

УДК 004.057.4

doi: 10.17586/2226-1494-2020-20-4-568-575

ОРГАНИЗАЦИЯ РЕЗЕРВИРОВАНИЯ ПАКЕТОВ ПРИ МНОГОПУТЕВЫХ ПЕРЕДАЧАХ РЕАЛЬНОГО ВРЕМЕНИ

И.И. Носков

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
 Адрес для переписки: noskovii@mail.ru

Информация о статье

Поступила в редакцию 17.05.20, принята к печати 19.06.20
 Язык статьи – русский

Ссылка для цитирования: Носков И.И. Организация резервирования пакетов при многопутевых передачах реального времени // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 4. С. 568–575. doi: 10.17586/2226-1494-2020-20-4-568-575

Аннотация

Предмет исследования. Исследованы механизмы организации резервированных многопутевых передач в компьютерных сетях. **Метод.** Разработан протокол прикладного уровня, позволяющий увеличить вероятность своевременной и безошибочной доставки данных в компьютерных сетях, функционирующих в условиях ограничений на время доставки, за счет использования резервированных многопутевых передач копий пакетов по разным каналам связи. **Основные результаты.** Разработан протокол, работающий поверх UDP и позволяющий выполнять резервированные многопутевые передачи. Исследование эффективности предложенного решения базируется на имитационном моделировании в среде OMNeT++. Разработаны модели предложенного протокола и компьютерной сети с возможностью резервированных передач. Проведены эксперименты и определены области эффективного использования разработанного протокола. В качестве критерия эффективности выбран мультипликативный критерий, отражающий запас времени безошибочно и своевременно переданных пакетов. Разработанный протокол показал эффективность при различных сценариях работы, в которых варьировались кратность резервирования и интенсивность поступления пакетов. **Практическая значимость.** Разработанные в данной работе алгоритмы и механизмы могут быть использованы для программной реализации протокола, осуществляющего резервированные многопутевые передачи с целью использования его в киберфизических системах реального времени.

Ключевые слова

сетевые протоколы, резервированные многопутевые передачи, UDP, ограничения на время доставки, вероятность доставки, системы реального времени

doi: 10.17586/2226-1494-2020-20-4-568-575

PACKET RESERVATIONS IN REAL-TIME MULTIPATH TRANSMISSIONS

I.I. Noskov

ITMO University, Saint Petersburg, 197101, Russian Federation
 Corresponding author: noskovii@mail.ru

Article info

Received 17.05.20, accepted 19.06.20
 Article in Russian

For citation: Noskov I.I. Packet reservations in real-time multipath transmissions. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2020, vol. 20, no. 4, pp. 568–575 (in Russian). doi: 10.17586/2226-1494-2020-20-4-568-575

Abstract

Subject of Research. The paper presents research of mechanisms of multipath redundant transmissions in computer networks. **Method.** The developed application level protocol gives the possibility to increase the probability of timely and faultless data delivery in computer networks which work within the conditions of delivery time limits using multipath redundant transmissions of packet copies via different channels. **Main Results.** The protocol with redundant multipath transmissions opportunity based on UDP transport protocol is developed. The efficiency analysis of the presented solutions is carried out on the basis of simulation modeling in OMNeT++ environment. Models of the proposed protocol and computer network with redundant transmissions opportunity are developed. Experiments with these models are carried out and efficiency area of the developed protocol application is determined. The multiplicative criterion that

shows time reserve of timely and faultless transmitted packets is used as an efficiency indicator. The presented protocol shows efficiency in various working cases with the intensity and redundancy coefficient change of packet arrival. **Practical Relevance.** The developed algorithms and mechanisms can be used for program implementation of protocol with redundant multipath transmissions aimed at its application in cyberphysic real-time systems.

Keywords

network protocols, multipath redundant transmissions, UDP, delivery time limits, delivery probability, real-time systems

Введение

В настоящее время наблюдается большой рост компьютерных сетей различного назначения, которые с каждым годом покрывают все большие площади и проникают в жизнь людей повсеместно. Возрастает количество сервисов с высоким уровнем доступности, предоставляющих свои услуги без перебоев в течение длительного времени. В этой связи естественно возрастают требования к надежности компьютерных сетей и их отказоустойчивости, что, в свою очередь, повышает интерес к вопросам оценки и повышения надежности [1–3], отказоустойчивости [4], безопасности [5], своевременности обслуживания [6] и производительности распределенных вычислительных систем и сетей различного прикладного назначения [7]. В промышленности требования к локальным вычислительным сетям (ЛВС) становятся все более серьезными, так как автоматизированные системы управления технологическим процессом (АСУ ТП) берут на себя все больший функционал, и потери данных могут повлечь серьезные издержки. В критически важных системах прерывание работы даже на миллисекунды может серьезно повлиять на работу системы. В стандарте МЭК 61850¹ указано, что на подстанциях не должна присутствовать потеря пакетов типа GOOSE и SMV. В стандарте МЭК 62439² установлено, что время восстановления связи на объектах должно быть менее 10 мс. Таким образом, наблюдается необходимость в разработке сетевых протоколов, повышающих вероятность безошибочной и своевременной доставки пакетов в компьютерных сетях, функционирующих в реальном масштабе времени.

В [8] приводится обзор современных достижений в области разработки протоколов транспортного уровня, позволяющих повысить надежность и отказоустойчивость компьютерных сетей. Основное внимание в данной работе уделяется развитию алгоритмов управления перегрузкой для лучшей производительности, описанию новых протоколов с установлением соединения и контролем передач, являющихся по сути доработками и аналогами протокола TCP (Transmission Control Protocol), а также описываются возможности многопутевой передачи на транспортном уровне с использованием протокола MPTCP (Multipath Transmission Control Protocol). В [9, 10] рассмотрены модификации протокола UDP (User Datagram Protocol) на прикладном уровне, представляющие собой сервисы с гарантией доставки и многопутевыми передачами. Описанные протоколы не адаптированы к передаче трафика, критичного к

задержкам и предназначенного для систем реального времени. Так, протоколы не предусматривают резервированные передачи для отправки критичных ко времени доставки пакетов по нескольким каналам связи одновременно. Данные протоколы разработаны поверх протокола UDP и доработаны для предоставления надежного сервиса с гарантией доставки. Однако нет протоколов с резервированными ненадежными передачами. Данные протоколы могут быть полезны в системах реального времени, где актуальность информации теряется очень быстро и нет возможности ждать повторных передач потерянных или искаженных пакетов, и приоритет отдается вновь прибывающим пакетам.

Надежность и своевременность передач в системах реального времени может быть обеспечена на основе концепции многопутевых резервированных передач (многопутевого резервированного обслуживания) [11–13], которая является развитием технологий широкополосного обслуживания [14, 15], многопутевой маршрутизации [16], многоадресных передач, транспортного кодирования [17] и динамического распределения запросов [18, 19].

В рамках концепции многопутевого резервированного обслуживания разработаны аналитические модели многопутевого резервированного обслуживания в кластерных и мультикластерных системах [11, 12], а также в сетях с многопутевой передачей [13]. В [11–13] показана концептуальная возможность обеспечить для систем реального времени на основе резервированного обслуживания повышение вероятности своевременного и безошибочного обслуживания, в [20, 21] эта возможность подтверждена результатами имитационного моделирования.

В настоящее время стоит задача привязки реализации концепции многопутевого резервированного обслуживания к конкретным протоколам, сетевому оборудованию и к программному обеспечению, в том числе к операционным системам.

Целью данной работы является разработка протокола, работающего поверх UDP и обеспечивающего резервированные передачи для увеличения вероятности своевременной и безошибочной доставки пакетов в компьютерных сетях, функционирующих в условиях ограничений на время доставки.

Для достижения указанной цели необходимо проанализировать существующие решения и выбрать уровень сетевой модели, на котором будет работать протокол, разработать структуру заголовка протокола и описать алгоритм его работы на стороне отправителя и приемника. Для доказательства эффективности разработанного протокола необходимо разработать имитационные модели в среде OMNeT++, провести эксперименты и выделить области эффективного использования в условиях ненадежности передач.

¹ МЭК 61850 стандарт «Сети и системы связи на подстанциях».

² МЭК 62439 стандарт «Промышленные сети связи. Сети с высокой готовностью к автоматической обработке».

Объект и задачи работы

Объектом исследования является компьютерная сеть, состоящая из n каналов связи (канал $0-n$) между отправителем (Клиент) и получателем (Сервер), в которой действует ограничение на время доставки пакетов. В каналах связи возможны ошибки и искажения передаваемых данных от отправителя к получателю. Данная сеть представлена на рис. 1.

Предполагается, что в данной сети уже есть резервные каналы связи с подключенным к ним оборудованием, которые могут быть использованы для холодного резерва и (или) связи с другими узлами сети. Таким образом, необходимо разработать протокол, позволяющий выполнять резервированные передачи через заданное число каналов для увеличения вероятности своевременной и безошибочной доставки данных без экономических затрат на покупку дополнительного сетевого оборудования.

Разработка протокола резервированных многопутевых передач

Концепция резервированных передач заключается в передаче копий пакетов по нескольким резервным каналам [13]. В качестве развития этого направления в работах [22–24] разработаны и изучены модели компьютерных сетей в среде OMNeT++, позволяющие выполнять резервированные передачи на базе протокола UDP в компьютерных сетях, функционирующих в условиях ограничений на время доставки. В данных работах авторы на примерах показывают эффективность резервированных передач в системах реального времени и выделяют области целесообразного использования данного механизма. Разработка архитектуры протокола, позволяющего выполнять резервированные передачи, с целью его дальнейшей программной реализации и использования в реальных системах, является актуальной и важной задачей.

Все протоколы сетевого и транспортного уровней, как правило, реализованы в ядре операционных систем и предоставляют API (Application Programming Interface) для работы с этими протоколами приложениям на прикладном уровне. Реализация новых протоколов на сетевом и транспортном уровнях требует изменения кода ядра взаимодействующих узлов, что является трудной задачей для развертывания, поэтому создание протоколов прикладного уровня, функцио-

нирующих на базе протоколов транспортного уровня, является приоритетным направлением [25–27].

Для реализации протокола с резервированными передачами предполагается использовать UDP-протокол транспортного уровня, так как данный протокол функционирует без установления соединения и не инициирует повторных передач при потерях. Использование протокола TCP не представляется возможным, поскольку теряется актуальность передаваемых данных за период времени, в течение которого будет определена потеря пакета, и повторно инициирован процесс передачи, что является очень важным в системах реального времени. На рис. 2 показана схема резервированной отправки данных с привязкой к протоколам и уровням модели TCP/IP для отправителя и приемника. В качестве протокола сетевого уровня подразумевается использование протокола IP (Internet Protocol) в качестве канального/физического – Ethernet. Протоколы данных уровней не обозначены на рисунке, так как они не добавляют дополнительной ясности в понимании работы протокола MRUT (Multipath Redundant UDP Transmissions).

Согласно рис. 2, протокол MRUT создает k копий передаваемого пакета (в соответствии с количеством доступных каналов для передачи и эффективным значением кратности передачи), после чего происходит отправка пакетов в UDP-сокеты. До узла назначения могут дойти не все пакеты, что обусловлено потерями и искажениями в канале передачи данных. При получении дубликатов одного и того же пакета, протокол MRUT детектирует и отбрасывает лишние пакеты и передает пользователю только один экземпляр.

На уровне протокола MRUT пользователь задает количество резервных каналов, по которым будет происходить передача данных. Так как протокол работает поверх UDP, на стороне приемной стороны создается необходимое количество соединений (UDP-сокетов), готовых принимать пакеты от отправителя. На стороне отправителя при отправке порции данных от пользователя, протокол создает копии каждого пакета и отправляет их через заданное пользователем количество резервных каналов посредством передачи данных в UDP-сокеты, функционирующие в рамках текущей резервированной передачи.

Протокол сетевого уровня IP предусматривает возможность фрагментации передаваемых пакетов на промежуточном сетевом оборудовании при превышении пакетом максимального размера пакета MTU (Maximum Transmission Unit), который может передать сетевой

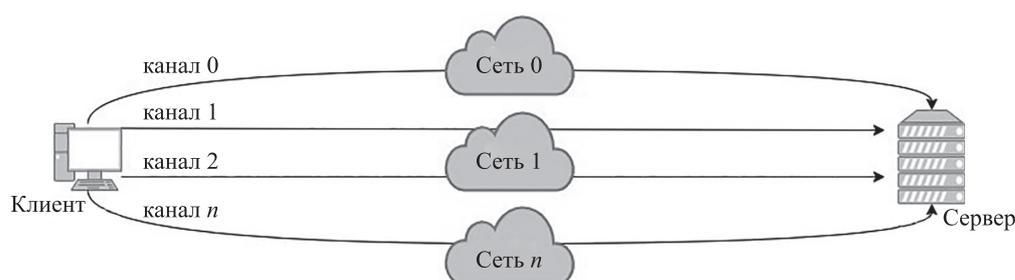


Рис. 1. Компьютерная сеть с резервными каналами

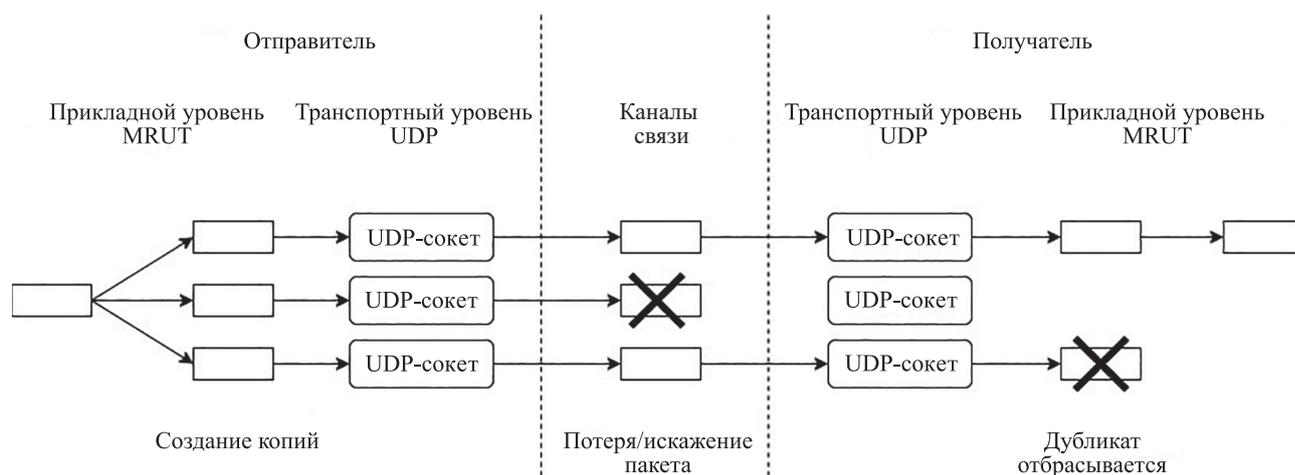


Рис. 2. Схема резервированной отправки данных

интерфейс. Однако, если в IP-заголовке пакета выставлен флаг «Не фрагментировать», то при размере пакета большем, чем MTU, пакет будет отброшен. Пакет также может быть отброшен еще на транспортном уровне протоколом UDP, так как в работе данного протокола предусмотрен механизм Path MTU Discovery, который определяет минимальный размер MTU для всего пути до адресата и сравнивает это значение с размером датаграммы, которую пользователь отправил в UDP-сокет. Если размер датаграммы больше, то пакет будет отброшен. При отключении данной функции датаграмма любого размера будет передана протоколу сетевого уровня, который фрагментирует ее и отправит по частям или отбросит. Также пакет может быть отброшен дальше по пути следования, что не является хорошим исходом для систем реального времени, где необходимо получение всех без исключения пакетов с минимальной задержкой. В работе [28] показана эффективность использования сегментации пакетов при резервированных передачах. В протоколе MRUT предлагается выполнять Path MTU Discovery и фрагментировать пакет на прикладном уровне, что позволит избежать фрагментации на сетевом уровне. Реализация данного подхода отражена на рис. 3 (темным цветом показаны фрагменты, потерянные в процессе передачи).

Фрагментация пакета на уровне протокола MRUT позволяет собрать пакет на стороне получателя, фрагменты которого получены по разным каналам связи. Для реализации данного функционала в заголовке пред-

лагаемого протокола необходимо учесть Fragment ID и Fragment Count, чтобы приемник смог зарезервировать буфер под входящие пакеты и определить момент, когда все фрагменты пакета получены. Для идентификации дублированных пакетов, которые пришли по нескольким каналам в заголовок необходимо добавить поле Packet ID. Пакеты с одинаковым Packet ID, принятые через разные каналы связи будут отброшены на стороне приемника как ненужные дубликаты. На рис. 4 представлен заголовок протокола MRUT и схема его инкапсуляции в существующие протоколы стека TCP/IP.

Перед отправкой пользователь задает сетевые интерфейсы, через которые планируется выполнять резервированные передачи пакетов, после чего передача идет по заданным каналам между отправителем и получателем.

На рис. 5 приведены диаграммы деятельности отправителя и получателя.

Перед отправкой данных протокол сравнивает размер пакета с минимальным значением MTU на пути к получателю. Затем пакет фрагментируется протоколом MRUT в соответствии с размером MTU, формируется заголовок к каждому фрагменту, после чего они отправляются по всем заданным резервным каналам.

Получатель принимает пакеты по всем резервным каналам, удаляя дубликаты уже полученных пакетов. Для приема фрагментированных пакетов предусмотрен механизм буферизации и сборки пакета из фрагментов перед передачей пользователю.

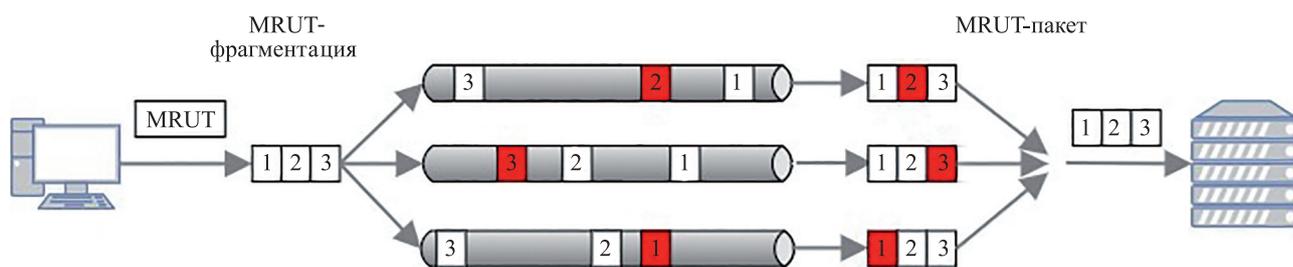


Рис. 3. Передача пакета с фрагментацией на уровне MRUT-протокола

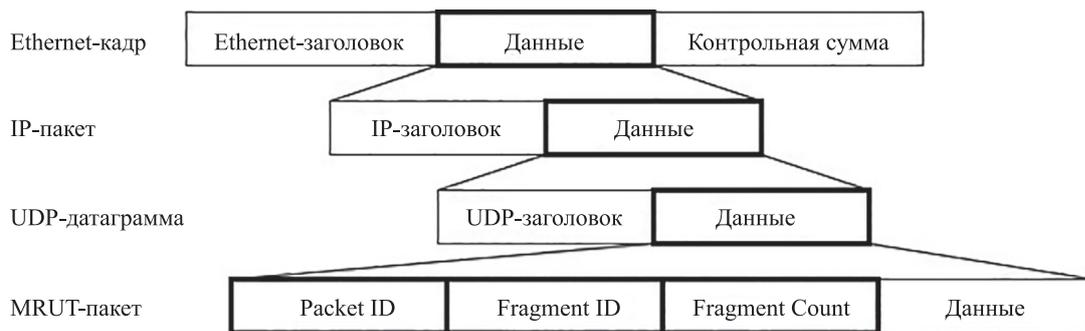


Рис. 4. Структура MRUT-пакета и его инкапсуляция в протоколы стека TCP/IP

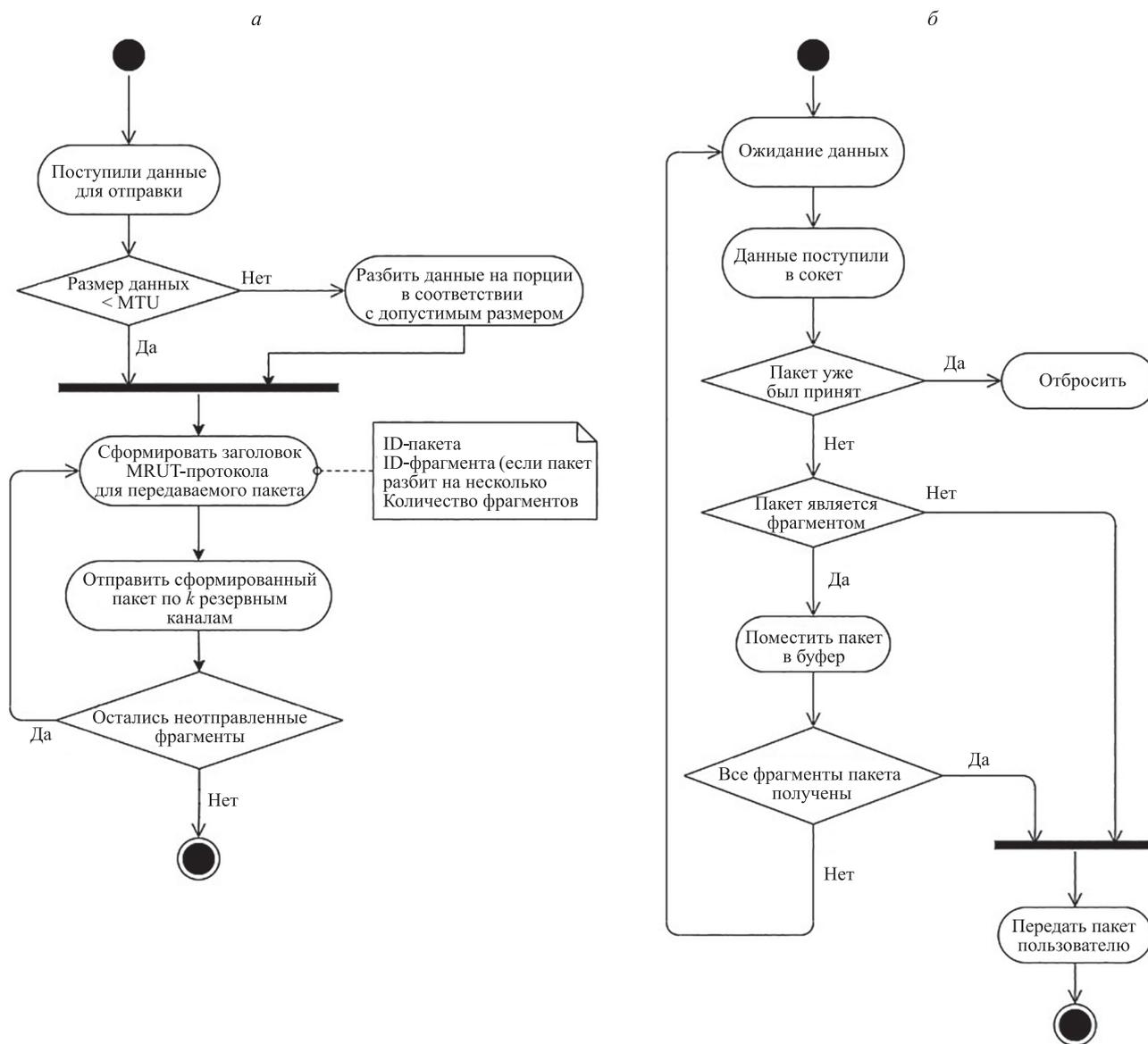


Рис. 5. UML-диаграммы деятельности отправителя (а) и получателя (б)

Исследование эффективности работы протокола резервированных многопутевых передач в среде OMNeT++

Для исследования эффективности разработанного протокола в среде OMNeT++ разработаны модели,

представляющие собой алгоритм его работы на стороне отправителя и получателя. Таким образом, в разработанной модели пользователь может осудать количество каналов связи, по которым будет осуществляться резервированная передача данных между клиентом и сервером. На рис. 6 приведена модель исследуемой ком-

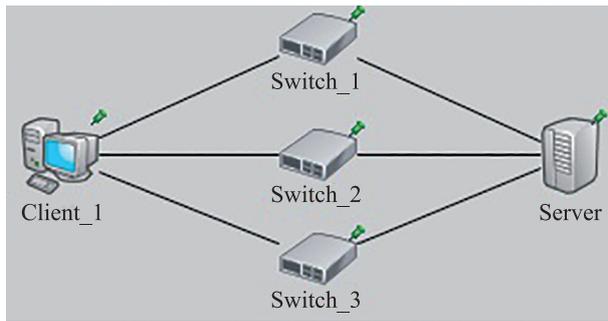


Рис. 6. Модель компьютерной сети в среде OMNeT++

пьютерной сети в среде OMNeT++. Резервированная передача в сети осуществляется через коммутаторы (Switch).

В качестве критерия эффективности резервированных передач был выбран критерий $M = P(t_0 - T)$, отражающий запас времени безошибочно и своевременно переданных пакетов от клиента к серверу, где P — вероятность своевременной и безошибочной доставки пакета (определяется имитационно); t_0 — ограничение времени на своевременную доставку, приемлемое для заданной системы; T — среднее время пребывания пакета в системе.

Проведен ряд экспериментов с заданными параметрами и варьированием кратности резервирования: $L = 10$ Мбит/с — пропускная способность каналов связи; $t_0 = 0,0005$ с — запас времени на доставку; $B = 0,0001$ — вероятность битовой ошибки в канале; λ — интенсивность поступления пакетов (варьируется при проведении экспериментов); длина пакетов для всего процесса моделирования принята равной 100 Б.

На рис. 7 представлены графики зависимости критерия M от кратности резервирования передач K при интенсивности поступления пакетов 1000 1/с и 2000 1/с.

Из полученного графика (рис. 7, кривая 1) при $\lambda = 1000$ 1/с видно, что при использовании резервированных передач в рамках разработанного протокола критерий эффективности M принимает большие значения, чем без использования резервированных передач. Что говорит об увеличении вероятности своевременной

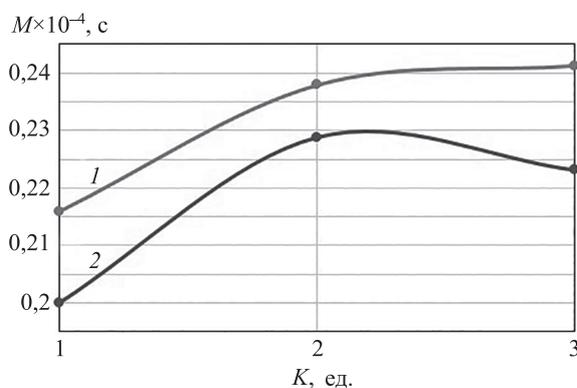


Рис. 7. Зависимость критерия эффективности M от кратности резервирования K при интенсивности λ : 1000 1/с (кривая 1); 2000 1/с (кривая 2)

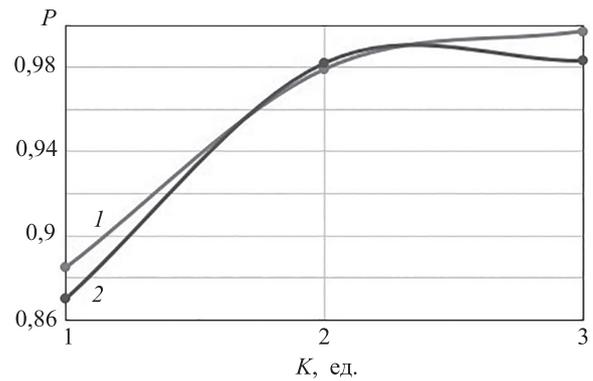


Рис. 8. Зависимость вероятности (P) своевременной и безошибочной доставки от кратности резервирования K при интенсивности: 1000 1/с (кривая 1); 2000 1/с (кривая 2)

и безошибочной доставки данных. При интенсивности $\lambda = 2000$ 1/с (рис. 7, кривая 2) протокол также показывает лучшие результаты, используя резервированные передачи. Однако значение критерия эффективности при $K = 3$ меньше, чем при $K = 2$, что говорит о дополнительных задержках в приемных буферах на стороне сервера, связанных с увеличившимся потоком трафика при резервированных передачах.

На рис. 8 изображены графики зависимости вероятности (P) своевременной и безошибочной доставки от кратности резервирования при различном значении интенсивности поступления пакетов.

Из полученных графиков (рис. 8) видно, что вероятность своевременной и безошибочной доставки растет при любой интенсивности. В данном случае не учитывается запас по времени относительно заданного лимита как в мультипликативном критерии M . Для $\lambda = 2000$ 1/с при использовании $K = 3$ нет значительного увеличения вероятности своевременной и безошибочной доставки относительно $K = 2$, что говорит об увеличении времени доставки пакетов из-за роста очередей сетевого оборудования при большей интенсивности поступления пакетов.

Заключение

В работе разработан протокол, работающий поверх UDP и обеспечивающий резервированные передачи для увеличения вероятности своевременной и безошибочной доставки пакетов в компьютерных сетях, функционирующих в условиях ограничений на время доставки. Протокол предусматривает отслеживание размера MTU (Maximum Transmission Unit) по пути следования пакетов и фрагментирует пакеты на прикладном уровне, что увеличивает вероятность доставки за счет того, что пакет не будет отброшен на промежуточном узле сетевым протоколом по превышению значения MTU, а также это позволит восстановить пакет по пришедшим с разных сетевых интерфейсов фрагментам, что невозможно при использовании фрагментации на сетевом уровне, так как на данном уровне пакеты собираются только из фрагментов, пришедших на один и тот же сетевой интерфейс. На стороне получателя протокол позволяет контролировать прием фрагментов и дубликатов

пакетов, передавая пользователю только уникальные пакеты.

Эффективность использования разработанного протокола показана путем имитационного моделирования в среде OMNeT++. Для этого была разработана модель протокола с возможностью резервированных передач, и проведены эксперименты при различной интенсивности поступления пакетов. Построены зависимости мультипликативного критерия, отражающего запас

времени безошибочно и своевременно переданных пакетов, а также вероятности безошибочно и своевременно переданных пакетов от кратности резервирования.

В дальнейшем планируется создать программную реализацию данного протокола на основе алгоритмов и диаграмм, разработанных в данной статье, после чего проанализировать эффективность ее работы на реальных системах.

Литература

1. Aysan H. *Fault-Tolerance Strategies and Probabilistic Guarantees for Real-Time Systems*. Vasteras, Sweden, Malardalen University, 2012. 190 p.
2. Cheng S.T., Chen C.M., Tripathi S.K. Fault-tolerance model for multiprocessor real-time systems // *Journal of Computer and System Sciences*. 2000. V. 61. N 3. P. 457–477. doi: 10.1006/jcss.2000.1704
3. Татарникова Т.М. Аналитико-статистическая модель оценки живучести сетей с топологией mesh // *Информационно-управляющие системы*. 2017. № 1(86). С. 17–22. doi: 10.15217/issnl684-8853.2017.1.17
4. Shooman M.L. *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*. John Wiley & Sons, 2002. 552 p.
5. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза. Ульяновск: Областная типография «Печатный двор», 2016. 544 с.
6. Татарникова Т.М., Елизаров М.А. Модель оценки временных характеристик при взаимодействии в сети интернета вещей // *Информационно-управляющие системы*. 2017. № 2(87). С. 44–50. doi: 10.15217/issnl684-8853.2017.2.44
7. Tatarnikova T.M., Kutuzov O.I. Model of a self-similar traffic generator and evaluation of buffer storage for classical and fractal queuing system // *Proc. 1st Moscow Workshop on Electronic and Networking Technologies (MWENT 2018)*. 2018. P. 1–3. doi: 10.1109/MWENT.2018.8337306
8. Polese M., Chiariotti F., Bonetto E., Rigotto F., Zanella A., Zorzi M. A survey on recent advances in transport layer protocols // *IEEE Communications Surveys and Tutorials*. 2019. V. 21. N 4. P. 3584–3608. doi: 10.1109/COMST.2019.2932905
9. Iyengar J., Thomson M. QUIC: A UDP-based multiplexed and secure transport // IETF, Working Draft: draft-ietf-quic-transport-08, Dec. 2017 [Электронный ресурс]. URL: <https://tools.ietf.org/id/draft-ietf-quic-transport-08.txt> (дата обращения: 28.05.2020).
10. Viernickel T., Froemmgen A., Rizk A., Koldehofe B., Steinmetz R. Multipath QUIC: A deployable multipath transport protocol // *Proc. IEEE International Conference on Communications (ICC 2018)*. 2018. P. 8422951. doi: 10.1109/ICC.2018.8422951
11. Bogatyrev V.A., Bogatyrev A.V. Functional reliability of a real-time redundant computational process in cluster architecture systems // *Automatic Control and Computer Sciences*. 2015. V. 49. N 1. P. 46–56. doi: 10.3103/S0146411615010022
12. Богатырев В.А., Богатырев А.В. Модель резервированного обслуживания запросов реального времени в компьютерном кластере // *Информационные технологии*. 2016. Т. 22. № 5. С. 348–355.
13. Богатырев В.А., Богатырев С.В. Резервированная передача данных через агрегированные каналы в сети реального времени // *Известия высших учебных заведений. Приборостроение*. 2016. Т. 59. № 9. С. 735–740. doi: 10.17586/0021-3454-2016-59-9-735-740
14. Lee M.H., Dudin A.N., Klimenok V.I. The SM/V/N queueing system with broadcasting service // *Mathematical Problems in Engineering*. 2006. V. 2006. P. 98171. doi: 10.1155/MPE/2006/98171
15. Dudin A.N., Sun' B. A multiserver MAP/PH/N system with controlled broadcasting by unreliable servers // *Automatic Control and Computer Sciences*. 2009. V. 43. N 5. P. 247–256. doi: 10.3103/S0146411609050046
16. Prasenjit Chanak, Tuhina Samanta, Indrajit Banerjee. Fault-tolerant multipath routing scheme for energy efficient wireless sensor networks // *International Journal of Wireless & Mobile Networks (IJWMN)*. 2013. V. 5. N 2. P. 33–45. doi: 10.5121/ijwmn.2013.5203
17. Krouk E., Semenov S. Application of coding at the network transport level to decrease the message delay // *Proc. 3rd International*

References

1. Aysan H. *Fault-Tolerance Strategies and Probabilistic Guarantees for Real-Time Systems*. Vasteras, Sweden, Malardalen University, 2012, 190 p.
2. Cheng S.T., Chen C.M., Tripathi S.K. Fault-tolerance model for multiprocessor real-time systems. *Journal of Computer and System Sciences*, 2000, vol. 61, no. 3, pp. 457–477. doi: 10.1006/jcss.2000.1704
3. Tatarnikova T.M. Analytical-statistical model of mesh network survivability evaluation. *Information and Control Systems*, 2017, no. 1(86), pp. 17–22. (in Russian). doi: 10.15217/issnl684-8853.2017.1.17
4. Shooman M.L. *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*. John Wiley & Sons, 2002, 552 p.
5. Shubinskii I.B. *Reliable Fault-Tolerant Information Systems. Synthesis Methods*. Ulyanovsk, Pechatnyj dvor Publ., 2016, 544 p. (in Russian)
6. Tatarnikova T.M., Elizarov M.A. Model of estimating temporal characteristics of IoT network interaction. *Information and Control Systems*, 2017, no. 2(87), pp. 44–50. (in Russian). doi: 10.15217/issnl684-8853.2017.2.44
7. Tatarnikova T.M., Kutuzov O.I. Model of a self-similar traffic generator and evaluation of buffer storage for classical and fractal queuing system. *Proc. 1st Moscow Workshop on Electronic and Networking Technologies (MWENT 2018)*, 2018, pp. 1–3. doi: 10.1109/MWENT.2018.8337306
8. Polese M., Chiariotti F., Bonetto E., Rigotto F., Zanella A., Zorzi M. A survey on recent advances in transport layer protocols. *IEEE Communications Surveys and Tutorials*, 2019, vol. 21, no. 4, pp. 3584–3608. doi: 10.1109/COMST.2019.2932905
9. Iyengar J., Thomson M. QUIC: A UDP-based multiplexed and secure transport. *IETF, Working Draft: draft-ietf-quic-transport-08, Dec. 2017*. Available at: <https://tools.ietf.org/id/draft-ietf-quic-transport-08.txt> (accessed: 28.05.2020).
10. Viernickel T., Froemmgen A., Rizk A., Koldehofe B., Steinmetz R. Multipath QUIC: A deployable multipath transport protocol. *Proc. IEEE International Conference on Communications (ICC 2018)*, 2018, pp. 8422951. doi: 10.1109/ICC.2018.8422951
11. Bogatyrev V.A., Bogatyrev A.V. Functional reliability of a real-time redundant computational process in cluster architecture systems. *Automatic Control and Computer Sciences*, 2015, vol. 49, no. 1, pp. 46–56. doi: 10.3103/S0146411615010022
12. Bogatyrev V.A., Bogatyrev A.V. The model of redundant service requests real-time in a computer cluster. *Informacionnye Tehnologii*, 2016, vol. 22, no. 5, pp. 348–355. (in Russian)
13. Bogatyrev V.A., Bogatyrev S.V. Redundant data transmission using aggregated channels in real-time network. *Journal of Instrument Engineering*, 2016, vol. 59, no. 9, pp. 735–740. (in Russian). doi: 10.17586/0021-3454-2016-59-9-735-740
14. Lee M.H., Dudin A.N., Klimenok V.I. The SM/V/N queueing system with broadcasting service. *Mathematical Problems in Engineering*, 2006, vol. 2006, pp. 98171. doi: 10.1155/MPE/2006/98171
15. Dudin A.N., Sun' B. A multiserver MAP/PH/N system with controlled broadcasting by unreliable servers. *Automatic Control and Computer Sciences*, 2009, vol. 43, no. 5, pp. 247–256. doi: 10.3103/S0146411609050046
16. Prasenjit Chanak, Tuhina Samanta, Indrajit Banerjee. Fault-tolerant multipath routing scheme for energy efficient wireless sensor networks. *International Journal of Wireless & Mobile Networks (IJWMN)*, 2013, vol. 5, no. 2, pp. 33–45. doi: 10.5121/ijwmn.2013.5203
17. Krouk E., Semenov S. Application of coding at the network transport level to decrease the message delay. *Proc. 3rd International*

- Symposium on Communication Systems Networks and Digital Signal Processing. Staffordshire University, UK, 2002. P. 109–112.
18. Богатырев В.А., Богатырев А.В., Богатырев С.В. Перераспределение запросов между вычислительными кластерами при их деградации // Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 54–58.
 19. Богатырев В.А., Богатырев С.В., Богатырев А.В. Оптимизация кластера с ограниченной доступностью кластерных групп // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2011. № 1(71). С. 63–67.
 20. Bogatyrev V.A., Parshutina S.A. Redundant distribution of requests through the network by transferring them over multiple paths // Communications in Computer and Information Science. 2016. V. 601. P. 199–207. doi: 10.1007/978-3-319-30843-2_21
 21. Bogatyrev V.A., Slastikhin I., The models of the redundant transmission through the aggregated channels // Advances in Computer Science Research. 2017. V. 72. P. 294–299. doi: 10.2991/itsmssm-17.2017.60
 22. Носков И.И., Богатырев В.А., Сластикхин И.А. Имитационная модель локальной компьютерной сети с агрегированием каналов и случайным методом доступа при резервировании передач // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 6(118). С. 1047–1053. doi: 10.17586/2226-1494-2018-18-6-1047-1053
 23. Носков И.И. Моделирование компьютерной сети с отказоустойчивым шлюзом в среде OMNeT++ // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 4. С. 673–679. doi: 10.17586/2226-1494-2019-19-4-673-679
 24. Noskov I.I., Bogatyrev V.A. Multipath redundant transmissions of critical to delays packets based on UDP protocol // CEUR Workshop Proceedings. 2020. V. 2590. P. 1–12.
 25. Carpenter B., Brim S. Middleboxes: Taxonomy and issues // IETF, RFC 3234, Feb. 2002 [Электронный ресурс]. URL: <https://rfc-editor.org/rfc/rfc3234.txt> (дата обращения: 03.06.2020).
 26. Edeline K., Donnet B. A first look at the prevalence and persistence of middleboxes in the wild // Proc. 29th International Teletraffic Congress (ITC). Genoa, Italy, 2017. V. 1. P. 161–168. doi: 10.23919/ITC.2017.8064352
 27. Papastergiou G., Fairhurst G., Ros D., Brunstrom A., Grinnemo K., Hurtig P., Khademi N., Tüxen M., Welzl M., Damjanovic D., Mangiante S. De-ossifying the Internet transport layer: A survey and future perspectives // IEEE Communications Surveys and Tutorials. 2017. V. 19. N 1. P. 619–639. doi: 10.1109/COMST.2016.2626780
 28. Богатырев В.А., Богатырев С.В. Эффективность резервирования и фрагментации пакетов при передаче по агрегированным каналам // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 165–170. doi: 10.17586/0021-3454-2017-60-2-165-170
 - Symposium on Communication Systems Networks and Digital Signal Processing. Staffordshire University, UK, 2002, pp. 109–112.
 18. Bogatyrev V.A., Bogatyrev A.V., Bogatyrev S.V. Requests redistribution between computing clusters under degradation. *Journal of Instrument Engineering*, 2014, vol. 57, no. 9, pp. 54–58. (in Russian)
 19. Bogatyrev V., Bogatyrev S., Bogatyrev A. Clusters optimisation with the limited availability of clusters groups. *Scientific and Technical Bulletin of St. Petersburg State University of Information Technologies, Mechanics and Optics*, 2011, no. 1(71), pp. 63–67. (in Russian)
 20. Bogatyrev V.A., Parshutina S.A. Redundant distribution of requests through the network by transferring them over multiple paths. *Communications in Computer and Information Science*, 2016, vol. 601, pp. 199–207. doi: 10.1007/978-3-319-30843-2_21
 21. Bogatyrev V.A., Slastikhin I., The models of the redundant transmission through the aggregated channels. *Advances in Computer Science Research*, 2017, vol. 72, pp. 294–299. doi: 10.2991/itsmssm-17.2017.60
 22. Noskov I.I., Bogatyrev V.A., Slastikhin I.A. Simulation model of local computer network with channel aggregation and random access method at redundant transfer. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 6, pp. 1047–1053 (in Russian). doi: 10.17586/2226-1494-2018-18-6-1047-1053
 23. Noskov I.I. Modeling of computer network with fault-tolerance gateway in OMNET++. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 4, pp. 673–679. (in Russian). doi: 10.17586/2226-1494-2019-19-4-673-679
 24. Noskov I.I., Bogatyrev V.A. Multipath redundant transmissions of critical to delays packets based on UDP protocol. *CEUR Workshop Proceedings*, 2020, vol. 2590, pp. 1–12.
 25. Carpenter B., Brim S. Middleboxes: Taxonomy and issues. *IETF, RFC 3234, Feb. 2002*. Available at: <https://rfc-editor.org/rfc/rfc3234.txt> (accessed: 03.06.2020).
 26. Edeline K., Donnet B. A first look at the prevalence and persistence of middleboxes in the wild. *Proc. 29th International Teletraffic Congress (ITC)*. Genoa, Italy, 2017, vol. 1, pp. 161–168. doi: 10.23919/ITC.2017.8064352
 27. Papastergiou G., Fairhurst G., Ros D., Brunstrom A., Grinnemo K., Hurtig P., Khademi N., Tüxen M., Welzl M., Damjanovic D., Mangiante S. De-ossifying the Internet transport layer: A survey and future perspectives. *IEEE Communications Surveys and Tutorials*, 2017, vol. 19, no. 1, pp. 619–639. doi: 10.1109/COMST.2016.2626780
 28. Bogatyrev V.A., Bogatyrev S.V. Effectiveness of redundancy and packet fragmentation in transmission via aggregated channels. *Journal of Instrument Engineering*, 2017, vol. 60, no. 2, pp. 165–170. (in Russian). doi: 10.17586/0021-3454-2017-60-2-165-170

Авторы

Носков Илья Игоревич — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0002-5489-4092, noskovii@mail.ru

Authors

Ilya I. Noskov — Postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0002-5489-4092, noskovii@mail.ru