков в пределах одной виртуальной сети в данной статье будем понимать возникновение ситуации, когда из-за одного потока останавливается (блокируется) передача других потоков в данной виртуальной сети на время, дольше, чем было запланировано в соответствии с необходимыми характеристиками передачи данного потока. В сетях SpaceFibre с требованиями реального времени объект данных должен быть доставлен приёмнику в течении времени, не превосходящего заданного таймаута. Если это требование не удовлетворяется, то пакет должен быть отброшен (если не отбрасывать такие пакеты, то они могут мешать вовремя доставлять следующие пакеты). В сети SpaceFibre пакеты могут отбрасываться или из-за истечения таймаута или вследствие некорректности сетевого адреса. Некорректный сетевой адрес может быть в результате ошибок при передаче по сети, искажения таблиц маршрутизации (вследствие сбоев или отказов в сетевых узлах) или ошибок при конфигурировании сети. Будем считать, что в рассматриваемых сетях используются механизмы парирования ошибок, благодаря которым вероятность таких ошибок пренебрежимо мала. Поэтому в качестве критерия, позволяющего оценить взаимовлияния будем использовать количество отброшенных пакетов.

Можно выделить следующие основные конфликты за ресурсы в одной виртуальной сети, наблюдаемые в пределах одного маршрутизатора. Два или более потоков, относящиеся к одной виртуальной сети, приходят в маршрутизатор по одному входному порту (рис 2, *а*). Они используют один и тот же входной буфер виртуального канала, обрабатываются одним и тем же контроллером входного порта сетевого уровня. Если из входного порта в буфер виртуального канала начал поступать пакет, относящийся к одному из потоков, до его завершения другой пакет поступать не начнёт. (Одновременно в буфере может находиться хвост одного пакета и начало следующего.) В соответствии со стандартом SpaceFibre если контроллер входа порта сетевого уровня начал обрабатывать один пакет, то пока он полностью не закончит его обработку (или не отбросит пакет), он не начнёт рассматривать следующий пакет из того же виртуального канала (даже если следующий уже полностью загружен в буфер, а передача текущего пакета приостановлена). Таким образом, если передача



а) *б*) *в*)

Рис. 2. Конфликты потоков данных в одной виртуальной сети
а) – общий входной порт, *б*) – общий выходной порт, *в*) общий входной порт и выходной порт

пакета через маршрутизатор в выходной порт по каким-то причинам остановится, то все следующие за ним по тому же виртуальному каналу пакеты также будут остановлены.

Два или более потоков, относящиеся к одной виртуальной сети, уходят из маршрутизатора по одному и тому же порту (рис 2, *б*). Они используют один и тот же контроллер выходного порта сетевого уровня, буфер выходного порта. Так же, как и в ситуации с входным портом, в этом случае если выходной порт занят передачей пакета, то пока он не закончится (или не будет отброшен), в этот выходной порт не сможет начать передаваться другой пакет из той же виртуальной сети.

Возможна комбинация этих ситуаций — несколько потоков данных одной виртуальной сети может приходить по одному порту и уходить в один и тот же выходной (рис. 2, *в*).

Поскольку в SpaceFibre используется червячная маршрутизация, один пакет в один момент времени может быть расположен в нескольких маршрутизаторах. Потенциально, он может занимать весь путь от источника к приёмнику.

В ходе анализа поведения сетей SpaceFibre были выявлены типовые причины, которые могут приводить к незапланированной в соответствии с логикой работы системы остановке (либо приостановке на недопустимо длительное время) передачи данных. К ним относятся неготовность терминального узла — приёмника к приёму данных, неготовность терминального узла — передатчика передавать оставшуюся часть пакета, генерация передатчиком некорректного по своим характеристикам трафика (вследствие некоторой внутренней ошибки). Сбои и отказы в транзитных маршрутизаторах могут приводить к сходным последствиям — генерации «лишнего» трафика, невозможности передавать текущий трафик из-за искажения значений счётчиков, передача трафика по некорректному пути. Если в рамках виртуальной сети другие потоки данных используют общие ресурсы с потоком, передача которого остановилась, то их передача так же может быть остановлена (либо приостановлена на недопустимо большое время). Приведённый список причин не является исчерпывающим, он может быть дополнен причинами, являющимися специфичными для конкретной системы.

Предлагаемая методика выбора адаптивного управления потоками данных для реализации в сетевых узлах

Предлагаемая методика включает в себя следующую последовательность действий.

1. Определение набора входных и выходных параметров для рассматриваемой системы (класса систем). В набор входных параметров необходимо включить те параметры, влияние которых на выходные параметры планируется оценивать. Входные параметры предлагается разделить на следующие группы: параметры, подлежащие оптимизации; параметры, значение которых необходимо выбрать, параметры, значением которых не представляется возможным управлять. К первой группе могут быть отнесены параметры, определяющие стоимость, физические характеристики реализации. Например, это может быть площадь, энергопотребление компонента, реализующего некоторый механизм, алгоритм. Ко второй группе можно отнести, например, значения таймаутов, ограничителей счётчиков событий (при неизменной разрядности самих счётчиков) в реализуемых вариантах алгоритмов. К третьей группе, например, могут быть отнесены характеристики внешних воздействий, приводящих к возникновению сбоев и отказов в системе.

2. Определение возможных причин взаимовлияния потоков данных для рассматриваемой системы (класса систем). Основано на определении общих ресурсов — ресурсов, используемых несколькими потоками данных.

3. Определение набора сценариев функционирования системы (узлов, входящих в состав системы), приводящих к возникновению взаимовлияния потоков данных. Для каждого из сценариев определение весового коэффициента, используемого для интегральной оценки характеристик. При определении коэффициента может быть учтена вероятность возникновения данного сценария в ходе функционирования системы.

4. Определение возможных алгоритмов поведения для сетевых узлов рассматриваемой системы (класса систем), потенциально обеспечивающих исключение или снижение взаимовлияния потоков при возникновении сценариев ошибочного поведения.

5. Определение набора вариантов реализации систем, которые будут подлежать сравнению для выбора оптимального варианта реализации, выбора значений входных параметров. Они будут на следующем этапе рассматриваться в качестве DMU (Data Management Unit).

6. Оценка значений входных и выходных параметров. (Требуется для входных параметров первой и второй группы. Входные параметры третьей группы являются входными данными при проектировании системы.) Может быть выполнена теоретически или с использованием имитационного моделирования (для оценки характеристик могут быть реализованы прототипы компонентов, реализующих адаптивное управление).

5. На основе DEA вычисление параметров эффективности реализаций. Для вычисления в общем случае может использоваться отношение взвешенной сумы выходных параметров (всех или некоторых) к взвешенной сумме входных параметров (всех или некоторых) (представлено формулой 1) или обратное соотношение суммы взвешенных входных параметров к сумме взвешенных выходных.

$$E = \text{sum}(l = 0, N - 1; Pl \cdot (\text{sum}(i = 0, Ny - 1; KYi \cdot yi) / \text{sum}(j = 0, Nx - 1; Kxj \cdot xj))), \quad (1)$$

где N — количество рассматриваемых вариантов поведения для системы; Pl — вероятность варианта l; Ny — количество выходных параметров; Nx — количество входных параметров; KYi — весовой коэффициент, соответствующий i выходному параметру; KXj — весовой коэффициент, соответствующий j входному параметру.

В зависимости от физического смысла выходных параметров и входных параметров первой группы может требоваться их минимизация или максимизация. Для входных параметров второй группы минимизация или максимизация их самих не имеет смысла (для них могут выбираться любые значения из допу-

стимого диапазона значений, позволяющие достичь лучших параметров оптимизации первой группы). Входные параметры третьей группы не подлежат управлению.

Полученные оценки эффективности может быть использовано для выбора лучшего для системы варианта реализации, либо для коррекции характеристик разработанных вариантов реализации, в качестве основы для разработки новых вариантов реализации.

Пример использования предлагаемой методики

Рассмотрим пример использования методики для класса систем, в которых незапланированное взаимовлияние между потоками может возникать в сетевых узлах (маршрутизаторах) при возникновении ситуаций, представленных на рис. 1. В качестве DMU (Data management Unit) будет рассматриваться виртуальная сеть SpaceFibre, в которой существует некоторое количество путей передачи данных с конфликтами. В каждом порту каждого маршрутизатора реализован контроллер, в котором реализуется алгоритм парирования конфликтов. Будем считать, что в пределах одного DMU во всех контроллерах используется одинаковый алгоритм.

Были выбраны следующие входные параметры. В первую группу включён параметр — накладные расходы на реализацию механизмов в контроллерах (относительная площадь) — x1. Данная группа параметров может быть дополнен значениями статического и динамического энергопотребления контроллера и др.) Во вторую группу включён параметр — значение нижней границы таймаута — x2. Данная группа параметров может быть дополнена количеством сетевых узлов в путях передачи данных, в которых возможны конфликты. В третью группу параметров могут быть включены количество путей передачи данных, характеристики передаваемых потоков данных, интенсивность и продолжительность действия ошибок (в данном рассмотрении для этих параметров будут использоваться константные значения, чтобы сократить его объём).

В качестве выходных параметров может быть выбрано:

- Суммарное количество (по всем потокам виртуальной сети, в том числе и для того, для которого возник ошибочный сценарий) успешно переданных (требуется максимизация) или суммарное количество отброшенных (требуется минимизация) пакетов для всех потоков данных. Может также использоваться доля отброшенных пакетов от общего количества пакетов (требуется минимизация). Обозначим эту группу параметров y1: ys1, yl1, yr1 соответственно. Позволяет оценить качество гарантированной доставки пакетов для виртуальной сети в целом (по отношению ко всем потокам данных).

- Количество успешно переданных (требуется максимизация), отброшенных (требуется минимизация) пакетов данных, доля отброшенных пакетов данных (требуется минимизация) суммарно по всем потокам виртуальной сети кроме того, для которого возникла незапланированная ситуация. Обозначим эту группу параметров y2: ys2, yl2, yr2 соответственно. Используется для характеризации степени взаимовлияния между потоками. Чем меньше данных из этих потоков потеряно, тем меньшее влияние на них оказал рассматриваемый поток, для которого произошёл ошибочный сценарий.

Данный перечень параметров может быть при необходимости дополнен разработчиком.

Для системы определен следующий перечень сценариев некорректного поведения (не является исчерпывающим, потенциально может быть дополнен):

1. (Сценарий 0) Узел приёмник не готов принимать очередной пакет.

2. (Сценарий 1) Узел-источник отправляет начало пакета, затем остальную часть пакета, спустя длительное время (больше времени таймаута).

Для того, чтобы получить лучшие значения выходных параметров для рассматриваемого примера, могут быть предложены дополни-

тельные режимы адаптивного управления потоками. Для виртуальной сети или для отдельного потока может быть задано не одно значение параметра (например, таймаута), а некоторые допустимые рамки. Наличие верхней границы таймаута определяется в соответствии с требованиями реального времени. Нижняя граница может принимать различные значения. Конкретное значение при этом может выбираться контроллером адаптивно с учётом текущей ситуации в маршрутизаторе, предыстории. При адаптивном выборе значения таймаута потенциально можно достичь сокращения количества отбрасываемых пакетов.

При использовании механизма таймаутов, таймаут считается для каждого текущего пакета. Если ошибочная ситуация продолжается долго — блокирует корректную передачу нескольких подряд идущих пакетов рассматриваемого потока (всех последующих, если ситуация возникла вследствие отказа). При использовании стандартного механизма таймаутов для каждого следующего пакета таймаут будет считаться снова. Для того, чтобы исключить это, для подобных сценариев может использоваться накопление истории — счёт подряд идущих пакетов, для которых сработал таймаут. По достижении таким счётчиком некоторого значения, далее пакеты могут начинать отбрасываться без счёта таймаута до тех пор, пока не возникнет возможность дальнейшей передачи очередного пакета.

Использование этих механизмов может позволить улучшить характеристики системы: снизить взаимовлияние между потоками (сократить количество отбрасываемых пакетов из потоков, для которых не возникали ошибочные сценарии), сократить общее количество отбрасываемых пакетов (с учётом того потока, для которого возник ошибочный сценарий). Но для их реализации требуются дополнительные аппаратные затраты. Необходимо реализовать дополнительные счётчики, автоматы, которые будут контролировать происходящие события для выбора схемы поведения. Для реализации были выбраны следующие варианты (перечень вариантов выбран для примера, не является исчерпывающим):

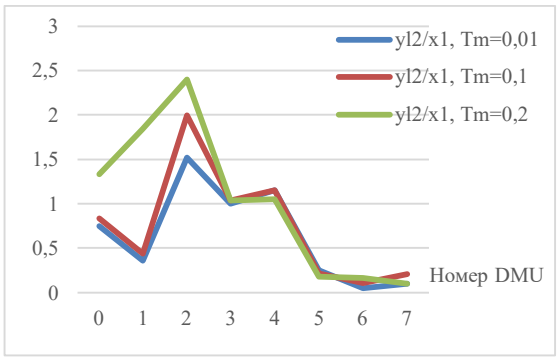
(0) После того, как достигнута нижняя граница значения таймаута, если выполняется следующее условие: входной буфер полон. В этом случае произошёл останов потоков данных, идущих через этот буфер.

(1) После того, как достигнута нижняя граница значения таймаута, если выполняется следующее условие: пакет полностью заполнил входной буфер и в буфере нет конца пакета. В этом случае хвост пакета расположен в предыдущем маршрутизаторе (в одном из предыдущих маршрутизаторов), таким образом, пакет заблокировал довольно большую часть пути. Вследствие этой ситуации возможны потенциальные блокировки другого трафика в предыдущих маршрутизаторах.

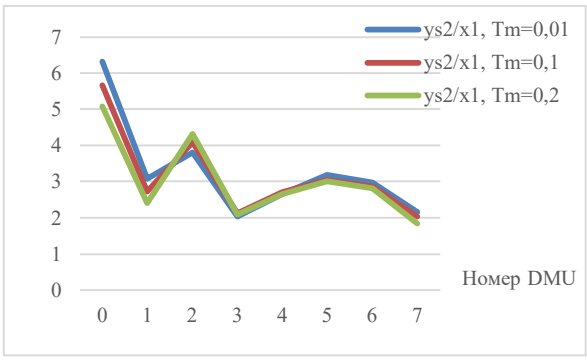
(2) После того, как достигнута нижняя граница значения таймаута, если выполняется следующее условие: во входном буфере есть конец пакета и буфер полон. В этом случае текущий пакет блокирует передачу следующего уже имеющегося пакета в рассматриваемом маршрутизаторе (также возможно, что заблокирован трафик, находящийся в предыдущих маршрутизаторах).

(3) После того, как достигнута нижняя граница значения таймаута, если выполняется следующее условие: во входном буфере есть более одного конца пакета (в отличие от (2) буфер при этом может быть не полон). В этом случае текущий пакет блокирует передачу следующего уже имеющегося пакета в рассматриваемом маршрутизаторе

(4) После того, как достигнута нижняя граница значения таймаута, если выполняется следующее условие: входной буфер пуст и текущий пакет не закончился. Своим существованием текущий пакет заблокировал движение следующего за ним в предыдущем (одном из предыдущих) маршрутизаторе, и также потенциально возможны блокировки в следующих маршрутизаторах (которых достигло начало пакета)



а) соотношение Yl2/x1



б) соотношение Ys2/x1

Рис. 3. Соотношение количества потерянных пакетов yl2 и ys2 и площади реализации для эксперимента 1 при разных значениях нижней границы таймаута

(5) Вариант, в котором поддерживаются варианты (0)–(4)

(6) После того, как достигнута нижняя граница значения таймаута, если выполняется следующее условие: предыдущий пакет с таким же адресом уже пришлось отбросить (или некоторое количество предыдущих пакетов уже пришлось сбросить)

(7) Вариант, в котором поддерживаются варианты (0)–(4), (6)

Для выбора варианта реализации и для выбора значения нижней границы таймаута может быть выполнена оценка эффективности с использованием DEA (управление верхней границей таймаута не рассматривается, поскольку для систем с требованиями реального времени он является фиксированным. Он определяется в соответствии с максимально допустимым временем доставки данных).

Для того, чтобы получить значения параметра x1 для каждого варианта контроллера была реализована RTL модель и выполнен ею синтез для оценки площади.

Оценка групп параметров y1 и y2 выполнялась с использованием аналитических и имитационных моделей соответствующих сетей (на обоих типах моделей были получены результаты, отличающиеся друг от друга не более, чем на 5%).

Для всех DMU во всех экспериментах использовалось 10 потоков пакетов, для одного из потоков выполнялся ошибочный сценарий. Каждый из десяти источников отправлял 1000 пакетов, суммарно отправлялась 10000 пакетов (увеличение количества отправляемых пакетов не оказывает сколько-нибудь заметного влияния на получаемые результаты). Интервалы между отправками последовательных пакетов в одном потоке использовались примерно одинаковые (Tr±Td).

Для каждого MDU были выполнены следующие эксперименты (данный перечень экспериментов не является исчерпывающим, выбран для примера, ряд параметров, которые потенциально могли бы использоваться в качестве входных, имеют фиксированные значения для того, чтобы ограничить объём рассматриваемых вариантов):

(эксперимент 0): сценарий 0, передача длинных пакетов (существенно длиннее размера буфера в маршрутизаторе), ошибка возникает 1 раз в 10 пакетов, продолжительность действия ошибки немного превосходит размер таймаута;

(эксперимент 1): сценарий 0, передача коротких пакетов (короче размера буфера в маршрутизаторе), ошибка возникает 1 раз в 10 пакетов, продолжительность действия ошибки немного превосходит размер таймаута;

(эксперимент 2): сценарий 0, передача длинных пакетов, ошибка возникает 1 раз в 10 пакетов, продолжительность действия ошибки существенно превосходит размер таймаута;

(эксперимент 3): сценарий 1, передача длинных пакетов, ошибка возникает 1 раз в 10

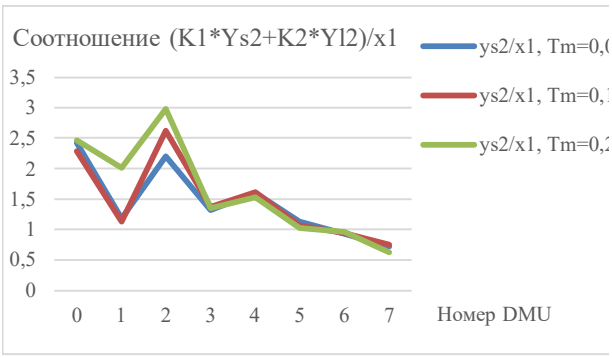


Рис. 4. Соотношение взвешенной суммы выходных параметров и входного параметра x1

пакетов, продолжительность действия ошибки не существенно превосходит размер таймаута.

Рассмотрим несколько оценок, выполненных с использованием предложенной методики.

Соотношение yl2/x1 (графики представлены на рис. 3, *а*) позволяет оценить влияние потока, для которого возник ошибочный сценарий, на остальные потоки. Как видно из этих графиков, лучшие (наименьшие) значения получены для DMU 5–7. (Они близки к идеальному значению, которое может быть достигнуто при использовании режима потоковой передачи.) Полученные результаты слабо зависят от выбора значений таймаута. Соотношение ys2/x1 (графики представлены на рис. 3, *б*) позволяет оценить общее количество потерянных пакетов в отношении к площади реализации. Как можно видеть из этих графиков, лучшие значения получены для DMU 3 и 7 (лучшими оказались другие DMU, чем в предыдущем случае).

Если необходимо выбрать вариант реализации DMU с учётом обоих выходных параметров, то может быть использована их взвешенная сумма:

$$E = (K1 \cdot y1 + K2 \cdot y2) / (x1). \quad (2)$$

Значение K1 и K2 определяется пользователем (разработчиком системы) в зависимости от того, какой из этих параметров для него является более важным (какой-то из этих коэффициентов потенциально может быть равен 0, если пользователю не нужен соответствующий параметр). На рис. 4 представлены графики зависимости при K1 = 0,3 и K2 = 0,7. В данном случае лучшим оказывается DMU 7.

Сравнение этих результатов, с результатами, полученными для DMU, в котором реализован классический механизм таймаутов (ys2 = 25,5, yl2 = 18,9) и потоковый режим (ys2 = 10, yl2 = 0) показывает, что использование DMU с потоковым режимом позволяет обеспечить полную независимость потоков данных при достаточно большом количестве потерянных пакетов. А механизм таймаутов, который был специально предложен в исходном стандарте для парирования взаимозависимостей между потоками, оказывается самым худшим и по общему количеству потерянных пакетов, и по уровню взаимозависимости.

Если в системе может возникать несколько сценариев, то оценка эффективности DMU может быть выполнена по следующей формуле:

$$Em = sum(i = 0, N - 1; Pi \cdot E(i)), \quad (3)$$

где N — количество сценариев некорректного поведения, для рассматриваемого примера N = 4; Pi — вероятность возникновения сценария, суммарная вероятность всех сценариев:

$$Sum(i = 0, N - 1; Pi) = 1. \quad (4)$$

Таким образом, предложенная методика может быть адаптирована для выполнения оценок в соответствии с параметрами, которые наиболее важны при разработке конкретной системы (класса систем), позволяет учесть возможные различные сценарии поведения системы в ходе эксплуатации.

Заключение

В статье предложена методика, позволяющая оценить эффективность существующих в стандарте SpaceFibre и новых предлагаемых механизмов для обеспечения независимости потоков пакетов, передаваемых по виртуальной сети SpaceFibre и использующих общие ресурсы, обоснован выбор критерия независимости. Предложена классификация типов входных параметров по отношению к процессу оптимизации. Данная методика обеспечивает возмож-

ность учитывать различных типы и количество входных параметров, различное количество выходных параметров. Оценки могут выполняться для разных параметров по отдельности или интегрально, для групп параметров.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение №FSRF-2023-0003, «Фундаментальные основы построения помехозащищённых систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга»

Литература

1. SpaceFibre - Very high-speed serial link. ECSS-E-ST-50-11C. ESA-ESTEC. Noordwijk, The Netherlands. 2019. 233 p.

2. *Zulkifli N., Sapit A., Mohammed A. N.* Development of small scale cluster computer for numerical analysis // CFDRI 2017, IOP Conference Series: Materials Science and Engineering. 2017. 6 p.

3. Deploying HPC Cluster with Mellanox InfiniBand Interconnect Solutions. Mellanox Technologies. 2017. 40 p.

4. *Liu J., Huang J., Lv W., Wang J.* APS: Adaptive packet spraying to isolate mix-flows in data center network // IEEE Trans Cloud Computing. 2020. Pp. 1–14.

5. *Shan D., Jiang W., Ren F.* Analyzing and enhancing dynamic threshold policy of data center switches // IEEE Transactions in Parallel Distributed Systems. 2017. Vol. 28, Iss. 9. Pp. 2454–2470.

6. *Baldi M., Sapio A.* Network Function Modelling and Performance Estimation // International Journal of Electrical and Computer Engineering. 2018. 17 p.

7. *Koleini S., Pahlevanzadeh B.* Enhancing High-Performance Computing (HPC) Security: A Comprehensive Review of Detection and Protection Strategies // Journal of Distributed Computing and Systems(JDCS). 2024. Pp. 12–24.

8. *Hyungro L., Luanzheng G., Meng T., Jesun F., Nathan T., Kougkas A., Xian-He S.* Data Flow Lifecycles for Optimizing Workflow Coordination // Proc. of the Intern. Conf. for High Performance Computing, Networking, Storage and Analysis. 2023. 15 p.

9. *Liu G., Wang Z., Zhou A. C., Mao R.* Adaptive key partitioning in distributed stream processing // CCF Trans. on High Perform. Computing. 2024. Pp. 164–178.

10. *Liang L., Filgueira, R., Yan Y., Heinis T.* Scalable Adaptive Optimizations for Stream-based Workflows in Multi-HPC-Clusters and Cloud Infrastructures // Future Generation Computer Systems. 2022. Pp. 102–116.

11. Sartori F., Lacerda D.P., Camargo L.F.R. Analysis and Management of Productivity and Efficiency in Production Systems for Goods and Services // CRC Press. 2020. 350 p.

12. *Čiković K. F., Lozic J.* Application of Data Envelopment Analysis (DEA) in Information and Communication Technologies // Tehnički glasnik. 2022. No. 16(1). Pp. 129–134

13. *da Silva A., de Carvalho F. M. R., Silva M. F. A., Ximenes D. E.* A new multiple criteria data envelopment analysis with variable return to scale: Applying bi-dimensional representation and super-efficiency analysis // Europ. J. of Operational Research. 2024. Pp. 308–322.

Поступила 3 марта 2025 г.

English

A METHODOLOGY FOR SELECTING ADAPTIVE FLOW CONTROL FOR SPACEFIBRE NETWORK NODES

Elena Alexandrovna Suvorova — PhD in Engineering, Associate Professor, Saint-Petersburg State University of Aerospace Instrumentation.
E-mail: wildcat15@yandex.ru

Vadim Borisovich Polyakov — Grand Dr. in Engineering, Associate Professor, Saint-Petersburg State University of Aerospace Instrumentation.

Address: 190000, Russian Federation, Saint Petersburg, Bolshaya Morskaya St., 67, building A.

Abstract: In most high-performance distributed computing systems, there is a need to transfer a large number of independent data flows (streams). In the SpaceFibre standard, the independent transmission of data flows is ensured through the use of virtual networks (virtual channels). The standard provides support for 64 virtual networks, which many times less than the number of data flows in modern high performance computing systems. As a result, it is necessary to ensure the independence of data flows transmitted within the same virtual network. There are two mechanisms in the standard – the Streaming mode and the timeout based mechanism, which can potentially be used to eliminate unplanned interaction of flows. The article suggests additional mechanisms for adaptive flow control that allow us to control the achievable characteristics. This article evaluates, compares the capabilities

of these mechanisms, and evaluates achievable characteristics depending on various scenarios of events that may provoke unplanned interaction of flows. Additional hardware costs are required to implement these mechanisms. The article proposes a methodology for evaluating the effectiveness of existing and proposed mechanisms in the standard based on Data Envelope Analysis. It allows the developer to choose the mechanisms taking into account the allowable hardware costs and the likelihood of various scenarios leading to unplanned effects characteristic of the system being developed.

Keywords: SpaceFibre, dynamic reconfiguration, real-time networks, DEA, adaptive data flow control, high performance computing systems.

The work was carried out with the financial support of the Ministry of Science and Higher Education of the Russian Federation, agreement No. FSRF-2023-0003, "Fundamental Principles of Building Noise-Resistant Systems of Space and Satellite Communications, Relative Navigation, Technical Vision, and Aerospace Monitoring"

References

1. SpaceFibre - Very high-speed serial link. ECSS-E-ST-50-11C. ESA-ESTEC. Noordwijk, The Netherlands. 2019. 233 p.

2. *Zulkifli N., Sapit A., Mohammed A. N.* Development of small scale cluster computer for numerical analysis. CFDRI 2017, IOP Conference Series: Materials Science and Engineering. 2017. 6 p.

3. Deploying HPC Cluster with Mellanox InfiniBand Interconnect Solutions. Mellanox Technologies. 2017. 40 p.

4. *Liu J., Huang J., Lv W., Wang J.* APS: Adaptive packet spraying to isolate mix-flows in data center network. IEEE Trans Cloud Computing. 2020. Pp. 1–14.

5. *Shan D., Jiang W., Ren F.* Analyzing and enhancing dynamic threshold policy of data center switches. IEEE Transactions in Parallel Distributed Systems. 2017. Vol. 28, Iss. 9. Pp. 2454–2470.

6. *Baldi M., Sapio A.* Network Function Modelling and Performance Estimation. International Journal of Electrical and Computer Engineering. 2018. 17 p.

7. *Koleini S., Pahlevanzadeh B.* Enhancing High-Performance Computing (HPC) Security: A Comprehensive Review of Detection and Protection Strategies. Journal of Distributed Computing and Systems(JDCS). 2024. Pp. 12–24.

8. *Hyungro L., Luanzheng G., Meng T., Jesun F., Nathan T., Kougkas A., Xian-He S.* Data Flow Lifecycles for Optimizing Workflow Coordination. Proc. of the Intern. Conf. for High Performance Computing, Networking, Storage and Analysis. 2023. 15 p.

9. *Liu G., Wang Z., Zhou A. C., Mao R.* Adaptive key partitioning in distributed stream processing. CCF Trans. on High Perform. Computing. 2024. Pp. 164–178.

10. *Liang L., Filgueira, R., Yan Y., Heinis T.* Scalable Adaptive Optimizations for Stream-based Workflows in Multi-HPC-Clusters and Cloud Infrastructures. Future Generation Computer Systems. 2022. Pp. 102–116.

11. Sartori F., Lacerda D.P., Camargo L.F.R. Analysis and Management of Productivity and Efficiency in Production Systems for Goods and Services. CRC Press. 2020. 350 p.

12. *Čiković K. F., Lozic J.* Application of Data Envelopment Analysis (DEA) in Information and Communication Technologies. Tehnički glasnik. 2022. No. 16(1). Pp. 129–134

13. *da Silva A., de Carvalho F. M. R., Silva M. F. A., Ximenes D. E.* A new multiple criteria data envelopment analysis with variable return to scale: Applying bi-dimensional representation and super-efficiency analysis. Europ. J. of Operational Research. 2024. Pp. 308–322.