ISSN 1684-8853 (print); ISSN 2541-8610 (online)

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНЫЙ ЖУРНАЛ

3(130)/2024

doi:10.31799/1684-8853-2024-3

ISSN 1684-8853 (print); ISSN 2541-8610 (online)

SCIENTIFIC JOURNAL

3(130)/2024

PEER REVIEWED JOURNAL

INFORMATSIONNO-UPRAVLIAIUSHCHIE SISTEMY (INFORMATION AND CONTROL SYSTEMS)

Contact information
The Editorial and Publishing Center, SUAI
67A, Bol'shaya Morskaia, 190000, Saint Petersburg, Russia
Website: http://i-us.ru/en, e-mail: ius.spb@gmail.com
Tel.: +7 - 812 494 70 02

The Journal was registered in the Ministry of Press, Broadcasting and Mass Media of the Russian Federation.
Registration Certificate JD № 77-12412 from April, 19, 2002.
Re-registration in the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) due to change of the founder A. Vostrikov,
PI № FS 77-82226 from November, 23, 2021

Submitted for publication 08.03.24. Passed for printing 27.06.24. Signed for printing: 01.07.2024.
Format $60\times84_{1/8}$. Phototype CentSchbkCyrill BT. Digital printing.

Layout original is made at the Editorial and Publishing Center, SUAI.
67A, Bol'shaya Morskaia, 190000, Saint Petersburg, Russia
Printed from slides at the Editorial and Publishing Center, SUAI.
67A, Bol'shaya Morskaia, 190000, Saint Petersburg, Russia

The journal is indexed in Scopus.

Free distribution.

doi:10.31799/1684-8853-2024-3 ISSN 1684-8853 (print); ISSN 2541-8610 (online)
НАУЧНЫЙ ЖУРНАЛ

3(130)/2024

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Учредитель
А. А. Востриков
Издатель
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Главный редактор
Е. А. Крук,
д-р техн. наук, проф., Москва, РФ
Ответственный секретарь
О. В. Муравцова

Редактор: А. Г. Ларионова
Корректор: Т. В. Звертановская
Дизайн: М. Л. Черненко, Ю. В. Умницына
Компьютерная верстка: Ю. В. Умницына

Адрес редакции: 190000, г. Санкт-Петербург,
ул. Большая Морская, д. 67, лит. А, ГУАП, РИЦ
Тел.: (812) 494-70-02, эл. адрес: ius.spb@gmail.com,
сайт: http://i-us.ru

Журнал входит в БД Scopus и в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук.

Сдано в набор 08.03.24. Подписано в печать 27.06.24. Дата выхода в свет: 01.07.2024.
Формат 60×841/8. Гарнитура CentSchbkCyrill BT. Печать цифровая.
Усл. печ. л. 5,5. Уч.-изд. л. 7,7. Тираж 1000 экз (1-й завод 50 экз.). Заказ № 227.
Оригинал-макет изготовлен в редакционно-издательском центре ГУАП.
190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А.
Отпечатано в редакционно-издательском центре ГУАП.
190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А.
Распространяется бесплатно.

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.
Перерегистрирован в Роскомнадзоре.
Свидетельство о регистрации ПИ № ФС77-82226 от 23 ноября 2021 г.

УДК 519.6
doi:10.31799/1684-8853-2024-3-2-10
EDN: FOOKRY

Научные статьи
Articles

Повышение точности стеганоанализа пространственной области изображений за счет дополнительных стегановложений

***Р. А. Солодуха*[a]**, *канд. техн. наук, доцент, orcid.org/0000-0002-3878-4221, standartal@list.ru*
[a]*Воронежский государственный университет инженерных технологий, Революции пр., 19, Воронеж, 394036, РФ*

Введение: *большинство стеганоаналитических алгоритмов используют стеганографический контейнер в исходном виде, пытаясь найти следы произведенного ранее воздействия. В то же время в случае атаки на основании известного стеганоалгоритма/стеганопрограммы, располагая даже модифицированным контейнером, аналитик может наблюдать закономерности в характере изменений контейнера при стегановложениях различного размера.* ***Цель:*** *сформировать векторы признаков на базе известного стеганоалгоритма и дополнительных вложений для выявления стеганографии в пространственной области изображений.* ***Результаты:*** *с помощью эмулятора показаны расхождения в корреляции значений стеганоалгоритма Triples analysis и глубины искажения контейнера. Разработан вектор признаков для выявления стеганографии пространственной области изображения, его эффективность подтверждена численным экспериментом с использованием регрессионной модели машинного обучения в среде MatLab. Для обеспечения воспроизводимости эксперимента датасеты и программный код представлены в Kaggle. На основе экспериментальных данных рассчитаны базовые метрики результативности машинного обучения. Подтверждено наличие статистических закономерностей отклика контейнера на дополнительные вложения, получены зависимости точности стеганоанализа от размера вектора признаков.* ***Практическая значимость:*** *на примере алгоритмов Bit Plane Complexity Segmentation и Least Significant Bits показана зависимость ошибки регрессии для векторов признаков различного размера. С помощью полученных оценок аналитик может варьировать точность/размер векторов признаков в зависимости от доступных вычислительных мощностей и размера обучающего множества.*

Ключевые слова *— стеганоанализ, вектор признаков, Bit Plane Complexity Segmentation, Least Significant Bits, стеганография, машинное обучение, метод опорных векторов, регрессия, дополнительные вложения, пространственная область.*

Для цитирования: Солодуха Р. А. Повышение точности стеганоанализа пространственной области изображений за счет дополнительных стегановложений. *Информационно-управляющие системы*, 2024, № 3, с. 2–10. doi:10.31799/1684-8853-2024-3-2-10, EDN: FOOKRY
For citation: Solodukha R. A. Increasing the accuracy of spatial domain steganalysis through additional embeddings. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 3, pp. 2–10 (In Russian). doi:10.31799/1684-8853-2024-3-2-10, EDN: FOOKRY

Введение

Доступность программ, реализующих файловую стеганографию (обзор приведен в работе [1]), позволяет любому пользователю компьютера осуществить несанкционированную передачу информации ограниченного доступа из ведомственной/корпоративной компьютерной сети. Наиболее популярными и простыми в использовании контейнерами для цифровой стеганографии [2] являются изображения [3–6] (в том числе векторная графика [7]), аудио- [8, 9] и видеофайлы [10]. При этом графические файлы можно легко замаскировать под составляющие деловой переписки и передать посредством сервиса электронной почты [11, 12].

По данным, приведенным в исследовании компании «СёрчИнформ» (Исследование уровня информационной безопасности в компаниях России и СНГ за 2020 год. https://static.searchinform.ru/uploads/sites/1/2022/05/issledovaniya-2021.pdf), именно электронная почта является «самым популярным каналом для слива данных в компаниях — на них приходится 45 % утечек в России и 41 % в СНГ». Для госсектора отмечено, что 50 % утечек персональных данных происходит посредством электронной почты (Итоги 2023 года. Исследование осведомленности и отношения сотрудников организаций государственного сектора к проблемам защиты персональных данных. https://static.searchinform.ru/uploads/sites/1/2023/10/issledovaniya-gr-2023-itog.pdf).

Системы противодействия утечкам (Data Leakage Prevention, DLP) способны выявить структурную файловую стеганографию и вложения, совершенные программным обеспечением, оставляющим сигнатуру [13]. Цифровой стеганоанализ несравнимо сложнее, и, несмотря на значительное количество методов стеганоанализа [14], такая функциональность в DLP-системах не заявлена. Это может быть связано как с отсут-

ствием спроса из-за непонимания заказчиками серьезности угрозы, так и со сложностью технической реализации проверки и принятия решения в онлайн-режиме, априорной невозможностью получить вывод в категорической форме.

Работы в направлении обнаружения стеганоконтента проводила компания McAfee. Веб-приложение Steganography Analysis Tool (Steganography defense initiative. https://web.archive.org/web/20210420075148/https://www.mcafee.com/enterprise/ru-ru/downloads/free-tools/steganography.html) позволяло проанализировать графический файл на наличие стеганографии. На данный момент страница приложения недоступна, что свидетельствует либо о потере компанией интереса к данному направлению, либо к его засекречиванию.

Примерами популярных стеганоалгоритмов, реализующих вложения в пространственную область изображения, являются BPCS (BitPlane Complexity Segmentation) [15] с глубиной искажения 5 бит или LSB (Least Significant Bits) [16] с глубиной искажения 1 бит, имеющие программные реализации в сегменте freeware как в скомпилированном виде, так и в виде исходного кода на github.com. Доступность потенциальному нарушителю и распространенность определяют выбор данных алгоритмов для экспериментальной части статьи.

Настоящая статья является развитием работы [17], где применялся стеганоаналитический алгоритм RS [18] для групп различного размера [19] и дополнительные вложения. А также продолжает направление [20, 21] по формированию и проверке эффективности векторов признаков с возможностью управления соотношением точность/ресурсоемкость, что важно для потокового режима работы DLP-систем.

Целью данной работы является формирование и анализ эффективности векторов признаков на основе дополнительных вложений для обнаружения BPCS- и LSB-стеганографии, выявление зависимости точности стеганоанализа от размера вектора признаков.

Обоснование идеи исследования

Искажения стеганографических контейнеров имеют закономерности, определяемые характеристиками изображения и стеганоалгоритмом. Стандартным способом увеличения точности стеганоанализа является обработка контейнера различными алгоритмами, т. е. увеличение размерности вектора признаков. При этом контейнер остается неизменным.

Пусть $S(\mathbf{I}, \mathbf{p})$ — стеганографическая функция, где $\mathbf{I}$ — изображение, а $\mathbf{p}$ — стегановложение (битовая строка), $\mathbf{I}' = S(\mathbf{I}, \mathbf{p})$ — модифицированное изображение. Задача статистического стеганоанализа состоит в выявлении взаимосвязи между специфическими характеристиками (признаками наличия стегановложения) $\mathbf{G}_{\mathbf{I}'}$ и размером $\mathbf{p}$.

Дополнительное вложение, осуществленное в $\mathbf{I}'$, также влияет на признаки наличия стегановложения, и этим влиянием можно управлять, варьируя размер дополнительного вложения. На этапе формирования обучающей выборки технология дополнительных вложений предполагает последовательное осуществление первичного $\mathbf{p}_1$ и дополнительного $\mathbf{p}_2$ вложений с размерами $|\mathbf{p}_1|$ и $|\mathbf{p}_2|$, получение контейнеров $\mathbf{I}' = S(\mathbf{I}, \mathbf{p}_1)$, $\mathbf{I}'' = S(\mathbf{I}', \mathbf{p}_2)$. При этом для $\mathbf{p}_3 = \mathbf{p}_1||\mathbf{p}_2$, где $||$ — конкатенация, имеет место соотношение $S(\mathbf{I}, \mathbf{p}_3) \neq S(\mathbf{I}', \mathbf{p}_2)$. Предполагается, что учет различных комбинаций размеров $\mathbf{p}_1$ и $\mathbf{p}_2$ способствует построению более точной регрессионной зависимости между $\mathbf{G}_{\mathbf{I}''}$ и $|\mathbf{p}_1|$, нежели между $\mathbf{G}_{\mathbf{I}'}$ и $|\mathbf{p}_1|$. Предикторами являются $\mathbf{G}_{\mathbf{I}''}$ и $|\mathbf{p}_2|$, зависимая переменная — $|\mathbf{p}_1|$.

Рассмотрим ситуацию с позиций практики стеганоанализа. Аналитику на исследование поступает файл, для которого требуется определить размер вложения, выполненный известной стеганопрограммой. В терминах настоящей статьи аналитик должен сформировать из исследуемого файла $\mathbf{I}'$ несколько файлов $\mathbf{I}''$ с известным размером дополнительного вложения $|\mathbf{p}_2|$, получить вектор признаков $\mathbf{G}_{\mathbf{I}''}$ и определить размер первичного вложения $|\mathbf{p}_1|$ с помощью ранее обученной регрессионной модели.

Идея искажения исходного контейнера, в том числе путем дополнительных вложений, реализована в ряде работ [22–24].

Набор признаков, полученный путем вычисления 23 функционалов от коэффициентов дискретного косинусного преобразования, описан в [22]. Каждый функционал применяется к изображению $\mathbf{J}_1$ и его калиброванной версии $\mathbf{J}_2$. Калиброванный признак рассчитывается как разность $F(\mathbf{J}_1) - F(\mathbf{J}_2)$, если F — скаляр, как L_1 — норма $||\mathbf{F}(\mathbf{J}_1) - \mathbf{F}(\mathbf{J}_2)||$, если $\mathbf{F}$ — вектор или матрица. Калиброванное JPEG-изображение получается следующим образом. Изображение разворачивается из частотного в пространственное представление, обрезается на несколько пикселей по обоим направлениям, опять сжимается в JPEG с прежними параметрами. Калиброванное изображение сохраняет свойства исходного на макроуровне. При этом коэффициенты дискретного косинусного преобразования изменяются за счет переформирования блоков 8×8, но сохраняют влияние процедуры компрессии. Таким образом, калиброванный набор признаков не чувствителен к визуальному контенту изображения, но чувствителен к изменениям при стегановложении.

Дополнительное вложение используется в работе [23] для обхода проблемы “cover source mismatch” при известных алгоритме и размере вложения. Предлагаемый метод заключается в создании «искусственного» обучающего набора, который формируется путем двукратного применения стеганографического алгоритма к исходным контейнерам (как пустым, так и заполненным). В работе показано, как наличие трех множеств: исходного, с дополнительным заполнением, с повторным дополнительным заполнением — позволяет осуществить классификацию «без учителя».

Эффективность распознавания сверточных нейронных сетей ухудшается, если в качестве контейнера использовано уменьшенное за счет интерполяции значений соседних пикселей (downsampling) изображение [24]. В качестве меры противодействия предлагается обучать сверточные нейронные сети на уменьшенных изображениях (полученных как из пустых, так и заполненных контейнеров) с дополнительным одно- и двукратным вложением. При атаке на основании известного стеганоалгоритма точность классификации увеличивается на 34,8 %.

Таким образом, работы [17, 23, 24] свидетельствуют о том, что в случае атаки на основании известного стеганоалгоритма атакующему становится доступна статистика поведения контейнера при различных размерах вложений, пусть и с некоторым «смещением».

Сопоставление характеристик, отображающих степень искажения контейнера, с элементами вектора признаков

Произведем теоретический расчет количества модифицированных пикселей монохромного изображения с учетом дополнительного вложения для алгоритма LSB Replacement, использующего псевдослучайную, без повторений генерацию координат пикселей для модификации.

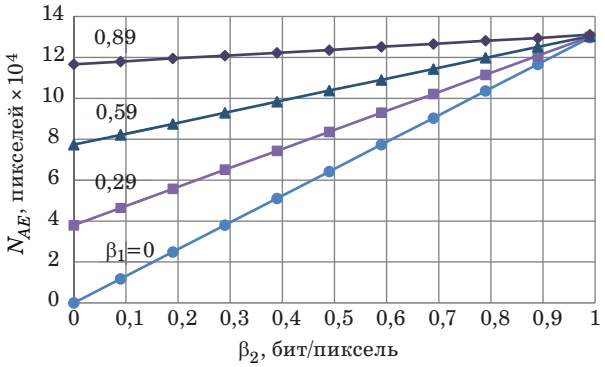
Предположим, что соотношение единиц и нулей в последних битах изображений и встраиваемой битовой строке одинаково, что будет приводить к изменению значений половины пикселей, содержащих скрываемые данные. Обозначим N количество пикселей контейнера, β_1 — размер первичного стегановложения, β_2 — размер дополнительного стегановложения [бит/пиксель], $\mu = 1/2$ пиксель/бит — коэффициент модификации (сколько пикселей изменяется при сокрытии 1 бита). Тогда количество измененных пикселей контейнера после первичного стегановложения (Payload) $N_P = \mu\beta_1 N$. При дополнительном стегановложении изменяются значения пикселей, как модифицированных первичным стегановложением, так и находящихся в исходном состоянии. При этом модифицированные пиксели частично возвращаются в исходное состояние. Количество изменений после дополнительного вложения (Additional Embedding) $N_{AE} = \mu\beta_2(N - N_P) + (N_P - \mu\beta_2 N_P)$.

Подставляя N_P и μ, получим $N_{AE} = (\beta_1 + \beta_2 - \beta_1\beta_2)N/2$.

В графическом представлении получаем семейство прямых, что подтверждено с помощью эмулятора случайного LSB Replacement. На рис. 1 представлено усредненное количество изменений первых 10 файлов из коллекции BOSSbase (Image Database BOSSbase 1.01. http://dde.binghamton.edu/download/ImageDB/BOSSbase_1.01.zip) в допущении, что все пиксели (512 × 512) доступны для модификации стеганоалгоритмом (в реальности часть пикселей отводится под метаданные, параметры алгоритма, хеш пароля и т. п.).

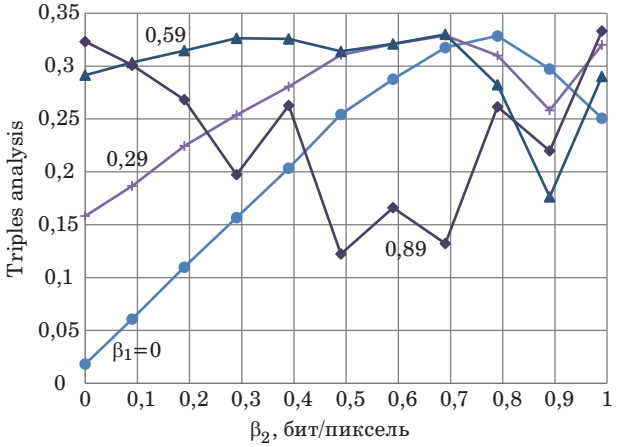
Стеганоалитические предикторы должны коррелировать с количеством изменений. Чем сильнее корреляция, тем точнее результаты. На рис. 2 представлены значения стеганоаналитического алгоритма Triples analysis (TA) [25]. Можно заметить, что кривые TA перестают коррелировать с изменениями, если совокупный размер вложения превышает 50 % [16]. Данный алгоритм показал средние результаты в исследованиях [20, 21] и хорошо подходит для тестирования в рамках настоящей статьи.

Triples analysis является обобщением Sample pairs analysis [26], идея которого состоит в анализе мощности множеств пар соседних пикселей, разности которых принимают одинаковые значения в естественном и модифицированном изображении. Все сводится к решению квадратного уравнения относительно размера вложения, где коэффициенты формируются из значений мощ-



■ ***Рис. 1.*** Усредненное количество модифицированных пикселей

■ ***Fig. 1.*** Average count of modified pixels



■ ***Рис. 2.*** Усредненные значения Triples analysis
■ ***Fig. 2.*** Average values of Triples analysis

ности множеств. ТА оперирует не парами, но тройками смежных пикселей, с решением кубического уравнения.

Формирование вектора признаков

В традиционных стеганоаналитических моделях [14] обучение проводится на выборке, состоящей из пустых и заполненных путем эмуляции стеганографических алгоритмов контейнеров. Контейнеры заполняются с некоторыми фиксированными размерами вложения, как правило, определяемыми в бит на пиксель [бит/пиксель]. Шаг заполнения выбирается исходя из требований к точности прогноза и разделимости получаемых классов.

Если выборка формируется посредством стеганографических приложений, то размер вложения целесообразно учитывать в процентах от максимально возможного для конкретного контейнера (данная информация отображается в стеганографических приложениях, задействованных в экспериментальной части работы). Например, в [20, 21] применяются размеры вложений {9, 19, 29, …, 99} процентов от максимально возможного. Далее понятие «размер вложения» имеет аналогичное содержание.

Пусть имеется набор из N контейнеров $\mathbf{F} = \{\mathbf{f}_n\}$, $n \in [1, N]$. В каждый контейнер реализованы первичные вложения $\mathbf{P} = \{\mathbf{p}_i\}$, $i \in [1, |\mathbf{P}|]$ ($|\mathbf{P}|$ – мощность множества $\mathbf{P}$), получен набор контейнеров $\mathbf{F}_P$, $\mathbf{F}_P = \{\mathbf{f}_n^i, \mathbf{f}_n\}$. Таким образом, для дополнительного вложения исходными являются $|\mathbf{P}|$ файлов с первичным вложением и исходный контейнер.

Затем в каждый контейнер $\mathbf{F}_P$ реализуются дополнительные вложения $\mathbf{A} = \{\mathbf{a}_j\}$, $j \in [1, |\mathbf{A}|]$, получен набор контейнеров $\mathbf{F}_{AE}$. При этом для $\mathbf{p} = \mathbf{a}$, $\mathbf{p} \in \mathbf{P}$, $\mathbf{a} \in \mathbf{A}$ комбинации размеров первичного и дополнительного вложений (0, $\mathbf{a}$) и ($\mathbf{p}$, 0) со статистической точки зрения можно считать идентичными, но для сохранения общности в наименовании файлов обучающего множества они формируются отдельно. Таким образом, $\mathbf{F}_{AE} = \{\mathbf{f}_n^{i,j}, \mathbf{f}_n^i, \mathbf{f}_n^j, \mathbf{f}_n\}$, $|\mathbf{F}_{AE}| = |\mathbf{P}| \cdot |\mathbf{A}| + |\mathbf{P}| + |\mathbf{A}| + 1$. В частном случае $|\mathbf{P}| = |\mathbf{A}|$, рассматриваемом в данной статье, $|\mathbf{F}_{AE}| = (|\mathbf{P}| + 1)^2$.

Предположим, что после применения стеганоаналитической функции S' к множеству $\mathbf{F}_{AE}$ каждому контейнеру сопоставлен набор признаков размером D, $S'(\mathbf{F}_{AE}) \to \mathbf{G}_{AE}$, $\mathbf{G}_{AE} = \{g_n^{i,j,d}\}$, $i \in [0, |\mathbf{P}|]$, $j \in [0, |\mathbf{A}|]$, $d \in [1, D]$, где $i, j = 0$ – индексы, обозначающие отсутствие первичного ($\mathbf{p}_0 \in \varnothing$) или дополнительного вложений ($\mathbf{a}_0 \in \varnothing$) соответственно. Таким образом, задача состоит в нахождении функционала $\Phi(\mathbf{G}_{AE}) \to \{|\mathbf{p}_i|\}$, где $|\mathbf{p}_i|$ – размер $\mathbf{p}_i$, $|\mathbf{p}_0| = 0$. В практическом контексте $\{g^{j,d}\}$ представляет собой матрицу размером $|A| \times D$, вытянутую в вектор:

$$\left(g^{0,1}, \ldots, g^{0,D}, g^{1,1}, \ldots, g^{1,D}, \ldots, g^{|A|,1}, \ldots, g^{|A|,D}\right),$$

которая содержит данные для машинного обучения.

Экспериментальная часть

В качестве программной реализации (программы доступны в Kaggle: https://www.kaggle.com/datasets/romansolodukha/steganoprograms) алгоритма Bit Plane Complexity Segmentation использована Qtech-HV02. Для LSB выбрана модификация LSB Replacement с псевдослучайным выбором пикселей для модификации в реализации The Third Eye. Применена реализация стеганоалгоритма ТА (Structural LSB Detectors. http://dde.binghamton.edu/download/structural_lsb_detectors) на языке MatLab, размещенная на сайте Digital Data Embedding Laboratory (Binghampton University) и модифицированная для применения на разных битовых плоскостях, остальные алгоритмы запрограммированы самостоятельно.

В качестве источника контейнеров использованы первые 1000 файлов коллекции BOSSbase 1.01 с переконвертацией PGM → → BMP24. В полученных файлах все три цветовых канала идентичны, поэтому для анализа использован канал красного цвета.

Для автоматизированного заполнения контейнеров использован скрипт AutoIt с шагом 10 % от максимального размера вложения от 9 до 99 % как для первичного, так и для дополнительного вложения ({|**p**|} = {|**a**|} = {9, 19, 29, …, 99}), выборка составила 121 000 контейнеров.

После преобразования стеганоаналитических данных в вектор признаков получен датасет (доступен в Kaggle: https://www.kaggle.com/datasets/romansolodukha/triples-for-bpsc-lsb-with-ae) из 11 000 элементов, что адекватно решаемой задаче [27].

В качестве прогнозной модели выбран стандартный регрессор Medium Gaussian с ядром $\sqrt{D}$ (D — количество предикторов) на базе метода опорных векторов (Support Vector Machine, SVM) из среды машинного обучения MatLab Regression Learner с настройками по умолчанию. Выбор регрессионной модели обучения обусловлен значительным количеством классов (одиннадцатью). Стандартные настройки не оптимизировались, так как цель исследования не в поиске максимально результативной модели обучения для полученного вектора признаков (как, например, в [28, 29]), а в оценке прироста точности распознавания при учете дополнительных вложений.

В качестве методики машинного обучения использована 5-fold кросс-валидация. В качестве метрик результативности [30] использованы коэффициент детерминации (R-Squared, R^2) и среднеквадратичная ошибка (Root Mean Square Error, RMSE).

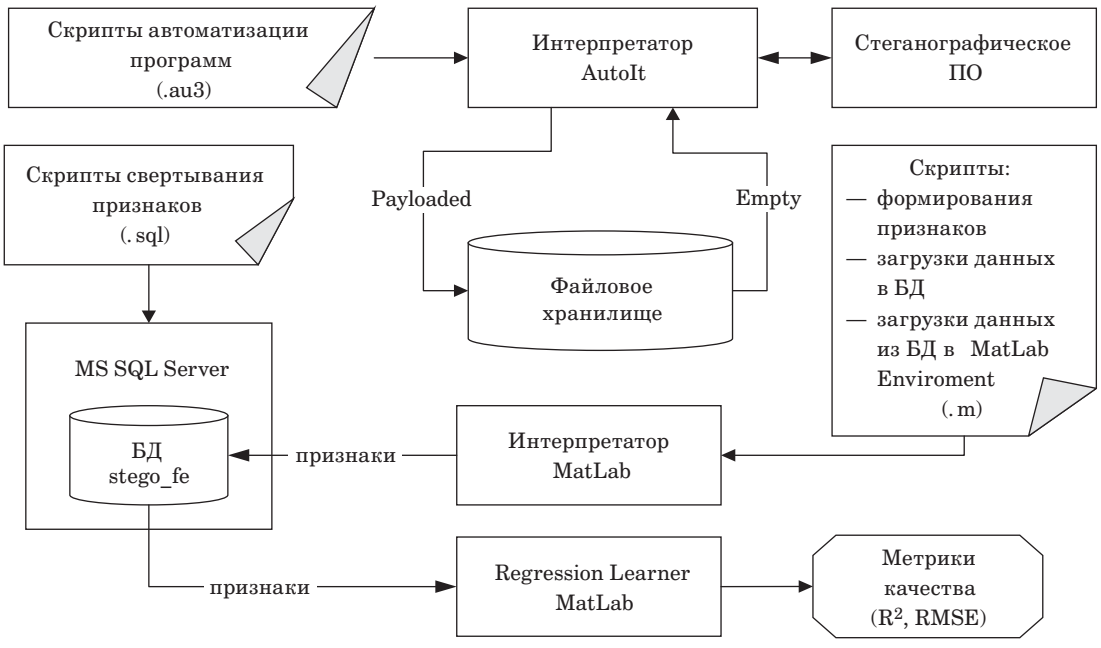
Выбор модели и метрик машинного обучения обусловлен использованием их в ряде подобных работ [23, 30–32], в частности в предшествующих работах [20, 21]. Поскольку речь идет об эффективности вектора признаков, модель машинного обучения, метрики и исходные изображения зафиксированы для адекватного сравнения.

Стенд для проведения эксперимента (рис. 3) собран на базе офисного компьютера Intel i5-12400 2,5 GHz, SSD 500 GB, RAM 32 GB под управлением Windows 10 Pro с установленным программным обеспечением MatLab R2017b, MS SQL Server 2019, AutoIt v3. Для данной конфигурации время преобразования данных в вектор признаков составило 17 с на 1000 строк, время одного вычисления ТА и сохранения результата в базу данных (БД) — 0,3 с.

Одной из задач исследования является оценка влияния на точность распознавания количества и размера учитываемых в векторе признаков дополнительных вложений. Для ранжирования признаков использованы алгоритмы Minimum Redundancy Maximum Relevance и Regressional ReliefF, встроенные в MatLab Regression Learner, которые в целом подтвердили убывание значимости признаков с возрастанием размера первичного вложения, наблюдаемое на рис. 2.

В этой связи план эксперимента содержит последовательное включение элементов в результирующий вектор признаков по мере увеличения размера дополнительного вложения, что отражено в таблице (например, столбец 1D содержит результаты без учета дополнительных вложений, столбец 11D — все дополнительные вложения, столбец 4D — дополнительные вложения 9, 29, 39 %).

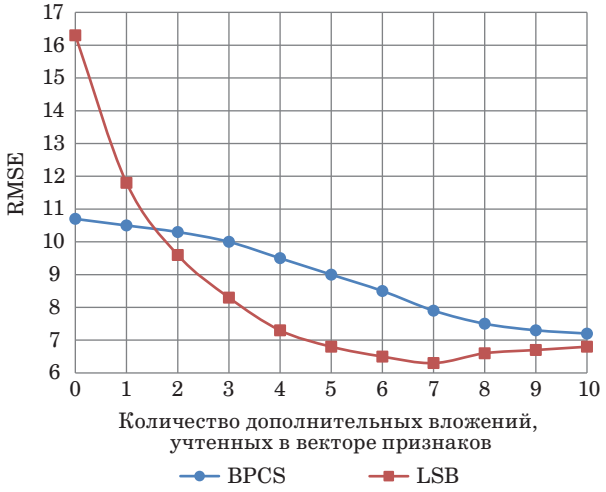
Видно, что с ростом количества признаков распознавание для BPCS плавно улучшается



■ ***Рис. 3.*** Схема численного эксперимента
■ ***Fig. 3.*** Program experiment scheme

■ Результаты применения векторов признаков разного размера
■ Results of applying different dimension feature vectors

Стеганография	Метрика	Вектор										
		1D	2D	3D	4D	5D	6D	7D	8D	9D	10D	11D
BPCS (D = 5)	RMSE	10,7	10,5	10,3	10,0	9,5	9,0	8,5	7,9	7,5	7,3	7,2
	R^2	0,88	0,89	0,89	0,9	0,91	0,92	0,93	0,94	0,94	0,95	0,95
LSB (D = 1)	RMSE	16,3	11,8	9,6	8,3	7,3	6,8	6,5	6,3	6,6	6,7	6,8
	R^2	0,73	0,86	0,91	0,93	0,95	0,95	0,96	0,96	0,96	0,95	0,95



■ ***Рис. 4.*** Зависимость RMSE от размера вектора признаков
■ ***Fig. 4.*** Dependence of RMSE on feature vector dimension

с максимальным приростом R^2 на 0,07 (кривая *BPCS* на рис. 4). Для LSB прирост R^2 составил 0,23, и минимум RMSE достигнут при учете дополнительных вложений размером 9–69 % (кривая *LSB* на рис. 4). RMSE уменьшилось для BPCS в 1,5 раза, для LSB в 2,6 раза.

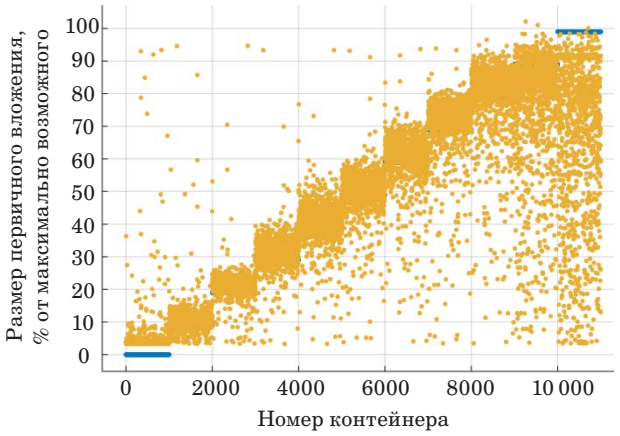
Таким образом, векторы признаков с максимальной достижимой точностью:

BPCS – $\left(g^{0,1}, ..., g^{0,5}, g^{1,1}, ..., g^{1,5}, ..., g^{10,1}, ..., g^{10,5}\right)$, размер вектора – 55;

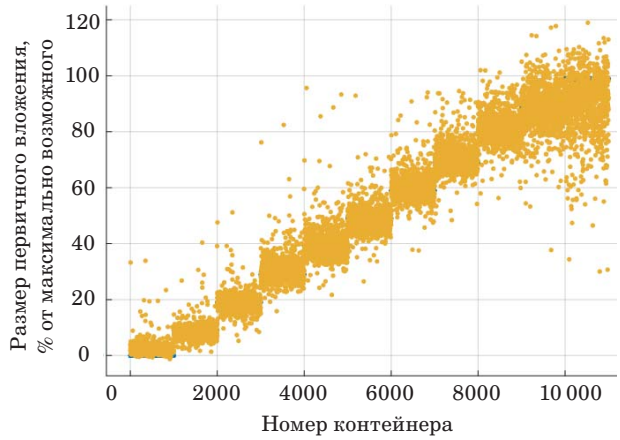
LSB – $\left(g^0, g^1, ..., g^7\right)$, размер вектора – 8.

Визуализированные данные по предсказанию размера вложения, выполненного для контейнеров, модифицированных LSB, представлены на рис. 5, 6. Контейнеры упорядочены по возрастанию размера вложения, синие отрезки – истинные значения.

Значительный прирост точности распознавания находится в области вложений, размер которых более 80 % от максимально возможного. Также за счет выхода прогнозных значений за область допустимых значений [0, 100] результаты можно уточнить, приравнивая к нулю отрицательные прогнозы и к 100 – прогнозы, данное значение превышающие.



■ ***Рис. 5.*** Предсказание без учета дополнительных вложений (один предиктор Triples analysis)
■ ***Fig. 5.*** Prediction without additional embeddings (one Triples analysis predictor)



■ ***Рис. 6.*** Предсказание с учетом дополнительных вложений (восемь предикторов Triples analysis)
■ ***Fig. 6.*** Prediction with additional embeddings (eight Triples analysis predictors)

Заключение

На основе учета результатов применения стеганоаналитического алгоритма ТА к контейнерам с дополнительным заполнением сформированы векторы признаков для цифрового стеганоанализа изображений, модифицированных алгоритмами BPCS и LSB.

Корректировка полученных векторов признаков выполнена по результатам численного эксперимента по определению размера стегановложения. Использована технология машинного обучения, реализованная в среде MatLab, — SVM-регрессия, с оценками коэффициента детерминации и среднеквадратичной ошибки в качестве метрик, что позволяет сравнить полученный результат с аналогичными работами.

Наблюдаемое улучшение распознавания (по метрике RMSE: BPCS — 1,5 раза, LSB — 2,6) подтверждает наличие статистических закономерностей отклика контейнера на дополнительные вложения.

Также получены зависимости оценки точности распознавания от размера вектора признаков, что позволяет аналитику управлять балансом между достоверностью и ресурсоемкостью обнаружения.

В дальнейших исследованиях по данной тематике предполагается провести аналогичный численный эксперимент для частотных областей изображений.

Литература

1. **Герлинг Е. Ю., Ахрамеева К. А.** Обзор современного программного обеспечения, использующего методы стеганографии. *Экономика и качество систем связи*, 2019, № 3 (13), с. 51–58. EDN: KEFWXI
2. **Верещагина Е. А., Золкин А. Л., Капецкий И. О.** *Совершенствование методов аудио-, видео- и сетевой стеганографии*: монография. М., РУСАЙНС, 2023. 140 с.
3. **Савельева М. Г., Урбанович П. П.** Метод стеганографического преобразования web-документов на основе растровой графики модели RGB. *Труды БГТУ. Серия 3: Физико-математические науки и информатика*, 2022, № 2 (260), с. 99–107. doi:10.52065/2520-6141-2022-260-2-99-107, EDN: OMAOWS
4. **Бречко А. А., Булгакова М. И.** Способ скрытия информационного взаимодействия. *Известия ТулГУ. Технические науки*, 2022, № 5, с. 152–158. doi:10.24412/2071-6168-2022-5-152-159
5. **Пономарев И. В., Строкин Д. И.** Стеганографические методы встраивания и обнаружения сокрытых сообщений, использующие gif-изображения в качестве файлов-контейнеров. *Известия Алтайского государственного университета*, 2022, № 1 (123), с. 112–115. doi:10.14258/izvasu(2022)1-18
6. **Мельман А. С., Петров П. О., Шелупанов А. А., Аристов А. В., Похолков Ю. П.** Встраивание информации в JPEG-изображения с маскировкой искажений в частотной области. *Доклады Томского государственного университета систем управления и радиоэлектроники*, 2020, т. 23, № 4, с. 45–50. doi:10.21293/1818-0442-2020-23-4-45-50
7. **Николайчук А. Н., Урбанович П. П.** Стеганографический метод на основе использования особенностей отображения элементов в формате SVG. *Труды БГТУ. Серия 3: Физико-математические науки и информатика*, 2023, № 1 (266), с. 64–70. doi:10.52065/2520-6141-2023-266-1-11
8. **Воронцова Н. В., Миляева И. В.** Стеганографическая защита информации. *Известия Тульского государственного университета. Технические науки*, 2020, № 12, с. 86–95. EDN: YWQQLM
9. **Рублёв Д. П., Макаревич О. Б., Федоров В. М.** Метод стеганографического встраивания сообщений в аудиоданные на основе вейвлет-преобразования. *Известия ЮФУ. Технические науки*, 2009, № 11, с. 199–205. EDN: LAUDHN
10. **Радаев С. В., Басов О. О., Мясин К. И., Мотиенко А. И.** Встраивание стеганографических сообщений в видеофайлы формата MPEG-4. *Экономика. Информатика*, 2018, т. 45, № 4, с. 769–781. doi:10.18413/2411-3808-2018-45-4-769-781
11. **Солодуха Р. А.** Концепция формирования системы противодействия стеганографическим каналам в компьютерных сетях органов внутренних дел. *Вестник Воронежского института МВД России*, 2021, № 1, с. 131–142.
12. **Мисюков Г. И.** Извлечение текстовой информации из изображений модифицированного текста. *Инженерный вестник Дона*, 2023, № 8 (104). http://ivdon.ru/ru/magazine/archive/n8y2023/8625 (дата обращения: 24.03.2024).
13. **Солодуха Р. А.** О возможностях сигнатурного анализа в цифровой стеганографии. *Вестник Воронежского института ФСИН России*, 2016, № 1, с. 52–57.
14. **Вильховский Д. Э.** Обзор методов стеганографического анализа изображений в работах зарубежных авторов. *Математические структуры и моделирование*, 2020, № 4 (56), с. 75–102. doi:10.24147/2222-8772.2020.4.75-102
15. **Kawaguchi E., Eason R.** Principle and applications of BPCS-steganography. *Multimedia Systems and Applications*, 1998, vol. 3528, pp. 464–473.
16. **Powel B. A.** Securing LSB embedding against structural steganalysis. *Journal of Computer Security*, 2021, vol. 30, iss. 42022, pp. 517–539. doi:https://doi.org/10.3233/JCS-200123
17. **Солодуха Р. А.** Использование дополнительного заполнения графических контейнеров для уточнения результатов RS-VGS-стеганоанализа. *Вестник Воронежского института МВД России*, 2014, № 1, с. 87–94.

18. **Fridrich J., Goljan M., Du R.** Reliable detection of LSB steganography in color and grayscale images. *Proc. of the Workshop on Multimedia and Security: Association for Computing Machinery*, New York, 2001. doi:https://doi.org/10.1145/1232454.1232466
19. **Solodukha R. A., Atlasov I. V.** Modification of RS-steganalysis to attacks based on known stego-program. *2017 Second Russia and Pacific Conf. on Computer Technology and Applications (RPC)*, Vladivostok, Russia, 2017, pp. 176–179. doi:10.1109/RPC.2017.8168093
20. **Солодуха Р. А.** Статистический стеганоанализ фотореалистичных изображений с использованием градиентных путей. *Вопросы кибербезопасности*, 2022, № 1(47), с. 26–36. doi:10.21681/2311-3456-2022-1-26-36.
21. **Солодуха Р. А.** Стеганоанализ изображений, модифицированных алгоритмом Bit Plane Complexity Segmentation. *Информационно-управляющие системы*, 2023, № 2, с. 27–38. doi:10.31799/1684-8853-2023-2-27-38, EDN: DXURBZ
22. **Fridrich J.** Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. *Information Hiding, 6th Intern. Workshop*, Toronto, Canada, May 23–25, 2004, Lecture Notes in Computer Science, 2005, vol. 3200, pp. 67–81. doi:10.1007/978-3-540-30114-1_6
23. **Lerch-Hostalot D.**, **Megias D.** Unsupervised steganalysis based on artificial training sets. *Engineering Applications of Artificial Intelligence*, 2016, vol. 50, pp. 45–59. http://dx.doi.org/10.1016/j.engappai.2015.12.013
24. **Kato H., Osuge K., Haruta S., Sasase I.** A preprocessing by using multiple steganography for intentional image downsampling on CNN-based steganalysis. *IEEE Access*, 2020, vol. 8, pp. 195578–195593. doi:10.1109/ACCESS.2020.3033814
25. **Ker A.** A general framework for structural steganalysis of LSB Replacement. *Proc. of the Information Hiding*, 2005, pp. 296–311.
26. **Dumitrescu S., Wu X., Memon D.** On steganalysis of random LSB embedding in continuous-tone images. *IEEE Intern. Conf. on Image Processing*, 2002, vol. 3, pp. 641–644.
27. **Парасич А. В., Парасич В. А., Парасич И. В.** Формирование обучающей выборки в задачах машинного обучения. Обзор. *Информационно-управляющие системы*, 2021, № 4, с. 61–70. doi:10.31799/1684-8853-2021-4-61-70
28. **Сирота А. А., Дрюченко М. А., Иванков А. Ю.** Стегоанализ цифровых изображений с использованием методов поверхностного и глубокого машинного обучения: известные подходы и новые решения. *Вестник ВГУ. Серия: Системный анализ и информационные технологии*, 2021, № 1, с. 33–52. doi:10.17308/sait.2021.1/3369
29. **Полунин А. А., Яндашевская Э.А.** Использование аппарата сверточных нейронных сетей для стегоанализа цифровых изображений. *Труды ИСП РАН*, 2020, № 4, с. 155–163. doi:10.15514/ISPRAS-2020-32(4)-11
30. **Лебедев И. С.** Адаптивное применение моделей машинного обучения на отдельных сегментах выборки в задачах регрессии и классификации. *Информационно-управляющие системы*, 2022, № 3, с. 20–30. doi:10.31799/1684-8853-2022-3-20-30
31. **Shankar D. D., Azhakath A. S.** Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO. *Multimed Tools Appl*, 2021, vol. 80, pp. 4073–4092. https://doi.org/10.1007/s11042-020-09820-7
32. **Kheddar H., Hemis M., Himeur Y., Megias D., Amirae A.** Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions. *Neurocomputing*, 2024, vol. 581, p. 127528. https://doi.org/10.1016/j.neucom.2024.127528

UDC 519.6
doi:10.31799/1684-8853-2024-3-2-10
EDN: FOOKRY

Increasing the accuracy of spatial domain steganalysis through additional embeddings

R. A. Solodukha[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-3878-4221, standartal@list.ru
[a]Voronezh State University of Engineering Technologies, 19, Revolucii Ave., 394036, Voronezh, Russian Federation

Introduction: Most steganalytical algorithms use the steganographic container in its original form, trying to reveal traces of payload. In the case of an attack based on a known steganographic algorithm or program the analyst can observe patterns in the changes of the container caused by various payload values even in a modified container. **Purpose:** To develop feature vectors based on known steganalytical algorithm and additional embeddings to reveal steganography in image spatial domain. **Results:** We show discrepancies in the correlation of Triples analysis results with the depth of container distortion. We develop a feature vector to detect spatial domain steganography. We verify its effectiveness by the numerical experiment using a machine learning regression model in MatLab. To ensure reproducibility of the experiments the datasets and scripts are presented in Kaggle. With the reference to the experimental data we confirm the presence of statistical patterns in the container's response to additional embeddings. We also obtain dependences of the steganalysis accuracy and the feature vector dimension. **Practical relevance:** For Bit Plane Complexity Segmentation and Least Significant Bits algorithms, the dependence of the regression error on different dimensions feature vectors is shown. Using the obtained estimates, the analyst can vary the accuracy/dimension of feature vectors accorfing to the available computing power and the size of the training set.

Keywords – steganalysis, feature vector, Bit Plane Complexity Segmentation, Least Significant Bits, steganography, machine learning, SVM-regression, additional embeddings, spatial domain.

For citation: Solodukha R. A. Increasing the accuracy of spatial domain steganalysis through additional embeddings. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 3, pp. 2–10 (In Russian). doi:10.31799/1684-8853-2024-3-2-10, EDN: FOOKRY

References

1. Gerling E., Ahrameeva K. The review of the modern software using steganography methods. *Ekonomika i kachestvo sistem svyazi*, 2019, no. 3 (13), pp. 51–58 (In Russian). EDN: KEFWXI
2. Vereshchagina E. A., Zolkin A. L., Kapeckij I. O. *Sovershenstvovanie metodov audio-, video- i setevoj steganografii* [Improvement of audio-, video- and network steganography]. Moskow, RUSAJNS Publ., 2023. 140 p. (In Russian).
3. Saveleva M. G., Urbanovich P. P. Method of steganographic transformation of web-documents based on raster graphics and RGB model. *Proceedings of BSTU. Issue 3, Physics and Mathematics. Informatics*, 2022, no. 2 (260), pp. 99–107 (In Russian). doi:10.52065/2520-6141-2022-260-2-99-107, EDN: OMAOWS
4. Brechko A. A., Bulgakova M. I. A method of hiding information communications. *Izvestiya TulGU. Tekhnicheskie nauki*, 2022, no. 5, pp. 152–158 (In Russian). doi:10.24412/2071-6168-2022-5-152-159
5. Ponomarev I. V., Strokin D. I. Steganographic methods for embedding and detecting hidden messages using GIF images as container files. *Izvestiya Altajskogo gosudarstvennogo universiteta*, 2022, no. 1 (123), pp. 112–115 (In Russian). doi:10.14258/izvasu(2022)1-18
6. Melman A. S., Petrov P. O., Shelupanov A. A., Aristov A. V., Pokholkov Y. P. Embedding information into JPEG images with distortion masking in frequency domain. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki*, 2020, vol. 23, no. 4, pp. 45–50 (In Russian). doi:10.21293/1818-0442-2020-23-4-45-50
7. Nikolaichuk A. N., Urbanovich P. P. A steganographic method based on the use of the features of elements displaying in SVG format. *Proceedings of BSTU. Issue 3, Physics and Mathematics. Informatics*, 2023, no. 1 (266), pp. 64–70 (In Russian). doi:10.52065/2520-6141-2023-266-1-11
8. Vorontsova N. V., Milyaeva I. V. Steganographic information protection. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki*, 2020, no. 12, pp. 86–95 (In Russian). EDN: YWQQLM
9. Rublyov D. P., Makarevich O. B., Fedorov V. M. Steganographical method for messages embedding to audiodata based on the wavelet-transform. *Izvestiya SFedU. Engineering Sciences*, 2009, no. 11, pp. 199–205 (In Russian). EDN: LAUDHN
10. Radaev S. V., Basov O. O., Myasin K. I., Motienko A. I. Embedding steganographic messages into MPEG-4 video files. *Economics. Information Technologies*, 2018, vol. 45, no. 4, pp. 769–781 (In Russian). doi:10.18413/2411-3808-2018-45-4-769-781
11. Solodukha R. A. Conception of forming the steganographic channels counteraction system in the internal affairs computer networks. *The Bulletin of Voronezh Institute of the Federal Penitentiary Service of Russia*, 2016, no. 1, pp. 52–57 (In Russian).
12. Misyukov G. I. Extraction text information from modified text image. *Inzhenernyj vestnik Dona*, 2023, no. 8 (104) (In Russian). Available at: http://ivdon.ru/ru/magazine/archive/n8y2023/8625 (accessed 29 March 2024).
13. Solodukha R. A. The possibilities of the signature analysis for the digital steganography. *The Bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2021, no. 1, pp. 131–142 (In Russian).
14. Vilkhovskiy D. E. A survey of steganalysis methods in the papers of foreign authors. *Mathematical Structures and Modeling*, 2020, no. 4 (56), pp. 75–102 (In Russian). doi:10.24147/2222-8772.2020.4.75-102
15. Kawaguchi E., Eason R. Principle and applications of BPCS-steganography. *Multimedia Systems and Applications*, 1998, vol. 3528, pp. 464–473.
16. Powel B. A. Securing LSB embedding against structural steganalysis. *Journal of Computer Security*, 2021, vol. 30, iss. 42022, pp. 517–539. doi:https://doi.org/10.3233/JCS-200123
17. Solodukha R. A. Additional embedding in graphic stego-container for RS-VGS-steganalysis results refinement. *The Bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2014, no. 1, pp. 87–94 (In Russian).
18. Fridrich J., Goljan M., Du R. Reliable detection of LSB steganography in color and grayscale images. *Proc. of the Workshop on Multimedia and Security: Association for Computing Machinery*, New York, 2001. doi:https://doi.org/10.1145/1232454.1232466
19. Solodukha R. A., Atlasov I. V. Modification of RS-steganalysis to attacks based on known stego-program. *2017 Second Russia and Pacific Conf. on Computer Technology and Applications (RPC)*, Vladivostok, Russia, 2017, pp. 176–179. doi:10.1109/RPC.2017.8168093
20. Solodukha R. A. Statistical steganalysis of photorealistic Images using gradient paths. *Voprosy kiberbezopasnosti*, 2022, no. 1(47), pp. 26–36 (In Russian). doi:10.21681/2311-3456-2022-1-26-36
21. Solodukha R. A. Steganalysis of Bit Plane Complexity Segmentation algorithm. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 2, pp. 27–38 (In Russian). doi:10.31799/1684-8853-2023-2-27-38, EDN: DXURBZ
22. Fridrich J. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. *Information Hiding, 6th Intern. Workshop*, Lecture Notes in Computer Science, 2005, vol. 3200, pp. 67–81. doi:10.1007/978-3-540-30114-1_6
23. Lerch-Hostalot D., Megias D. Unsupervised steganalysis based on artificial training sets. *Engineering Applications of Artificial Intelligence*, 2016, vol. 50, pp. 45–59. http://dx.doi.org/10.1016/j.engappai.2015.12.013
24. Kato H., Osuge K., Haruta S., Sasase I. A Preprocessing by using multiple steganography for intentional image downsampling on CNN-based steganalysis. *IEEE Access*, 2020, vol. 8, pp. 195578–195593. doi:10.1109/ACCESS.2020.3033814
25. Ker A. A general framework for structural steganalysis of LSB Replacement. *Proc. of the Information Hiding*, 2005, pp. 296–311.
26. Dumitrescu S., Wu X., Memon D. On steganalysis of random LSB embedding in continuous-tone images. *IEEE Intern. Conf. on Image Processing*, 2002, vol. 3, pp. 641–644.
27. Parasich A. V., Parasich V. A., Parasich I. V. Training set formation in machine learning tasks. Survey. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 4, pp. 61–70 (In Russian). doi:10.31799/1684-8853-2021-4-61-70
28. Sirota A. A., Dryuchenko M. A., Ivankov A. Yu. Steganalysis of digital images by means of shallow and deep machine learning: existing approaches and new solutions. *Proceedings of Voronezh State University. Series: Systems Analysis and Information Technologies*, 2021, no. 1, pp. 33–52 (In Russian). doi:10.17308/sait.2021.1/3369
29. Polunin A. A., Yandashevskaya E. A. Using of convolutional neural networks for steganalysis of digital images. *Proc. of the Institute for System Programming of the RAS*, 2020, vol. 32, iss. 4, pp. 155–164 (In Russian). doi:10.15514/ISPRAS–2020–32(4)–11
30. Lebedev I. S. Adaptive application of machine learning models on separate segments of a data sample in regression and classification problems. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 3, pp. 20–30 (In Russian). doi:10.31799/1684-8853-2022-3-20-30
31. Shankar D. D., Azhakath A. S. Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO. *Multimed Tools Appl*, 2021, vol. 80, pp. 4073–4092. https://doi.org/10.1007/s11042-020-09820-7
32. Kheddar H., Hemis M., Himeur Y., Megías D., Amirae A. Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions. *Neurocomputing*, 2024, vol. 581, p. 127528. https://doi.org/10.1016/j.neucom.2024.127528

УДК 004.62, 004.7
doi:10.31799/1684-8853-2024-3-11-23
EDN: XSSHJI

Научные статьи
Articles

Модель реплицируемой системы хранения данных с использованием среднего возраста информации в качестве показателя актуальности данных

Д. Р. Крылов[a], *магистрант, orcid.org/0009-0008-5901-5342*
Е. Д. Пойманова[a], *канд. техн. наук, доцент, orcid.org/0000-0002-7903-2480*
А. М. Тюрликов[a], *доктор техн. наук, профессор, orcid.org/0000-0001-7132-094X, turlikov@guap.ru*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *актуальной задачей для реплицируемых систем хранения данных на основе ведущих и ведомых узлов является обеспечение баланса согласованности и доступности. Общепринятого количественного показателя, характеризующего такой баланс, не существует, однако при достижении баланса обеспечивается актуальность данных, которую количественно можно оценить с помощью среднего возраста информации.* ***Цель:*** *разработать модель, которая будет отражать основные особенности реплицируемых систем хранения данных и позволит сформулировать и решить задачу минимизации возраста информации за счет распределения узлов системы на ведущие и ведомые.* ***Результаты:*** *предложена модель реплицируемой системы хранения данных на основе ведущих и ведомых узлов с использованием среднего возраста информации в качестве показателя актуальности данных. В рамках модели сформулирована оптимизационная задача по распределению узлов на ведомые и ведущие, при котором минимизируется средний возраст информации с учетом показателей надежности доставки данных при перезаписи уже имеющегося фрагмента данных в хранилище и получено ее приближенное решение.* ***Практическая значимость:*** *представленная модель отражает общие особенности реплицируемых систем хранения данных и может быть использована в реальных системах при решении задачи соблюдения баланса согласованности и доступности.* ***Обсуждение:*** *ключевой особенностью предложенной модели является допущение о независимости события успешной доставки обновления данных для разных ведомых узлов. Если эти события будут зависимыми, то можно высказать гипотезу, что решение рассмотренной оптимизационной задачи дает не точное значение, а оценку снизу для среднего возраста информации. Подтверждение или опровержение данной гипотезы является предметом дальнейших исследований.*

Ключевые слова *— средний возраст информации, системы хранения данных, репликация, ведущие узлы, ведомые узлы.*

Для цитирования: Крылов Д. Р., Пойманова Е. Д., Тюрликов А. М. Модель реплицируемой системы хранения данных с использованием среднего возраста информации в качестве показателя актуальности данных. *Информационно-управляющие системы*, 2024, № 3, с. 11–23. doi:10.31799/1684-8853-2024-3-11-23, EDN: XSSHJI

For citation: Krylov D. R., Poymanova E. D., Turlikov A. M. Modeling a replicated storage system with the use of the average age of information as an indicator of data relevance. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 3, pp. 11–23 (In Russian). doi:10.31799/1684-8853-2024-3-11-23, EDN: XSSHJI

Введение

В современных сервисах широко используются распределенные системы хранения данных, обеспечивающие высокую доступность информации, дробя ее на фрагменты (реплики) и сохраняя их на некотором множестве узлов, которые могут находиться в разных географических точках [1]. Таким образом, даже при выходе из строя одного из узлов данные не теряются и система может поддерживать свою работоспособность, так как реплика содержится и на других узлах [2]. Также в таких системах важна согласованность данных, при которой есть возможность считывать или записывать самую последнюю версию данных. Этот принцип позволяет избегать конфликтов при выполнении параллельных операций. Согласно теореме CAP (Consistency, Availability, Partition — согласованность, доступность, распределенность) [3], в распределенной системе невозможно одновременно достичь полного соблюдения согласованности и доступности, так как больший приоритет в пользу одного из принципов будет оказывать влияние на другой. Например, при наличии большого числа реплик, дающих высокую доступность, нужно обновлять каждую реплику при каждой перезаписи для получения согласованности, что по многим причинам в реальных условиях невозможно [4]. Соответственно, в таких системах должен быть соблюден баланс между доступностью и согласованностью.

Как известно, основными операциями, которые происходят в системах хранения данных современных сервисов, являются запись и чтение данных. Однако самая распространенная операция — это перезапись уже имеющейся информации на более новую [5]. С обновлением акту-

ализируется версия информации и сохраняется момент времени, в который произошло данное обновление.

Для обеспечения согласованности и поддержки высокой доступности данных используются особенности таких реплицируемых систем хранения данных, которые в англоязычной литературе называются “leader-based systems”, узлы в таких системах называются “leaders” и “followers”. В отечественной литературе нет соответствующей устоявшейся терминологии, поэтому в настоящей работе эти системы будем называть системами на основе ведущих (leader) и ведомых (follower) узлов. Такие системы применяются в современных крупномасштабных хранилищах, таких как Google Spanner, Amazon DynamoDB, Apple Foundation, где используется алгоритм Paxos, а его альтернатива Raft — в MongoDB и InfluxDB, которые позволяют выбирать из множества узлов некоторое подмножество в качестве ведущих [6–12]. Суть подхода заключается в том, чтобы ведущие узлы, выбранные для некоторого определенного фрагмента данных, гарантированно получали последнюю версию обновления этого фрагмента, а остальные, ведомые узлы, тоже могли получить его последнюю версию, но уже без каких-либо гарантий. Гарантии стабильной записи на ведущие узлы достигаются последовательной записью, в то время как запись на ведомые узлы происходит после ведущих через многоадресную рассылку. Чтение становится возможным только после обновления всех ведущих узлов, а доступность достигается наличием их реплик [13].

Для отслеживания актуальности данных и оценки эффективности работы системы в настоящем исследовании использован такой показатель, как возраст информации (Age of Information, AoI) [14–16], широко применяемый в работах, связанных с системами массового обслуживания [17–21]. Использование данной метрики целесообразно при наличии временных меток обновлений у данных, относительно которых можно проследить устаревание информации с течением времени.

Проводилось мало исследований, связанных с системами хранения данных, имеющих ведущие и ведомые узлы, с использованием такой метрики, как возраст информации, для анализа эффективности работы подобных систем. Например, в работе [22] изучалось влияние количества ведущих узлов по отношению к ведомым на актуальность информации внутри системы. В указанной работе также были приведены результаты, свидетельствующие о наличии оптимального состояния системы, при котором возраст информации минимизируется. В работе [23] продолжены исследования из работы [22] в направлении разработки метода с динамической периодической синхронизацией, который позволяет устанавливать оптимальный период синхронизации в соответствии с переменной нагрузкой.

На данный момент проводятся исследования в области влияния ведущих узлов на старение информации в системе, а также динамического управления возрастом информации в этих системах [22, 23]. С увеличением числа ведущих узлов увеличивается задержка последующих обновлений, в связи с чем информация будет устаревать. Однако при низком числе ведущих узлов возраст информации также будет увеличиваться, так как они гарантированно выдают самую последнюю версию информации. Следовательно, в работе системы существуют оптимальные наборы параметров, при которых будет соблюдаться баланс между согласованностью и доступностью данных.

В работе [22] интервалы между моментами обновления на ведомых узлах распределены по экспоненциальному закону и отсутствуют обоснования связи данного допущения с использованием многоадресной рассылки. В настоящем исследовании удалось приблизиться к принципу работы реальных систем, где в канале передачи могли бы случиться потери пакетов или их повреждения, а также другие непредвиденные обстоятельства, из-за чего доставка могла бы быть не выполнена. Для учета специфики многоадресной рассылки предполагается, что одно и то же обновление успешно передается всем ведомым узлам только с некоторой вероятностью. Данная вероятность является параметром модели. Также из недостатков [22] стоит выделить допущение о зависимости процесса чтения от процесса записи обновления. В нашем исследовании момент прибытия запроса на чтение не зависит от других процессов, протекающих в системе, что в большей мере, по сравнению с работой [22], отражает особенности реальных систем.

В настоящей статье исследуется влияние количества ведущих узлов на возраст информации, полученной запросом на чтение. Рассматривается два принципа записи на узлы: для ведущих узлов обновление происходит гарантированно и последовательно, а новая информация становится доступной для чтения только после обновления всех ведущих узлов. Для ведомых узлов обновление происходит с некоторой вероятностью и при успешной записи становится доступно для чтения сразу. Полученная с некоторых случайно выбранных узлов информация по запросу на чтение дает результат, по которому можно судить о среднем возрасте информации.

Описание модели системы

Рассмотрим систему хранения данных на основе ведущих и ведомых узлов. Всего в системе находится n узлов, все они содержат один и тот же фрагмент данных, который представляет из себя реплику. Некоторые из этих узлов объявляются ведущими. Количество ведущих узлов обозначим l. Остальные узлы называются ведомыми, их количество обозначим f. Ключевое отличие ведущего узла от ведомого состоит в том, что ведущий гарантированно получает самую последнюю версию обновления, тем самым обеспечивая согласованные запись и чтение. Такие гарантии достигаются за счет последовательной записи обновления для ведущих узлов. Для ведомых узлов обновление отправляется с помощью многоадресной рассылки без гарантии успешной доставки, что обусловлено возможными ошибками в канале, потерями пакетов данных и другими причинами, следующими из реальных условий работы систем [24]. Если узел хранит в себе последнюю версию данных, то он называется согласованным.

Время работы системы делится на кадры, которые в свою очередь делятся на слоты (рис. 1). Слот берется за единицу времени. Каждый кадр имеет некоторый номер, который обозначим k. Число слотов внутри кадра соответствует числу ведущих узлов l.

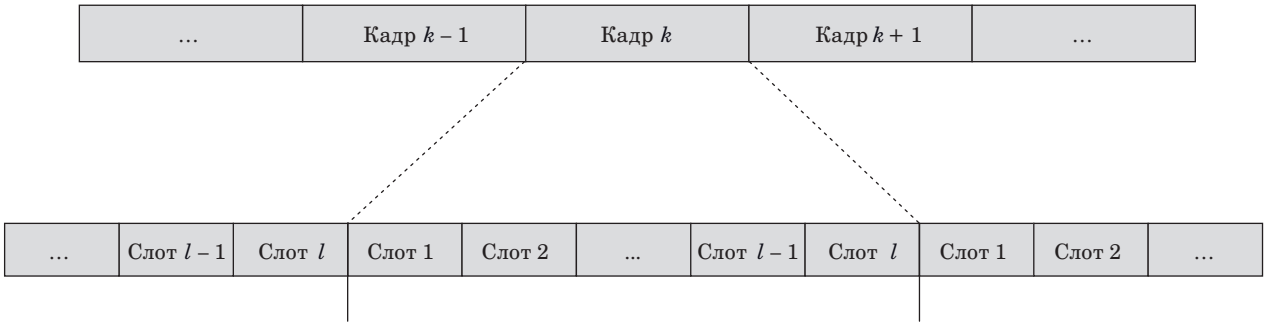
В начале каждого кадра происходит инициализация нового обновления, которое поступает в систему для дальнейшей записи на узлы. Однако чтение данного обновления становится возможным только после его фиксации в системе. В первую очередь обновление записывается на ведущие узлы, а только потом на ведомые узлы. После записи на ведущие узлы обновление фиксируется и становится доступным для чтения. Процесс записи на ведущие и ведомые узлы различается.

Ведущие узлы. Обновление на ведущих узлах происходит последовательно, в связи с чем на запись требуется фиксированное количество времени. Будем считать, что на полное обновление одного ведущего узла требуется ровно один слот, а так как за кадр все они должны провести операцию записи, то в каждом кадре должно быть l слотов. Поскольку фиксация произойдет только в начале следующего кадра, версия, на которую обновляются ведущие узлы, для чтения не доступна.

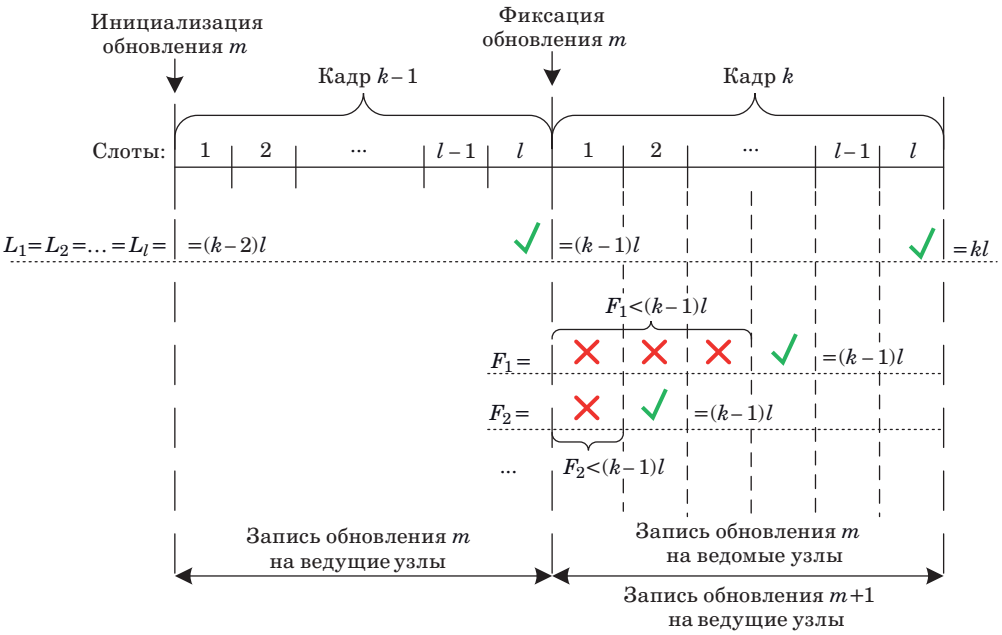
Ведомые узлы. После обновления всех ведущих узлов в предыдущем кадре и фиксации обновления в начале текущего процесс записи начинается на ведомых узлах. Так как процесс записи в данном случае осуществляется с помощью многоадресной рассылки, данные отправляются одновременно на все ведомые узлы. Запись в таком случае не гарантирована и проходит успешно только с некоторой вероятностью p. События успешной доставки обновления данных для разных ведомых узлов независимы. В каждом слоте повторяется попытка записи для каждого ведомого узла.

Запись каждого нового обновления на ведущие и ведомые узлы в системе занимает два кадра (рис. 2). Рассмотрим запись обновления под номером m в кадрах $k-1$ и k. В кадре $k-1$ происходит запись на ведущие узлы. Обновление m инициализируется в момент времени $(k-1)l$, где l — число слотов внутри кадра, и при инициализации в обновлении указывается временная метка. Обновление доставляется на узлы вместе с данной временной меткой $(k-1)l$ и сохраняется в узле при успешной записи до следующего обновления. Временные метки последнего обновления у ведущих и ведомых узлов на рис. 2 обозначены как L_i и F_j соответственно, где $i \in \{1, 2, \ldots, l\}$ — номер ведущего узла, а $j \in \{1, 2, \ldots, n-l\}$ — номер ведомого узла. Так как момент фиксации обновления происходит только в следующем кадре после инициализации (в данном случае фиксация будет в k-м кадре), то пользователь, запрашивающий информацию с ведущих узлов, может получить только предыдущую версию данных с временной меткой $(k-2)l$.

С наступлением следующего кадра под номером k происходит фиксация версии обновления m,



■ ***Рис. 1.*** Разделение кадра на слоты
■ ***Fig. 1.*** Frame segmentation into slots



■ ***Рис. 2.*** Процесс записи m-го обновления
■ ***Fig. 2.*** The process of writing the m-th update

что позволяет получать ее запросом на чтение. Также стоит отметить, что в этом кадре параллельно происходит инициализация $(m + 1)$-го обновления и запись на ведущие узлы $(m + 1)$-й версии данных. В начале данного кадра на всех ведущих узлах уже доступна m-я версия информации с ее временной меткой $(k - 1)l$. Однако процесс записи m-й версии на ведомые узлы происходит только в данном кадре, после фиксации. Успешная запись обновления (обозначена «∨» на рис. 2) для каждого ведомого узла происходит с некоторой вероятностью p в каждом слоте. В случае неудачного исхода записи (обозначен «×» на рис. 2) для ведомого узла предпринимается еще одна попытка записи в следующем слоте. Значение вероятности p является показателем надежности доставки данных при перезаписи уже имеющегося фрагмента данных в хранилище. Максимальное количество попыток обновления ведомого узла равняется числу слотов l внутри кадра. В случае успешного обновления узла версия данных на нем актуализируется и сохраняется временная метка данного обновления. В начале кадра с номером k временная метка на ведомых узлах не может быть новее, чем $(k - 2)l$, но может быть старее.

Для получения информации используются запросы на чтение, которые отправляются на r случайно выбранных узлов системы. Число запросов не может превышать общее число узлов в системе. Случайный выбор узлов модели отражает такую особенность реальных систем, как равномерное распределение нагрузки между узлами. Предполагается, что данные, полученные запросом на чтение с разных узлов, могут нести разный возраст информации, поэтому в качестве ответа система выбирает те данные, которые имеют наименьший возраст информации. Если среди заданного фиксированного количества r узлов в наличии хотя бы один ведущий узел, то считывание последней версии информации будет гарантировано. Чтение информации с узла происходит в начале слота.

В настоящей работе изучается средний возраст информации, полученной запросом на чтение. Возраст информации $\Delta_i(t)$ на i-м узле в момент времени t представляет из себя разность текущего момента времени t и временной метки $N_i(t)$ последнего обновления узла под номером i:

$$\Delta_i(t) = t - N_i(t). \quad (1)$$

Возраст информации запроса на чтение $\Delta_i(t)$ в момент времени t — это минимальный возраст информации среди r узлов, на которые отправлялся запрос:

$$\Delta(t) = \min(\Delta_1(t), \ldots, \Delta_r(t)). \quad (2)$$

В соответствии с работами [9, 10] средний возраст информации $\overline{\Delta}$ рассчитывается следующим образом:

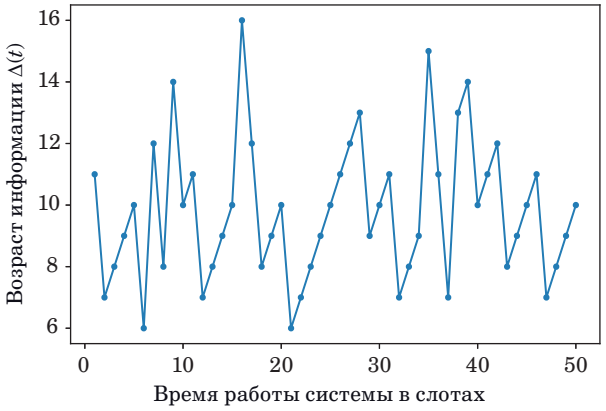
$$\overline{\Delta} = \lim_{T\to\infty} \frac{\int_0^T \Delta(t)\mathrm{d}t}{T}. \quad (3)$$

Рассмотренная выше модель реплицируемой системы хранения данных на основе ведущих и ведомых узлов описывается следующим набором параметров: n — количество узлов в системе, l — количество ведущих узлов, r — количество узлов в запросе на чтение, p — вероятность успешной записи на ведомые узлы.

Для иллюстрации работы модели было выполнено имитационное моделирование со следующими параметрами: $n = 50, l = 5, r = 4, p = 0{,}1$. На рис. 3 построен график зависимости возраста информации $\Delta(t)$ от номера слота t, в котором производится запрос на чтение. По графику видно, что изменение возраста информации по запросу на чтение имеет сложный характер, поэтому определение среднего возраста информации является отдельной задачей.

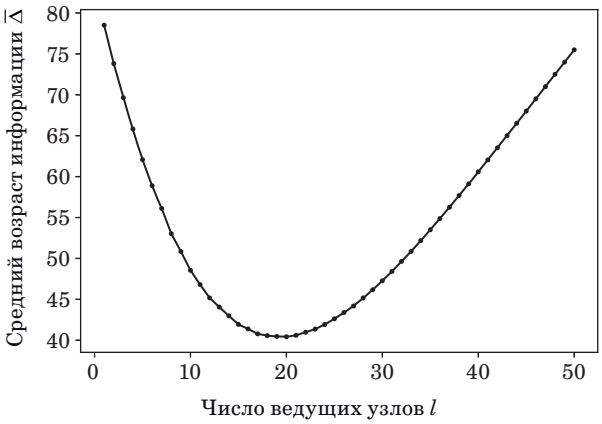
График зависимости среднего возраста информации от числа ведущих узлов в системе (рис. 4) получен в результате моделирования при параметрах $n = 50$, $p = 0{,}003$, $r = 4$. Для возможности сравнения результатов параметры n и r были выбраны в соответствии с работой [22]. На графике виден минимум среднего возраста информации при 19 ведущих узлах. При малом числе ведущих узлов в запросе на чтение слишком редко попадаются согласованные узлы из-за нерегулярного обновления ведомых узлов при их подавляющем количестве. В случае, когда ведущих узлов больше 19, средний возраст информации начинает расти из-за увеличения числа слотов в кадрах, что увеличивает задержку между инициализациями новых обновлений.

Далее будет показано, как получить зависимость среднего возраста информации от параметров модели без использования имитационного моделирования.



■ ***Рис. 3.*** Зависимость возраста информации $\Delta(t)$ от номера слота t, в котором производится запрос на чтение

■ ***Fig. 3.*** Dependence of the age of information $\Delta(t)$ on the slot number t in which the read request is made



■ ***Рис. 4.*** Зависимость среднего возраста информации $\bar{\Delta}$ от числа ведущих узлов в системе

■ ***Fig. 4.*** Graph of the dependence of average age of information on the number of leader nodes in the system

Определение зависимости среднего возраста информации от параметров модели

Рассмотрим кадр под номером k в системе с некоторым числом ведущих узлов l и ведомых узлов f. Длительность слота принята за единицу времени. В начале кадра k у всех l ведущих узлов временная метка L последнего обновления принимает значения $(k-1)l$. У f ведомых узлов временные метки F могут отличаться и принимать значения из диапазона $\{(k-2)l, (k-3)l, \ldots, 0\}$. Таким образом, в начале кадра k временные метки принимают следующие значения:

$$L_1^{(k)} = L_2^{(k)} = \ldots = L_l^{(k)} = (k-1)l,$$
$$F_j^{(k)} \in \{(k-2)l,\ (k-3)l,\ \ldots,\ 0\}, \qquad (4)$$

где $j \in \{1, 2, \ldots, f\}$.

Обозначим $X_j^{(k)}$ возраст информации для j-го ведомого узла в кадре с номером k, а $F_j^{(k)}$ — временную метку j-го ведомого узла к началу кадра с номером k. Тогда возраст информации в начале кадра с номером k рассчитывается следующим образом:

$$X_j^{(k)} = kl - F_j^{(k)} + 1, \qquad (5)$$

где $j \in \{1, 2, \ldots, f\}$.

Далее будем считать, что система работает неограниченно долго, и сформулируем и докажем ряд утверждений.

Утверждение 1. Математическое ожидание возраста информации в начале кадра для всех ведомых узлов одинаково и равно

$$\lim_{k\to\infty} E[X_j^{(k)}] = \left(\frac{1}{1-(1-p)^l} + 1\right) l + 1. \qquad (6)$$

Доказательство:

Рассмотрим ведущий узел с номером j в некотором кадре с номером k. Введем в рассмотрение случайную величину $D_j^{(k)}$, которая может принимать значение $D_j^{(k)} \in \{1, 2, 3, ...\}$:

$$D_j^{(k)} = \frac{X_j^{(k)} - 1}{l} - 1. \quad (7)$$

Последовательность данных случайных величин $D_j^{(k)}$ является марковской цепью с счетным числом состояний и описывается графом, изображенным на рис. 5, где $q = (1-p)^l$.

Введем обозначение для стационарного распределения марковской цепи:

$$\pi_i \triangleq \lim_{k\to\infty} \Pr\left\{D_j^{(k)} = i\right\},$$

где $i = 1, 2, \ldots$.

Для любого $i > 1$ выполняется равенство

$$\pi_i = \pi_{i-1} q = \pi_1 q^{i-1}. \quad (8)$$

Из условия нормировки $\sum_{i=1}^{\infty} \pi_i = 1$ и (8) получаем

$$\sum_{i=1}^{\infty} \pi_1 q^{i-1} = \frac{\pi_1}{1-q} = 1.$$

Следовательно:

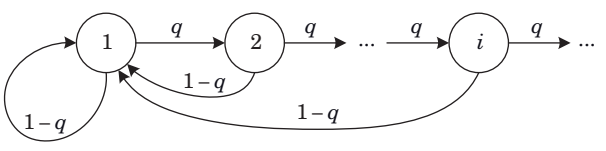
$$\pi_1 = 1 - q.$$

Используя стационарное распределение, получаем

$$\lim_{k\to\infty} E\left[D_j^{(k)}\right] = \sum_{i=1}^{\infty} i\pi_i = \sum_{i=1}^{\infty} i(1-q)q^{i-1} = \frac{1}{1-q}. \quad (9)$$

Покажем, как вычислить $\lim_{k\to\infty} E\left[X_j^{(k)}\right]$. Из выражения (7) получаем

$$X_j^{(k)} = \left(D_j^{(k)} + 1\right) l + 1. \quad (10)$$



■ ***Рис. 5.*** Марковская цепь в виде графа для $D_j^{(k)}$

■ ***Fig. 5.*** Markov chain represented as a graph for $D_j^{(k)}$

Перейдя от (10) к пределу при $k \to \infty$ и вычислив математическое ожидание, получили следующее выражение:

$$\lim_{k\to\infty} E\left[X_j^{(k)}\right] = \left(\lim_{k\to\infty} E\left[D_j^{(k)}\right] + 1\right) l + 1. \quad (11)$$

Подставив выражение (9) в (11) и учитывая, что $q = (1-p)^l$, получаем

$$\lim_{k\to\infty} E\left[X_j^{(k)}\right] = \left(\frac{1}{1-q} + 1\right) l + 1 = \left(\frac{1}{1-(1-p)^l} + 1\right) l + 1,$$

что и требовалось доказать.

Пусть выбрано r ведомых узлов с номерами $j_1, j_2, \ldots, j_r$ для запросов на чтение. Обозначим $Y^{(k)}$ случайную величину:

$$Y^{(k)} = \min\left(X_{j_1}^{(k)}, \ldots, X_{j_r}^{(k)}\right). \quad (12)$$

Утверждение 2. Математическое ожидание возраста информации для r запросов на чтение в слоте с номером τ от начала кадра для любого набора ведомых узлов $j_1, j_2, \ldots, j_r$ одинаково и равно

$$\lim_{k\to\infty} E\left[Y^{(k)} \mid \tau\right] = l + \tau + \frac{l(1-p)^{r(\tau-1)}}{1-(1-p)^{lr}}. \quad (13)$$

Доказательство:

Рассмотрим случай для $\tau = 1$, т. е. запросы поступили в начале кадра. Используя аргументацию из доказательства утверждения 1 и заменяя q на значение, равное $(1-p)^{lr}$, получим

$$\lim_{k\to\infty} E[Y^{(k)} \mid 1] = \left(\frac{1}{1-(1-p)^{lr}} + 1\right) l + 1.$$

Теперь рассмотрим случай, когда запрос на чтение поступил в слоте $\tau \in \{2, \ldots, l\}$. Введем в рассмотрение два события:

1) ни в одном из слотов с номерами $1, 2, \ldots, \tau - 1$ ни у одного из r выбранных узлов не произойдет обновление. Это событие далее будем обозначать как событие $\bar{A}$;

2) хотя бы в одном из слотов с номерами 1, 2, …, $\tau - 1$ хотя бы у одного из r выбранных узлов произойдет обновление. Это событие далее будем обозначать как событие A.

Поскольку события, связанные с доставкой обновления, происходят независимо друг от друга для разных ведомых узлов в одном слоте и независимо в разные слоты для одного узла, вероятности событий A и $\bar{A}$ вычисляются следующим образом:

$$\Pr\{A\} = 1-(1-p)^{r(\tau-1)}; \quad (14)$$

$$\Pr\{\bar{A}\} = (1-p)^{r(\tau-1)}. \quad (15)$$

Если происходит событие A, то в слоте с номером τ значение $Y^{(k)} = \min\left(X_{j_1}^{(k)}, \ldots, X_{j_r}^{(k)}\right)$ будет равно возрасту информации на ведущем узле. То есть возраст информации будет равен $l + \tau$:

$$\lim_{k\to\infty} E\left[Y^{(k)} \mid A, \tau\right] = l + \tau. \quad (16)$$

Если происходит событие $\bar{A}$, то в слоте с номером τ значение $Y^{(k)} = \min\left(X_{j_1}^{(k)}, \ldots, X_{j_r}^{(k)}\right)$ будет равно возрасту информации в начале кадра, увеличенное на τ:

$$\lim_{k\to\infty} E\left[Y^{(k)} \mid \bar{A}, \tau\right] = \left(\frac{1}{1-(1-p)^{lr}} + 1\right) l + \tau. \quad (17)$$

Подставляя (14) в (16) и (15) в (17), получаем

$$\lim_{k\to\infty} E[Y^{(k)} \mid \tau] =$$

$$= \lim_{k\to\infty} E[Y^{(k)} \mid A, \tau]\Pr\{A\} + \lim_{k\to\infty} E[Y^{(k)} \mid \bar{A}, \tau]\Pr\{\bar{A}\} =$$

$$= (l+\tau)\left(1-(1-p)^{r(\tau-1)}\right) +$$

$$+ \left(\left(\frac{1}{1-(1-p)^{lr}} + 1\right) l + \tau\right)(1-p)^{r(\tau-1)} =$$

$$= l + \tau + \frac{l(1-p)^{r(\tau-1)}}{1-(1-p)^{lr}},$$

что и требовалось доказать.

Утверждение 3. Математическое ожидание возраста информации для r запросов на чтение в произвольно выбранном слоте для любого набора ведомых узлов $j_1, j_2, \ldots, j_r$ одинаково и равно

$$\lim_{k\to\infty} E[Y^{(k)}] = l + \frac{l+1}{2} + \frac{1}{1-(1-p)^r}. \quad (18)$$

Доказательство:

Так как запросы в любом слоте кадра появляются с одинаковой вероятностью, то справедливо следующее равенство:

$$\lim_{k\to\infty} E[Y^{(k)}] = \sum_{\tau=1}^{l} \lim_{k\to\infty} E\left[Y^{(k)} \mid \tau\right]\frac{1}{l}.$$

Подставляя в предыдущее равенство выражение (13), получаем

$$\lim_{k\to\infty} E[Y^{(k)}] = \sum_{\tau=1}^{l}\left[1 + \frac{\tau}{l} + \frac{(1-p)^{r(\tau-1)}}{1-(1-p)^{lr}}\right] =$$

$$= l + \frac{l+1}{2} + \frac{1}{1-(1-p)^r},$$

что и требовалось доказать.

Пусть в кадре с номером k выбран i-й ведущий узел. Обозначим возраст информации в этом узле $Z_i^{(k)}$. Так как все ведущие узлы имеют гарантированно последнюю версию данных, легко доказать справедливость следующего утверждения.

Утверждение 4. Математическое ожидание возраста информации для запроса на чтение ведущему узлу с номером i в слоте с номером τ от начала кадра для любого ведущего узла i одинаково и равно

$$\lim_{k\to\infty} E[Z_i^{(k)} \mid \tau] = l + \tau. \quad (19)$$

Из того, что запросы в любом слоте кадра появляются с одинаковой вероятностью, вытекает следующее утверждение.

Утверждение 5. Математическое ожидание возраста информации для запроса на чтение ведущему узлу с номером i в произвольно выбранном слоте для любого ведущего узла i одинаково и равно

$$\lim_{k\to\infty} E[Z_i^{(k)}] = l + \frac{l+1}{2}. \quad (20)$$

Используя приведенные выше утверждения, сформулируем и докажем утверждение относительно среднего возраста информации согласно выражению (3). Для этого рассмотрим случай, когда в произвольный момент времени посылаются запросы к случайно выбранным узлам, среди которых могут быть выбраны как ведущие, так и ведомые.

Утверждение 6. Математическое ожидание среднего возраста информации $\bar{\Delta}$ для r запросов к случайно выбранным узлам, среди которых l ведущих и $n - l$ ведомых, при $r \le n - l$ равно

$$\bar{\Delta} = l + \frac{l+1}{2} + \frac{1}{1-(1-p)^r} \cdot \frac{(n-l)!(n-r)!}{(n-l-r)!n!}. \quad (21)$$

Если $n - l < r \le n$, то математическое ожидание среднего возраста информации

$$\bar{\Delta} = l + \frac{l+1}{2}.$$

Доказательство:

Введем в рассмотрение два события:

1) ни один из выбранных узлов не является ведущим, т. е. все выбранные узлы являются ведомыми. Это событие далее будем обозначать как $\overline{B}$;

2) хотя бы один из выбранных узлов является ведущим. Такое событие будем обозначать как B.

Следует отметить, что если число запросов r превышает число ведущих узлов l, т. е. $r > n - l$, то событие B будет возникать с вероятностью 1. В противном случае для вероятностей появления введенных событий справедливы следующие выражения:

$$\Pr\left\{\overline{B}\right\} = \frac{n-l}{n}\cdot\frac{n-l-1}{n-1}\cdot\ldots\cdot\frac{n-l-r-1}{n-r-1} = \prod_{i=0}^{r-1}\frac{n-l-i}{n-i} = \frac{(n-l)!(n-r)!}{(n-l-r)!n!}; \quad (22)$$

$$\Pr\{B\} = 1 - \frac{(n-l)!(n-r)!}{(n-l-r)!n!}. \quad (23)$$

Рассматривая введенные события (22) и (23) и используя утверждения 3 и 5, для случая $r \le n - l$ получаем

$$\overline{\Delta} = \lim_{k\to\infty} E\left[Y^{(k)}\right]\Pr\left\{\overline{B}\right\} + \lim_{k\to\infty} E\left[Z_i^{(k)}\right]\Pr\{B\} = \left(l + \frac{l+1}{2}\right)\cdot\left(1 - \frac{(n-l)!(n-r)!}{(n-l-r)!n!}\right) + \left(l + \frac{l+1}{2} + \frac{1}{1-(1-p)^r}\right)\cdot\frac{(n-l)!(n-r)!}{(n-l-r)!n!} = l + \frac{l+1}{2} + \frac{1}{1-(1-p)^r}\cdot\frac{(n-l)!(n-r)!}{(n-l-r)!n!}.$$

Если $r > n - l$, то, используя вышеупомянутые $\Pr\left\{\overline{B}\right\} = 0$, $\Pr\{B\} = 1$ для среднего возраста информации, получаем

$$\lim_{k\to\infty} E\left[\overline{\Delta}\right] = l + \frac{l+1}{2}.$$

Следовательно, утверждение 6 доказано.

Таким образом, получено выражение для расчета среднего возраста информации при заданных параметрах системы. Далее будет сформулирована оптимизационная задача по выбору числа ведущих узлов для минимизации среднего возраста информации.

Выбор числа ведущих узлов в системе

Выше была получена явная зависимость среднего возраста информации от параметров модели (21), что позволяет сформулировать оптимизационную задачу по выбору числа ведущих узлов при заданных значениях параметров n, p и r:

$$l_{\text{opt}} = \arg\min_{1\le l\le n}\overline{\Delta}(l, n, p, r). \quad (24)$$

Для решения оптимизационной задачи (24) сложно получить явную зависимость l_{opt} от параметров модели. Далее показано, как можно получить в явном виде приближенное решение для этой задачи.

Введем в рассмотрение следующую функцию:

$$f(l, n, p, r) = \frac{l+1}{2} + l + \frac{1}{1-(1-p)^r}\cdot\left(\frac{n-l}{n}\right)^r. \quad (25)$$

Можно доказать, что функция $f(l)$ является верхней оценкой для (21), и минимальные значения для $f(l)$ и для среднего возраста информации, вычисляемого по формуле (21) при $n > 50$, достигаются при значениях l, отличающихся не более чем на 1. Сформулируем следующую оптимизационную задачу:

$$\tilde{l}_{\text{opt}} = \left[\arg\min_{1\le l\le n} f(l, n, p, r)\right], \quad (26)$$

где [] означает округление до ближайшего целого числа.

Так как $f(l, n, p, r)$ является унимодальной и выпуклой вниз функцией по переменной l, решение для (26) может быть легко получено следующим образом.

Рассмотрим выражение (25) как функцию от действительной переменной l. Вычисляя первую производную по l и приравнивая к 0, получим следующее уравнение:

$$\frac{3}{2} - \frac{r(n-l)^{r-1}}{n^r - (n-np)^r} = 0. \quad (27)$$

Решение уравнения (27) при большом n становится отрицательным. Это означает, что для каждого набора параметров существует некоторое критическое значение числа узлов n такое, что использование ведущих узлов неизбежно будет приводить к увеличению среднего возраста информации. Следовательно, при достижении этого критического значения в системе следует использовать только один ведущий узел.

Используя решение уравнения (27), получаем, что решение оптимизационной задачи (26) для фиксированных n, p и r определяется следующим образом:

$$\tilde{l}_{\text{opt}}(n, p, r) = \\ = \max\left(n - \left(\frac{3}{2r}\left(n^r - (n - np)^r \right) \right)^{\frac{1}{r-1}}, 1 \right), \quad (28)$$

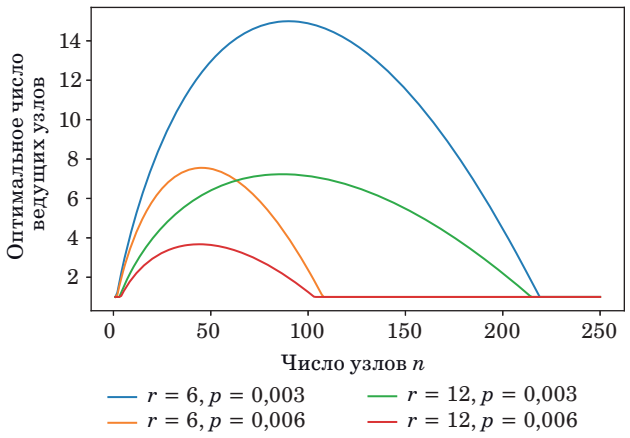
где $r > 1$.

Выражение (28) является приближенным решением оптимизационной задачи (24) по выбору числа ведущих узлов. Следует отметить, что при большом числе узлов в системе приближенное решение незначительно отличается от оптимального. Далее, при обсуждении полученных результатов, для краткости изложения, там, где это не будет вызывать неоднозначности, данное решение будем называть оптимальным. Ниже будут наглядно продемонстрированы особенности работы системы с использованием полученного выражения (28) в зависимости от различных параметров.

Графики зависимости оптимального числа ведущих узлов $\tilde{l}_{\text{opt}}$ от общего числа всех узлов в системе n (рис. 6) построены при фиксированных параметрах p и r. Для наглядной демонстрации свойств системы были выбраны значения $p = 0{,}003$, $p = 0{,}006$, $r = 6$ и $r = 12$. Можно заметить, что при фиксированном числе узлов в запросе на чтение r с увеличением вероятности успешной доставки p уменьшается максимальное значение $\tilde{l}_{\text{opt}}$. Вначале число ведущих узлов, при которых средний возраст информации минимален, возрастает до некоторого порогового значения n, превышая которое число ведущих узлов начинает уменьшаться вплоть до одного ведущего узла. С увеличением вероятности успешной доставки p данное пороговое значение уменьшается. При фиксированном значении p с увеличением r максимальное значение $\tilde{l}_{\text{opt}}$ также уменьшается, а пороговое значение n остается неизменным.

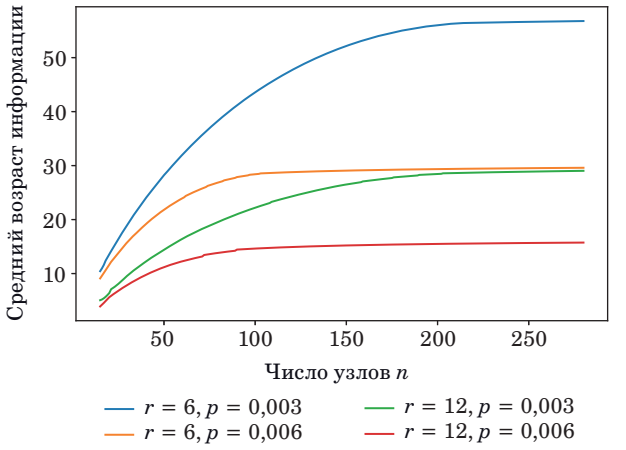
Зависимости среднего возраста информации от числа узлов в системе при оптимальном соотношении между ведущими и ведомыми узлами показаны на рис. 7. При построении этих зависимостей для каждого набора параметров n, p и r использовалось выражение (28). Далее, с использованием данного значения в качестве числа лидеров, вычислялось значение среднего возраста информации согласно выражению (21). Следует отметить, что использование в качестве выбора числа лидеров решения оптимизационной задачи (26) вместо (24) влияет на значения среднего возраста информации при малом количестве узлов в системе. Это проявляется в том, что, если число узлов n не превышает 20, график зависимости среднего возраста информации от числа узлов в системе имеет «волнообразный вид», что отличает его от вида графика этой зависимости при большем числе узлов.

Из графиков, представленных на рис. 7, следует, что уменьшение вероятности p успешной доставки обновления на ведомые узлы приводит к увеличению среднего возраста информации в системе, которое можно компенсировать увеличением числа узлов в запросе на чтение r. Также отметим, что после достижения критического значения n наблюдается медленный рост среднего возраста информации, что объясняется следующим. После достижения критического значения в системе присутствует только один ведущий узел, и выражение (21) принимает вид



■ ***Рис. 6.*** Зависимость оптимального числа ведущих узлов $\tilde{l}_{\text{opt}}$ от общего числа узлов n в системе

■ ***Fig. 6.*** The dependence of the optimal number of leader nodes $\tilde{l}_{\text{opt}}$ on the total number of nodes n



■ ***Рис. 7.*** Зависимость среднего возраста информации от общего числа узлов n в системе при оптимальном выборе числа ведущих узлов

■ ***Fig. 7.*** Graphs of the dependence of the average age of information on the total number of the nodes n under optimal selection of the number of leader nodes

$$\bar{\Delta} = 2 + \frac{1}{1-(1-p)^r} \cdot \frac{n-r}{n}.$$

Таким образом, наглядно продемонстрированы основные особенности работы системы при использовании оптимального числа ведущих узлов в зависимости от других параметров системы.

Заключение

Предложена модель, отражающая основные особенности реплицируемых систем хранения данных, такие как хранение некоторого фрагмента данных (реплики) на множестве узлов и подразделение их на ведущие и ведомые. Первая обеспечивает доступность данных в системе, а вторая повышает уровень согласованности. Рассмотрен такой показатель качества функционирования системы, как средний возраст информации, полученной по запросу на чтение. В рамках предложенной модели сформулирована оптимизационная задача по распределению узлов на ведомые и ведущие, при котором минимизируется средний возраст информации. Найдено приближенное решение данной оптимизационной задачи. Учитываются показатели надежности доставки данных при обновлении, т. е. при перезаписи уже имеющегося фрагмента данных в хранилище, и выборе числа ведущих и ведомых узлов. Предложенная модель может быть использована в качестве базового элемента при проектировании более сложных систем для решения задачи соблюдения баланса согласованности и доступности. Одной из важных особенностей данной модели является допущение о том, что события успешной доставки обновления данных на разные узлы независимы. Так как в реальных системах используется многоадресная передача, и сообщение, адресованное нескольким узлам, может идти по одному маршруту, указанное допущение может быть несправедливо, и возникнет зависимость между событиями доставки одного обновления разным узлам. Используя подходы из работ [25–27], можно предложить модель, которая будет учитывать зависимость между этими событиями. Можно также высказать гипотезу, что при такой зависимости полученное решение оптимизационной задачи дает оценку снизу для среднего возраста информации, а не его точное значение, что служит предметом для дальнейшего исследования.

Финансовая поддержка

Исследование выполнено при финансовой поддержке Российского научного фонда, грант № 22-19-00305 «Пространственно-временные стохастические модели беспроводных сетей с большим числом абонентов».

Литература

1. **Wiesmann M., Pedone F., Schiper A., Kemme B., and Alonso G.** Understanding replication in databases and distributed systems. *Proc. 20th IEEE Intern. Conf. on Distributed Computing Systems*, IEEE, 2000, pp. 464–474. doi:10.1109/ICDCS.2000.840959
2. **Богатырев В. А., Богатырев С. В., Богатырев А. В.** Оценка готовности компьютерной системы к своевременному обслуживанию запросов при его совмещении с информационным восстановлением памяти после отказов. *Научно-технический вестник информационных технологий, механики и оптики*, 2023, т. 23, № 3, с. 608–617. doi:10.17586/2226-1494-2023-23-3-608-617
3. **Lee E. A., Akella R., Bateni S., Lin S., Lohstroh M., Menard C.** Consistency vs. availability in distributed cyber-physical systems. *ACM Transactions on Embedded Computing Systems*, 2023, vol. 22, no. 5s, pp. 1–24. https://doi.org/10.1145/3609119
4. **Bogatyrev V. A., Bogatyrev A. V., Bogatyrev S. V.** (2023). Multipath Transmission of Heterogeneous Traffic in Acceptable Delays with Packet Replication and Destruction of Expired Replicas in the Nodes that Make Up the Path. In: *Distributed Computer and Communication Networks. DCCN 2022. Communications in Computer and Information Science*/ V. M. Vishnevskiy, K. E. Samouylov, D. V. Kozyrev (eds). Springer, Cham, 2023, vol. 1748. https://doi.org/10.1007/978-3-031-30648-8_9
5. **Armstrong T. G., Ponnekanti V., Borthakur D., Callaghan M.** LinkBench: A database benchmark based on the Facebook social graph. *Proc. of the 2013 ACM SIGMOD Intern. Conf. on Management of Data*, 2013, pp. 1185–1196. https://doi.org/10.1145/2463676.2465296
6. **Corbett J. C., Dean J., Epstein M., Fikes A., Frost C., Furman J. J., Ghemawat S., Gubarev A., Heiser C., Hochschild P., Hsieh W., Kanthak S., Kogan E., Li H., Lloyd A., Melnik S., Mwaura D., Nagle D., Quinlan S., Rao R., Rolig L., Saito Y., Szymaniak M., Taylor C., Wang R., and Woodfor D.** Spanner: Google's globally distributed database. *ACM Trans. Comput. Syst.*, 2013, vol. 31, no. 3, Article 8, 22 p. doi:http://dx.doi.org/10.1145/2491245
7. **Mathew S., Varia J.** Overview of amazon web services. *Amazon Whitepapers*, 2014, vol. 105, no. 1, pp. 22.
8. **Chrysafis C., Collins B., Dugas S., Dunkelberger J., Ehsan M., Gray S., Grieser A., Herrnstadt O., LevAri K., Lin T., McMahon M., Schiefer N., and**

Shraer A. FoundationDB record layer: A multi-tenant structured datastore. *2019 Intern. Conf. on Management of Data (SIGMOD '19)*, June 30–July 5, 2019, Amsterdam, Netherlands. ACM, New York, NY, USA, 16 p. https://doi.org/10.1145/3299869.3314039

9. **Chandra T. D., Griesemer R., Redstone J.** Paxos made live: An engineering perspective. *Proc. of the Twenty-sixth Annual ACM Symp. on Principles of Distributed Computing*, 2007, pp. 398–407. https://doi.org/10.1145/1281100.1281103
10. **Ongaro D., Ousterhout J.** In search of an understandable consensus algorithm. *2014 USENIX Annual Technical Conf. (USENIX ATC 14)*, 2014, pp. 305–319.
11. **Zhou S., Mu S.** {Fault-Tolerant} replication with {Pull-Based} consensus in {MongoDB}. *18th USENIX Symp. on Networked Systems Design and Implementation (NSDI 21)*, 2021, pp. 687–703.
12. **Zhu X., Nie X., Liu J.** Time series database optimization based on InfluxDB. *2023 Intern. Conf. on Power, Electrical Engineering, Electronics and Control (PEEEC)*, IEEE, 2023, pp. 879–885. doi:10.1109/PEEEC60561.2023.00172
13. **Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V.** Efficiency of servicing heterogeneous traffic when allocating cluster nodes for redundant execution of latency-critical requests. *CEUR Workshop Proc.*, 2021, vol. 3057, pp. 266–273.
14. **Yates R. D., Sun Y., Brown D. R., Kaul S. K., Modiano E., Ulukus S.** Age of information: An introduction and survey. *IEEE Journal on Selected Areas in Communications*, 2021, vol. 39, no. 5, pp. 1183–1210. doi:10.1109/JSAC.2021.3065072
15. **Sun Y., Kadota I., Modiano E.** *Age of Information: A New Metric for Information Freshness*. Springer Nature, 2022. doi:10.2200/s00954ed2v01y201909cnt023
16. **Broadhead J. S., Pawełczak P.** Data freshness in mixed-memory intermittently-powered systems. *2021 IEEE Intern. Symp. on Information Theory (ISIT)*, IEEE, 2021, pp. 3361–3366. doi:10.1109/ISIT45174.2021.9518156
17. **Борисовская А. В., Тюрликов А. М.** Оценка среднего возраста информации в системах со случайным доступом и множественным выходом. *Информационно-управляющие системы*, 2023, № 1, с. 51–60. doi:10.31799/1684-8853-2023-1-51-60, EDN: UBBHKD
18. **Kumar M. S., Dadlani A., Moradian M., Maham B., Tsiftsis T. A.** Age of information in multi-source updating systems: An M/G/1 vacation queueing model. *ICC 2023-IEEE Intern. Conf. on Communications*, IEEE, 2023, pp. 63–68. doi:10.1109/ICC45041.2023.10278746
19. **Борисовская А. В.** Модели сенсорных сетей с зависимыми источниками. *T-Comm: Телекоммуникации и транспорт*, 2023, т. 17, № 7, с. 21–28. doi:10.36724/2072-8735-2023-17-7-21-28
20. **Chen Z., Deng D., Yang H. H., Pappas N., Hu L., Jia Y., Wang M., Quek T. Q. S.** Analysis of age of information in dual updating systems. *IEEE Transactions on Wireless Communications*, 2023, vol. 22, iss. 11, pp. 8003–8019. doi:10.1109/TWC.2023.3257356
21. **Rizk A., Le Boudec J. Y.** A Palm calculus approach to the distribution of the age of information. *IEEE Transactions on Information Theory*, 2023, vol. 69, iss. 12, pp. 8097–8110. doi:10.1109/TIT.2023.3326381
22. **Behrouzi-Far A., Soljanin E., Yates R. D.** Data freshness in leader-based replicated storage. *2020 IEEE Intern. Symp. on Information Theory (ISIT)*, IEEE, 2020, pp. 1806–1811. doi:10.1109/ISIT44484.2020.9174411
23. **Zhang C., Wang L., Xiao L., Jiang S., Han M., Wang J., Wei B., Qin G.** Minimizing the cost of periodically replicated systems via model and quantitative analysis. *Front. Comput. Sci.*, 2024, vol. 18, Article 185206. https://doi.org/10.1007/s11704-023-2625-8
24. **Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V.** Control of multipath transmissions in the nodes of switching segments of reserved paths. *2022 Intern. Conf. on Information, Control, and Communication Technologies (ICCT)*, 2022, pp. 1–5.
25. **Ateya A. A., Bushelenkov S., Muthanna A., Paramonov A., Koucheryavy A., Chelloug S. A., Abd El-Latif A. A.** Multipath routing scheme for optimum data transmission in dense Internet of Things. *Mathematics*, 2023, vol. 11, iss. 19, p. 4168. doi:10.3390/math11194168, EDN ZQDDWQ
26. **Bushelenkov S., Paramonov A., Muthanna A., Abd El-Latif A. A., Koucheryavy A., Alfarraj O., Pławiak P., Ateya A. A.** Multi-story building model for efficient IoT network design. *Mathematics*, 2023, vol. 11, iss. 6, p. 1403. doi:10.3390/math11061403, EDN VMJVEM
27. **Vorobyova D., Muthanna A., Paramonov A., Markelov O. A., Koucheryavy A., Ali G., ElAffendi M., Abd El-Latif A. A.** IoT network model with multimodal node distribution and data-collecting mechanism using mobile clustering nodes. *Electronics*, 2023, vol. 12, iss. 6, p. 1410. doi:10.3390/electronics12061410, EDN BHNVEU

UDC 004.62, 004.7
doi:10.31799/1684-8853-2024-3-11-23
EDN: XSSHJI

Modeling a replicated storage system with the use of the average age of information as an indicator of data relevance

D. R. Krylov[a], Master Student, orcid.org/0009-0008-5901-5342
E. D. Poymanova[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-7903-2480
A. M. Turlikov[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-7132-094X, turlikov@guap.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: An urgent task for leader-based replicated storage is to ensure consistency and availability balance. There is no generally accepted quantitative indicator characterizing such a balance; however, achieving the balance ensures data relevance, which can be quantified using the average age of the information. **Purpose:** To propose a model that represents the main features of a replicated storage system and makes it possible to formulate and solve the task of minimizing the age of information by distributing system nodes into leaders and followers. **Results:** We propose a model of a replicated data storage system based on leaders and followers with the use of the average age of information as a data relevance indicator. Within the framework of the proposed model, we formulate an optimization problem for the distribution of nodes into followers and leaders, which minimizes the average age of information with indicators of reliability of data delivery taken in consideration when overwriting an existing fragment of data in the storage. We also obtain an approximate solution to this optimization problem. **Practical relevance:** The proposed model represents general features of a replicated storage system and can be used in real systems when solving the problem of maintaining a consistency and availability balance. **Discussion:** A key feature of the proposed model is the assumption that the event of successful data update delivery is independent for different followers. If these events are dependent, we can hypothesize that the considered optimization problem solution will not be an exact value, but a lower estimate for the average age of information. The confirmation or refutation of this hypothesis is a subject for further research.

Keywords — average age of information, data storage, replication, leaders, followers.

For citation: Krylov D. R., Poymanova E. D., Turlikov A. M. Modeling a replicated storage system with the use of the average age of information as an indicator of data relevance. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 3, pp. 11–23 (In Russian). doi:10.31799/1684-8853-2024-3-11-23, EDN: XSSHJI

Financial support

The research was financially supported by the Russian Science Foundation, grant No. 22-19-00305 “Spatio-temporal stochastic models of wireless networks with a large number of subscribers”.

References

1. Wiesmann M., Pedone F., Schiper A., Kemme B., and Alonso G. Understanding replication in databases and distributed systems. *Proc. 20th IEEE Intern. Conf. on Distributed Computing Systems*, IEEE, 2000, pp. 464–474. doi:10.1109/ICDCS.2000.840959
2. Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V. Assessment of the readiness of a computer system for timely servicing of requests when combined with information recovery of memory after failures. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2023, vol. 23, no. 3, pp. 608–617 (In Russian). doi:10.17586/2226-1494-2023-23-3-608-617
3. Lee E. A., Akella R., Bateni S., Lin S., Lohstroh M., Menard C. Consistency vs. availability in distributed cyber-physical systems. *ACM Transactions on Embedded Computing Systems*, 2023, vol. 22, no. 5s, pp. 1–24. https://doi.org/10.1145/3609119
4. Bogatyrev V. A., Bogatyrev A. V., Bogatyrev S. V. *Multipath Transmission of Heterogeneous Traffic in Acceptable Delays with Packet Replication and Destruction of Expired Replicas in the Nodes that Make Up the Path*. In: Vishnevskiy V. M., Samouylov K. E., Kozyrev D. V. (eds). *Distributed Computer and Communication Networks. DCCN 2022. Communications in Computer and Information Science*. Springer, Cham, 2023, vol. 1748. https://doi.org/10.1007/978-3-031-30648-8_9
5. Armstrong T. G., Ponnekanti V., Borthakur D., Callaghan M. LinkBench: A database benchmark based on the Facebook social graph. *Proc. of the 2013 ACM SIGMOD Intern. Conf. on Management of Data*, 2013, pp. 1185–1196. https://doi.org/10.1145/2463676.2465296
6. Corbett J. C., Dean J., Epstein M., Fikes A., Frost C., Furman J. J., Ghemawat S., Gubarev A., Heiser C., Hochschild P., Hsieh W., Kanthak S., Kogan E., Li H., Lloyd A., Melnik S., Mwaura D., Nagle D., Quinlan S., Rao R., Rolig L., Saito Y., Szymaniak M., Taylor C., Wang R., and Woodfor D. Spanner: Google’s globally distributed database. *ACM Trans. Comput. Syst*., 2013, vol. 31, no. 3, Article 8, 22 p. doi:http://dx.doi.org/10.1145/2491245
7. Mathew S., Varia J. Overview of amazon web services. *Amazon Whitepapers*, 2014, vol. 105, no. 1, pp. 22.
8. Chrysafis C., Collins B., Dugas S., Dunkelberger J., Ehsan M., Gray S., Grieser A., Herrnstadt O., LevAri K., Lin T., McMahon M., Schiefer N., and Shraer A. FoundationDB record layer: A multi-tenant structured datastore. *2019 Intern. Conf. on Management of Data (SIGMOD ’19)*, June 30–July 5, 2019, Amsterdam, Netherlands. ACM, New York, NY, USA, 16 p. https://doi.org/10.1145/3299869.3314039
9. Chandra T. D., Griesemer R., Redstone J. Paxos made live: An engineering perspective. *Proc. of the Twenty-sixth Annual ACM Symp. on Principles of Distributed Computing*, 2007, pp. 398–407. https://doi.org/10.1145/1281100.1281103
10. Ongaro D., Ousterhout J. In search of an understandable consensus algorithm. *2014 USENIX Annual Technical Conf. (USENIX ATC 14)*, 2014, pp. 305–319.
11. Zhou S., Mu S. {Fault-Tolerant} replication with {Pull-Based} consensus in {MongoDB}. *18th USENIX Symp. on Networked Systems Design and Implementation (NSDI 21)*, 2021, pp. 687–703.
12. Zhu X., Nie X., Liu J. Time series database optimization based on InfluxDB. *2023 Intern. Conf. on Power, Electrical Engineering, Electronics and Control (PEEEC)*, IEEE, 2023, pp. 879–885. doi:10.1109/PEEEC60561.2023.00172
13. Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V. Efficiency of servicing heterogeneous traffic when allocating cluster nodes for redundant execution of latency-critical requests. *CEUR Workshop Proc*., 2021, vol. 3057, pp. 266–273.
14. Yates R. D., Sun Y., Brown D. R., Kaul S. K., Modiano E., Ulukus S. Age of information: An introduction and survey. *IEEE Journal on Selected Areas in Communications*, 2021, vol. 39, no. 5, pp. 1183–1210. doi:10.1109/JSAC.2021.3065072
15. Sun Y., Kadota I., Modiano E. *Age of Information: A New Metric for Information Freshness*. Springer Nature, 2022. doi:10.2200/s00954ed2v01y201909cnt023
16. Broadhead J. S., Pawełczak P. Data freshness in mixed-memory intermittently-powered systems. *2021 IEEE Intern. Symp. on Information Theory (ISIT)*, IEEE, 2021, pp. 3361–3366. doi:10.1109/ISIT45174.2021.9518156
17. Borisovskaya A. V., Turlikov A. M. Estimation of the average age of information in random access systems with multiple departure. *Informatsionno-upravliaiushchie sistemy* [In-

formation and Control Systems], 2023, no. 1, pp. 51–60 (In Russian). doi:10.31799/1684-8853-2023-1-51-60, EDN: UBBHKD
18. Kumar M. S., Dadlani A., Moradian M., Maham B., Tsiftsis T. A. Age of information in multi-source updating systems: An M/G/1 vacation queueing model. *ICC 2023-IEEE Intern. Conf. on Communications*, IEEE, 2023, pp. 63–68. doi:10.1109/ICC45041.2023.10278746
19. Borisovskaya A. V. Models of sensor networks with correlated sources. *T-Comm*, 2023, vol. 17, no. 7, pp. 21–28 (In Russian). doi:10.36724/2072-8735-2023-17-7-21-28
20. Chen Z., Deng D., Yang H. H., Pappas N., Hu L., Jia Y., Wang M., Quek T. Q. S. Analysis of age of information in dual updating systems. *IEEE Transactions on Wireless Communications*, 2023, vol. 22, iss. 11, pp. 8003–8019. doi:10.1109/TWC.2023.3257356
21. Rizk A., Le Boudec J. Y. A Palm calculus approach to the distribution of the age of information. *IEEE Transactions on Information Theory*, 2023, vol. 69, iss. 12, pp. 8097–8110. doi:10.1109/TIT.2023.3326381
22. Behrouzi-Far A., Soljanin E., Yates R. D. Data freshness in leader-based replicated storage. *2020 IEEE Intern. Symp. on Information Theory (ISIT)*, IEEE, 2020, pp. 1806–1811. doi:10.1109/ISIT44484.2020.9174411
23. Zhang C., Wang L., Xiao L., Jiang S., Han M., Wang J., Wei B., Qin G. Minimizing the cost of periodically replicated systems via model and quantitative analysis. *Front. Comput. Sci*., 2024, vol. 18, Article 185206. https://doi.org/10.1007/s11704-023-2625-8
24. Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V. Control of multipath transmissions in the nodes of switching segments of reserved paths. *2022 Intern. Conf. on Information, Control, and Communication Technologies (ICCT)*, 2022, pp. 1–5.
25. Ateya A. A., Bushelenkov S., Muthanna A., Paramonov A., Koucheryavy A., Chelloug S. A., Abd El-Latif A. A. Multipath routing scheme for optimum data transmission in dense Internet of Things. *Mathematics*, 2023, vol. 11, iss. 19, p. 4168. doi:10.3390/math11194168, EDN ZQDDWQ
26. Bushelenkov S., Paramonov A., Muthanna A., Abd El-Latif A. A., Koucheryavy A., Alfarraj O., Pławiak P., Ateya A. A. Multi-story building model for efficient IoT network design. *Mathematics*, 2023, vol. 11, iss. 6, p. 1403. doi:10.3390/math11061403, EDN VMJVEM
27. Vorobyova D., Muthanna A., Paramonov A., Markelov O. A., Koucheryavy A., Ali G., ElAffendi M., Abd El-Latif A. A. IoT network model with multimodal node distribution and data-collecting mechanism using mobile clustering nodes. *Electronics*, 2023, vol. 12, iss. 6, p. 1410. doi:10.3390/electronics12061410, EDN BHNVEU

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая Scopus и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, что снижает рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12 языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org

УДК 621.391.1:621.395
doi:10.31799/1684-8853-2024-3-24-31
EDN: QEGHLU

Научные статьи
Articles

Управление характеристиками систем массового обслуживания через сдвиг законов распределений в виде вероятностных смесей

В. Н. Тарасов[a], *доктор техн. наук, профессор, orcid.org/0000-0002-9318-0797, v.tarasov@psuti.ru*
Н. Ф. Бахарева[a], *доктор техн. наук, профессор, orcid.org/0000-0002-9850-7752*
[a]*Поволжский государственный университет телекоммуникаций и информатики, Льва Толстого ул., 23, Самара, 443010, РФ*

Введение: *необходимость минимизации времени ожидания в очереди и объемов буферов хранения данных в перспективных системах передачи данных остается актуальной и требует постоянной доработки.* ***Цель:*** *расширение класса систем массового обслуживания как систем с подвергнутыми операции сдвига законами распределений в виде вероятностных смесей для решения поставленной проблемы.* ***Методы:*** *метод спектрального решения интегрального уравнения Линдли на основе теории преобразования Лапласа.* ***Результаты:*** *разработаны численно-аналитическая и имитационная модели для двух различных систем с гиперэкспоненциальным и гиперэрланговским входными распределениями. Выявлено, что сдвиг законов распределений вправо уменьшает коэффициенты вариаций, а они вносят основной вклад в формирование величины среднего времени ожидания требований в очереди. Тогда в системах со сдвинутыми распределениями время ожидания уменьшится многократно в зависимости от величины параметра сдвига. Учитывая функциональную зависимость основных критериев эффективности систем от среднего времени ожидания по формулам Литтла, убеждаемся в возможности их регулирования с помощью параметра временного сдвига. Это позволит контролировать основные характеристики реальных систем передачи данных, что важно для теории и практики проектирования таких систем.* ***Практическая значимость:*** *полученные результаты представляют большой интерес для теории и практики передачи данных, позволяя регулировать основные параметры систем передачи данных.* ***Обсуждение:*** *для развития проведенных исследований важны результаты внедрения предложенного подхода в теорию и практику передачи данных. Для этого необходимо получить результаты работы экспериментального программно-аппаратного комплекса для подтверждения данных численно-аналитических и имитационных моделей.*

Ключевые слова *— системы с временным сдвигом, изображение Лапласа, интегральное уравнение Линдли, спектральное решение, дискретно-событийное моделирование, GPSS World.*

Для цитирования: Тарасов В. Н., Бахарева Н. Ф. Управление характеристиками систем массового обслуживания через сдвиг законов распределений в виде вероятностных смесей. *Информационно-управляющие системы*, 2024, № 3, с. 24–31. doi:10.31799/1684-8853-2024-3-24-31, EDN: QEGHLU

For citation: Tarasov V. N., Bakhareva N. F. Controlling the characteristics of a queueing system through shifting distribution laws in the form of probabilistic mixtures. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 3, pp. 24–31 (In Russian). doi:10.31799/1684-8853-2024-3-24-31, EDN: QEGHLU

Введение

В открытой печати исследования в заявленной предметной области авторами не обнаружены, хотя применяемый основной метод спектрального решения уравнения Линдли используется во многих работах [1–3 и др.]. Настоящее исследование является логическим продолжением работ [4, 5–8]. Рассмотрим однолинейные системы массового обслуживания (СМО) A/B/1, в которых законы распределения A и B подвергнуты операции сдвига вправо, и тогда функции плотности, с помощью которых формируется система, имеют вид

$$a(t) = \begin{cases} a(t - t_0), & t \ge t_0 \\ 0, & 0 \le t < t_0 \end{cases};$$

$$b(t) = \begin{cases} b(t - t_0), & t \ge t_0 \\ 0, & 0 \le t < t_0 \end{cases}. \qquad (1)$$

Применяемый метод спектрального решения требует выполнения условия преобразования функции (1) по Лапласу.

Временной сдвиг законов распределений, формирующих СМО, уменьшает коэффициенты вариаций распределений и тем самым приводит СМО к наиболее общему типу G/G/1. Основная идея определения средней задержки требований в очереди путем решения интегрального уравнения Линдли спектральным методом сводится к установлению закона распределения времени ожидания через изображения Лапласа $A^*(s)$, $B^*(s)$ функций плотности $a(t)$ и $b(t)$. Для решения этой задачи конструируется рациональная функция

$$A^*(-s)\,B^*(s) - 1 = \alpha(s)/\beta(s) \qquad (2)$$

комплексной переменной s. Таким образом, сам метод спектрального решения включает эта-

пы построения дробно-рациональных функций $\alpha(s)$, $\beta(s)$ и нахождения ее нулей и полюсов в комплексной плоскости.

В настоящей статье представлены результаты исследований по двум характерным системам. Первая система образована потоками, определяемыми сдвинутой функцией гиперэкспоненциального распределения второго порядка

$$F(t)=\begin{cases}1-\sum\limits_{k=1}^{2}p_i e^{-\lambda_i(t-t_0)}, & t\ge t_0\\ 0, & 0\le t<t_0\end{cases},\quad \sum_{i=1}^{2}p_i=1$$

и сдвинутой функцией экспоненциального распределения

$$F(t)=\begin{cases}1-e^{-\lambda(t-t_0)}, & t\ge t_0\\ 0, & 0\le t<t_0\end{cases}.$$

Вторая система сформирована потоками, описываемыми сдвинутой функцией гиперэрланговского распределения второго порядка

$$F(t)=\begin{cases}\sum\limits_{i=1}^{2}p_i\left[1-e^{-\lambda_i(t-t_0)}\sum\limits_{k=0}^{1}\dfrac{[\lambda_i(t-t_0)]^k}{k!}\right], & t\ge t_0\\ 0, & 0\le t<t_0\end{cases},$$

$$\sum_{i=1}^{2}p_i=1$$

и сдвинутой функцией распределения Эрланга второго порядка

$$F(t)=\begin{cases}1-e^{-\lambda(t-t_0)}\sum\limits_{k=0}^{1}\dfrac{[\lambda(t-t_0)]^k}{k!}, & t\ge t_0\\ 0, & 0\le t<t_0\end{cases}.$$

Тогда первая СМО будет описываться функциями плотности

$$a(t)=p\lambda_1 e^{-\lambda_1(t-t_0)}+(1-p)\lambda_2 e^{-\lambda_2(t-t_0)};$$
$$b(t)=\mu e^{-\mu(t-t_0)}, \qquad (3)$$

а вторая –

$$a(t)=p\lambda_1^2(t-t_0)e^{-\lambda_1(t-t_0)}+(1-p)\lambda_2^2(t-t_0)e^{-\lambda_2(t-t_0)};$$
$$b(t)=\mu^2(t-t_0)e^{-\mu(t-t_0)}. \qquad (4)$$

Численно-аналитическая модель первой СМО представлена в работе [5], а второй — в [6]. Имитационные модели данных систем апробированы в [8]. Здесь же мы будем акцентировать внимание не на численно-аналитических моделях, а на свойствах систем с запаздыванием во времени, а именно на возможности контроля (управления) основных характеристик СМО с помощью величины параметра сдвига t_0.

Ближе всех к системам с запаздыванием стоят работы зарубежных авторов [9, 10]. В настоящей работе авторами использованы известные приемы и методы аппроксимации законов распределений [11–13]. Значительный интерес с точки зрения теории массового обслуживания представляют работы [14–23].

Постановка и решение задачи

Пусть заданы СМО, описываемые функциями плотности (3) и (4). На их численно-аналитических и имитационных моделях требуется провести вычислительный и имитационный эксперименты с целью подтвердить возможности управления основными характеристиками СМО. Тем самым признать, что основные выводы [4] для систем с простыми законами распределений полностью справедливы и для систем с составными распределениями.

Как известно из теории вероятностей, сдвиг закона распределения вправо на величину t_0 влечет за собой увеличение математического ожидания случайной величины на эту же величину, и при этом значение коэффициента вариации, обратно пропорциональное математическому ожиданию, уменьшится. Тогда мы можем утверждать, что среднее время ожидания в системе уменьшится, и в этом будет заключаться принципиальное отличие рассматриваемых систем от классических систем массового обслуживания [4].

Из свойства запаздывания теории преобразования Лапласа следует, что для любой скалярной величины $t_0>0$ справедливо равенство $L[f(t-t_0)]=e^{-st_0}\cdot F^*(s)$, где $\mathrm{Re}(s)>0$. Тогда для спектрального разложения $A^*(-s)B^*(s)-1=\alpha(s)/\beta(s)$ для СМО с операционным сдвигом имеет место равенство

$$\alpha(s)/\beta(s)=e^{t_0 s}A^*(-s)e^{-t_0 s}B^*(s)-1=$$
$$=A^*(-s)B^*(s)-1. \qquad (5)$$

Следовательно, спектральные решения для двух совершенно различных систем — системы с запаздыванием и соответствующей ей классической системы — по форме совпадают. Тогда будут совпадать и расчетные формулы для среднего времени ожидания, но для системы с запаздыванием будут изменены параметры образующих законов распределений.

Численно-аналитическое решение задачи для первой СМО

Рассмотрим систему, образованную с помощью функций плотности (3) с изображениями Лапласа

$$A^*(s) = \left[p\left(\frac{\lambda_1}{\lambda_1 + s}\right) + (1-p)\left(\frac{\lambda_2}{\lambda_2 + s}\right) \right] e^{-t_0 s};$$

$$B^*(s) = \frac{\mu}{s+\mu} e^{-t_0 s},$$

и кратко напомним об основных сведениях об этой системе [5].

Спектральное решение как для классической системы, так и системы с запаздыванием, описываемой функциями плотности (3), будет иметь вид

$$\frac{\alpha(s)}{\beta(s)} = \left[p\frac{\lambda_1}{\lambda_1 - s} + (1-p)\frac{\lambda_2}{\lambda_2 - s} \right] \frac{\mu}{\mu + s} - 1 =$$

$$= \frac{s(s^2 - l_1 s - l_0)}{(s-\lambda_1)(\lambda_2 - s)(\mu + s)} = \frac{s(s+\sigma_1)(s-\sigma_2)}{(s-\lambda_1)(\lambda_2 - s)(\mu + s)},$$

где коэффициенты квадратного трехчлена $l_0 = \mu[\lambda_1(1-p) + \lambda_2 p] - \lambda_1\lambda_2$, $l_1 = \lambda_1 + \lambda_2 - \mu$ и нули разложения зависят от параметров λ_1, λ_2, μ распределений (3). Здесь корни числителя разложения будут $-\sigma_1 = -(\sqrt{l_1^2/4 + l_0} - l_1/2)$ и $\sigma_2 = \sqrt{l_1^2/4 + l_0} + l_1/2$. Через знак "–" обозначен отрицательный корень. «Решение для среднего времени ожидания имеет вид

$$\bar{W} = 1/\sigma_1 - 1/\mu, \qquad (6)$$

где $\sigma_1 = \sqrt{l_1^2/4 + l_0} - l_1/2$» [5]. Здесь следует отметить, что согласно методу спектрального решения в выражениях для среднего времени ожидания участвуют только отрицательные корни числителя разложения, которые в самих выражениях берутся со знаком плюс.

Для определения параметров выражения (6) используем уравнения моментов до второго порядка включительно. Для распределения (3) соответственно значения среднего интервала между поступлениями требований $\bar{\tau}_\lambda$ и коэффициента вариации c_λ:

$$\bar{\tau}_\lambda = p\lambda_1^{-1} + (1-p)\lambda_2^{-1} + t_0;$$

$$c_\lambda^2 = \frac{[(1-p^2)\lambda_1^2 - 2\lambda_1\lambda_2 p(1-p) + p(2-p)\lambda_2^2]}{[t_0\lambda_1\lambda_2 + (1-p)\lambda_1 + p\lambda_2]^2}. \qquad (7)$$

Для закона обслуживания

$$\bar{\tau}_\mu = \mu^{-1} + t_0;\ c_\mu = (1 + \mu t_0)^{-1}. \qquad (8)$$

Из уравнений моментов (7) и (8) определим параметры распределений (3) [5]:

$$\lambda_1 = 2p/(\bar{\tau}_\lambda - t_0),\ \lambda_2 = 2(1-p)/(\bar{\tau}_\lambda - t_0),$$

$$p = \frac{1}{2}\left[1 - \sqrt{\frac{c_\lambda^2\bar{\tau}_\lambda^2 - (\bar{\tau}_\lambda - t_0)^2}{c_\lambda^2\bar{\tau}_\lambda^2 + (\bar{\tau}_\lambda - t_0)^2}}\right],\ \mu = 1/(\bar{\tau}_\mu - t_0). \qquad (9)$$

Теперь все готово для использования выражения (6) для среднего времени ожидания при заданных значениях числовых характеристик распределений (3) при варьировании величины параметра сдвига $0 < t_0 < \bar{\tau}_\mu$. При этом учитываем, насколько уменьшается коэффициент вариации c_λ при операции сдвига закона распределения. Отношение c_λ при $t_0 = 0$ к значению c_λ при $0 < t_0 < \bar{\tau}_\mu$ составляет $1 + t_0\frac{\lambda_1\lambda_2}{\lambda_1 - p(\lambda_1 - \lambda_2)}$, т. е. коэффициент вариации уменьшается во столько раз. Фрагмент программы расчета на Mathcad для одного варианта (рис. 1) полностью раскрывает алгоритм расчета среднего времени ожидания и средней длины очереди в системе $\bar{N}_q$.

Серия расчетов на Mathcad (табл. 1) проведена для случаев умеренной ρ = 0,55 и высокой ρ = 0,95 нагрузки при коэффициенте вариации $c_\lambda = 2$ для первой системы без сдвига ($t_0 = 0$) при единичном времени обслуживания. В таблицах среднее время ожидания и средняя длина очереди в системах с временным сдвигом обозначены $\bar{W}$ и $\bar{N}_q$, а в классической системе — $\bar{W}_{кл}$ и $\bar{N}_{q\,кл}$.

Результаты численно-аналитического моделирования убедительно демонстрируют зави-

τμ := 1 τλ := 20/19 cλ := 2 ρ := τμ/τλ = 0.95 t0 := 0.99

p := 1/2 − √([cλ²·τλ² − (τλ − t0)²] / 4·[cλ²·τλ² + (τλ − t0)²]) = 0.00044234 μ := 1/(τμ − t0) = 100

λ1 := 2·p/(τλ − t0) = 0.014125 λ2 := 2·(1 − p)/(τλ − t0) = 31.91864811 cμ := 1/(1 + μ·t0) = 0.01

K := 1 + t0·λ1·λ2/[λ1·(1 − p) + λ2·p] = 16.80672269 cλ := cλ/K = 0.119

C1 := μ·[(1 − p)λ1 + p·λ2] − λ1·λ2 = 2.37289984 C2 := λ1 + λ2 − μ = −68.06722689

S1 := √((C2²/4) + C1) − C2/2 = 68.10207018 W := 1/S1 − 1/μ = 4.684 × 10⁻³

Nq := W/τλ = 4.45 × 10⁻³

■ ***Рис. 1.*** Результаты расчета на Mathcad для одного варианта для первой системы

■ ***Fig. 1.*** Calculation results on Mathcad for one option for the first system

■ ***Таблица 1.*** Результаты вычислительных экспериментов для первой СМО

■ ***Table 1.*** Results of computational experiments for the first QS

Входные параметры				Выходные результаты			
ρ	c_λ	c_μ	t_0	$\bar{W}$	$\bar{N}_q$	$\bar{W}_{кл}$	$\bar{N}_{q\,кл}$
0,55	1,989	0,990	0,01	2,68	1,47	2,72	1,50
	1,890	0,900	0,1	2,33	1,21		
	1,450	0,500	0,5	0,80	0,35		
	1,010	0,100	0,9	0,03	0,01		
	0,911	0,010	0,99	0,00	0,00		
0,95	1,981	0,990	0,01	47,23	44,44	47,46	45,08
	1,810	0,900	0,1	45,21	39,23		
	1,050	0,500	0,5	36,54	23,54		
	0,290	0,100	0,9	13,35	6,84		
	0,119	0,010	0,99	0,005	0,002		

симость основных характеристик СМО от величины параметра сдвига законов распределений. При этом наблюдаем непрерывность численно-аналитической модели: при убывании параметра сдвига значения характеристик системы с операционным сдвигом стремятся к их значениям для обычной системы без сдвига.

Численно-аналитическое решение задачи для второй СМО

Теперь рассмотрим СМО, сформированную функциями плотности (4) с изображениями Лапласа

$$A^*(s)=\left[p\left(\frac{\lambda_1}{\lambda_1+s}\right)^2+(1-p)\left(\frac{\lambda_2}{\lambda_2+s}\right)^2\right]e^{-t_0 s};$$

$$B^*(s)=\left(\frac{\mu}{\mu+s}\right)^2 e^{-t_0 s}.$$

Спектральное решение

$$\frac{\alpha(s)}{\beta(s)}=\left[p\left(\frac{\lambda_1}{\lambda_1-s}\right)^2+(1-p)\left(\frac{\lambda_2}{\lambda_2-s}\right)^2\right]\times$$

$$\times e^{t_0 s}\left(\frac{\mu}{\mu+s}\right)^2 e^{-t_0 s}-1=$$

$$=\left[p\left(\frac{\lambda_1}{\lambda_1-s}\right)^2+(1-p)\left(\frac{\lambda_2}{\lambda_2-s}\right)^2\right]\left(\frac{\mu}{\mu+s}\right)^2-1=$$

$$=\frac{-s(s+s_1)(s+s_2)(s-s_3)(s-s_4)(s-s_5)}{(\lambda_1-s)^2(\lambda_2-s)^2(\mu+s)^2}$$

с полным выводом формулы для среднего времени ожидания для этой системы приведено в работе [6]:

$$\bar{W}=\frac{1}{s_1}+\frac{1}{s_2}-\frac{2}{\mu}, \qquad (10)$$

«где s_1, s_2 — абсолютные значения отрицательных корней $-s_1$, $-s_2$ многочлена пятой степени $s^5-c_4s^4-c_3s^3-c_2s^2-c_1s-c_0$ с коэффициентами $c_0=-2\lambda_1\lambda_2\mu(\lambda_1\lambda_2-\mu\lambda_1-p\mu\lambda_2+p\mu\lambda_1)$, $c_1=-\mu^2(\lambda_1^2-p\lambda_1^2+p\lambda_2^2)-\lambda_1\lambda_2(\lambda_1\lambda_2-4\mu\lambda_1-4\mu\lambda_2+4\mu^2)$, $c_2=-2\mu(\lambda_1^2+4\lambda_1\lambda_2+\lambda_2^2)+2\mu^2(\lambda_1+\lambda_2)+2\lambda_1\lambda_2\times(\lambda_1+\lambda_2)$, $c_3=-(\lambda_1^2+4\lambda_1\lambda_2+\lambda_2^2)-\mu(\mu-4\lambda_1-4\lambda_2)$, $c_4=2(\lambda_1+\lambda_2-\mu)$» [6].

Для использования (10) определим параметры распределений (4) из уравнений моментов

$$\bar{\tau}_\lambda=2p\lambda_1^{-1}+2(1-p)\lambda_2^{-1}+t_0,$$

$$c_\lambda^2=\frac{2[\lambda_1^2+p(\lambda_1-\lambda_2)(\lambda_1-3\lambda_2)-2p^2(\lambda_1-\lambda_2)^2]}{\{2[\lambda_1-p(\lambda_1-\lambda_2)]+t_0\lambda_1\lambda_2\}^2},$$

$$\bar{\tau}_\mu=2/\mu+t_0,\ \ c_\mu=\sqrt{2}/(2+\mu t_0).$$

Для этого получены следующие результаты:

$$\lambda_1=4p/(\bar{\tau}_\lambda-t_0),\ \ \lambda_2=4(1-p)/(\bar{\tau}_\lambda-t_0),$$

$$\mu=2/(\bar{\tau}_\mu-t_0),\ \ p=\frac{1}{2}\pm\sqrt{\frac{1}{4}-\frac{3(\bar{\tau}_\lambda-t_0)^2}{8[(\bar{\tau}_\lambda-t_0)^2+c_\lambda^2\bar{\tau}_\lambda^2]}}$$

при $0<t_0<\bar{\tau}_\mu$ [6].

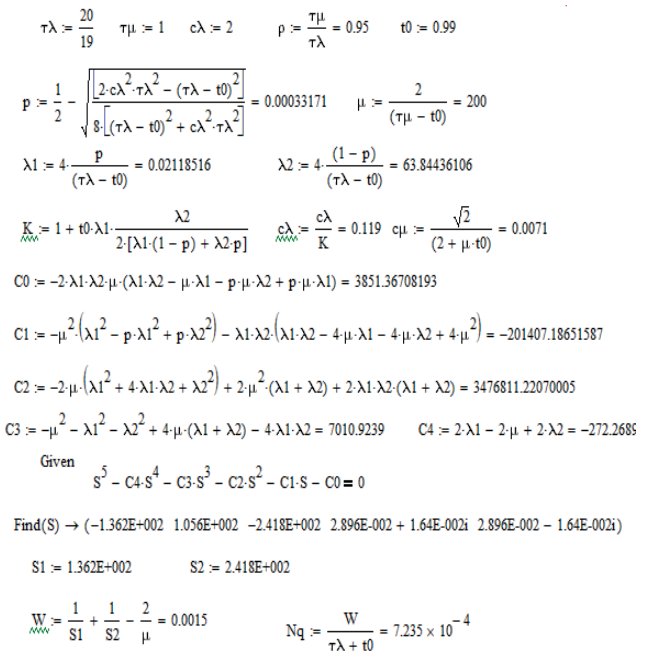
Отношение c_λ при $t_0=0$ к значению c_λ при $0<t_0<\bar{\tau}_\mu$ в этом случае составляет

$$1+t_0\frac{\lambda_1\lambda_2}{2[\lambda_1-p(\lambda_1-\lambda_2)]},$$

т. е. коэффициент вариации уменьшается во столько раз. Фрагмент программы расчета на Mathcad для одного варианта показан на рис. 2.

Результаты серии расчетов на Mathcad приведены в табл. 2 для случаев умеренной ρ = 0,55 и высокой ρ = 0,95 нагрузки при коэффициенте вариации $c_\lambda = 2$ для второй системы при единичном времени обслуживания.

Результаты вычислительных экспериментов (см. табл. 1 и 2) полностью доказывают наши предположения относительно систем со сдвинутыми законами распределений. Основные характеристики рассматриваемых систем явно зависят от величины параметра сдвига, тем самым признана возможность их контролирования. Результаты также подтверждают выполнение свойства непрерывности рассматриваемых си-



■ ***Рис. 2.*** Результаты расчета на Mathcad для одного варианта для второй системы

■ ***Fig. 2.*** Calculation results on Mathcad for one option for the second system

■ ***Таблица 2.*** Результаты вычислительных экспериментов для второй СМО

■ ***Table 2.*** Results of computational experiments for the second QS

Входные параметры				Выходные результаты			
ρ	c_λ	c_μ	t_0	$\bar{W}$	$\bar{N}_q$	$\bar{W}_{кл}$	$\bar{N}_{q\,кл}$
0,55	1,989	0,700	0,01	2,04	1,12	2,08	1,14
	1,890	0,636	0,1	1,73	0,90		
	1,450	0,354	0,5	0,45	0,20		
	1,010	0,071	0,9	0,01	0,00		
	0,911	0,007	0,99	0,00	0,00		
0,95	1,981	0,700	0,01	42,68	40,16	42,80	40,66
	1,810	0,636	0,1	41,53	36,03		
	1,050	0,354	0,5	36,54	23,54		
	0,290	0,071	0,9	14,88	7,62		
	0,119	0,007	0,99	0,002	0,001		

стем с запаздыванием: при уменьшении величины параметра t_0 основные характеристики приближаются к их соответствующим характеристикам для классических систем. Этого и стоило ожидать, так как при $t_0 = 0$ распределения (3) и (4) будут описывать классические СМО.

Имитационное моделирование в GPSS World

Далее используем апробированные [8] имитационные модели рассматриваемых систем. В работе [8] представлены коды программ на языке GPSS World с использованием логических переключателей для фаз законов распределений и соответствующих генераторов случайных величин. «При этом распределение Эрланга рассматривается как частный случай гамма-распределения. Генераторы составных распределений включают программы генерации взвешенных экспоненциальных и эрланговских распределений. В этих генераторах предусмотрен сдвиг закона распределения вправо на соответствующую величину» [8]. Ввиду трудоемкости имитационных экспериментов ограничимся одним вариантом для каждой системы.

Пояснения по входным параметрам для первой имитационной модели. Задаем параметр сдвига $t_0 = 0{,}01$ и средние значения интервалов поступлений и обслуживания $\bar{\tau}_\lambda = 20/19$, $\bar{\tau}_\mu = 1$, тогда загрузка $\rho = \bar{\tau}_\mu / \bar{\tau}_\mu = 0{,}95$. Из равенств (9) определим параметры распределений (3):

$$\lambda_1 = 2p/(\bar{\tau}_\lambda - t_0) = 0{,}212,$$

$$\lambda_2 = 2(1-p)/(\bar{\tau}_\lambda - t_0) = 1{,}706,$$

$$p = \frac{1}{2}\left[1 - \sqrt{\frac{c_\lambda^2\bar{\tau}_\lambda^2 - (\bar{\tau}_\lambda - t_0)^2}{c_\lambda^2\bar{\tau}_\lambda^2 + (\bar{\tau}_\lambda - t_0)^2}}\right] = 0{,}111,$$

$$\mu = 1/(\bar{\tau}_\mu - t_0) = 1{,}010.$$

Тогда средние интервалы для первой и второй фаз гиперэкспоненциального распределения $1/\lambda_1 = 4{,}707$, $1/\lambda_2 = 0{,}586$.

Вариант расчета для случая $\rho = 0{,}95$, $t_0 = 0{,}01$ представлен на рис. 3, *а*.

Пояснения по входным параметрам для второй имитационной модели. Задаем параметр сдвига $t_0 = 0{,}01$ и средние значения интервалов поступлений и обслуживания $\bar{\tau}_\lambda = 20/19$, $\bar{\tau}_\mu = 1$, тогда загрузка $\rho = \bar{\tau}_\mu / \bar{\tau}_\mu = 0{,}95$. Из равенств для найденных параметров распределений (4) установим их числовые значения:

$$\lambda_1 = 4p/(\bar{\tau}_\lambda - t_0) = 0{,}308,$$

$$\lambda_2 = 4(1-p)/(\bar{\tau}_\lambda - t_0) = 3{,}528,$$

$$\mu = 2/(\bar{\tau}_\mu - t_0) = 2{,}02,$$

$$p = \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{3(\bar{\tau}_\lambda - t_0)^2}{8[(\bar{\tau}_\lambda - t_0)^2 + c_\lambda^2\bar{\tau}_\lambda^2]}} = 0{,}08.$$

Тогда средние интервалы для первой и второй фаз гиперэрланговского распределения $1/\lambda_1 = 3{,}246$, $1/\lambda_2 = 0{,}283$.

а)
```
FACILITY ENTRIES UTIL. AVE.TIME AVAIL. OWNER PEND INTER RETRY DELAY
CHAN     1000001 0.951   1.010    1    2007930  0    0     0     56

QUEUE MAX CONT. ENTRY ENTRY(0) AVE.CONT. AVE.TIME  AVE.(-0) RETRY
QCHAN 368  57  1000057 26354    44.296    47.049    48.322    0
```

б)
```
FACILITY ENTRIES UTIL. AVE.TIME AVAIL. OWNER PEND INTER RETRY DELAY
CHAN     1000001 0.954   1.010    1    2000863  0    0     0     6

QUEUE MAX CONT. ENTRY ENTRY(0) AVE.CONT. AVE.TIME  AVE.(-0) RETRY
QCHAN 309  7   1000007 21173    40.260    42.652    43.575   0
```

■ ***Рис. 3.*** Результаты прогона имитационной модели для первой (*а*) и второй (*б*) системы

■ ***Fig. 3.*** Results of running the simulation model for the first (*а*) and second (*б*) system

Вариант расчета второй системы показан на рис. 3, *б*.

Имитационное моделирование даже в случае небольшого сдвига законов распределений подтверждает чувствительность моделей и их полное соответствие численно-аналитическому моделированию (см. табл. 1 и 2).

Заключение

Полученные результаты численно-аналитического (табл. 1 и 2) и имитационного моделирования (рис. 3) полностью подтверждают выдвинутые выше предположения о системах с операционным сдвигом законов распределений. Сдвиг законов распределений приводит к функциональной зависимости их числовых характеристик и параметров и, следовательно, основных характеристик системы от параметра сдвига.

Адекватность представленных моделей систем однозначно подтверждена результатами моделирования. Параметр сдвига становится управляющим параметром для регулирования величин основных характеристик СМО. Таким образом, результаты аналитического и имитационного моделирования явно демонстрируют возможность управлять характеристиками СМО через параметр сдвига законов распределения.

Литература

1. **Kleinrock L.** *Queueing Systems*. Vol. I. Wiley, 1974. 448 p.
2. **Do T. V., Chakka R., Sztrik J.** Spectral expansion solution methodology for QBD-M processes and applications in future internet engineering. *ICCSAMA*, 2016, pp. 131–142. doi:10.1007/978-3-319-00293-4-11
3. **Ma X. A., Wang Y., Zhu X., Liu W., Lan Q., Xiao W.** Spectral method for two-dimensional ocean acoustic propagation. *Sci. Eng.*, 2021, no. 9, pp. 1–19. doi: https://doi.org/ 10.3390/jmse9080892
4. **Тарасов В. Н., Бахарева Н. Ф.** Управление характеристиками системы массового обслуживания через сдвиг законов распределений. *Информационно-управляющие системы*, 2023, № 5, с. 55–63. doi:10.31799/1684-8853-2023-5-55-63, EDN: IVEQJM
5. **Тарасов В. Н.** Расширение класса систем массового обслуживания с запаздыванием. *Автоматика и телемеханика*, 2018, № 12, с. 57–70. doi:10.31857/S000523100002857-6, EDN: YPGRWX
6. **Тарасов В. Н.** Особенности аналитического моделирования систем массового обслуживания с гиперэрланговским и эрланговским распределениями. *Информационные технологии*, 2023, т. 29, № 6, с. 284–289. doi:10.17587/it.29.284-289
7. **Tarasov V. N.** Comparison of two queuing systems with ordinary and shifted Erlang distributions. *Proc. of the IEEE Intern. Scientific-Practical Conf. "Problems of Infocommunications Science and Technology" (PIC S and T)*, 2019, pp. 899–902. doi:10.1109/PICST47496.2019.9061271
8. **Тарасов В. Н., Бахарева Н. Ф.** Имитационное моделирование систем массового обслуживания на основе составных распределений — вероятностных смесей. *T-Comm: Телекоммуникации и транспорт*, 2023, т. 17, № 3, с. 14–19. doi:10.36724/2072-8735-2023-17-3-14-19
9. **Novitzky S., Pender J., Rand R. H., Wesson E.** Limiting the oscillations in queues with delayed information through a novel type of delay announcement. *Queueing Systems*, 2020, vol. 95, pp. 281–330. doi:https://doi.org/10.1007/s11134-020-09657-9
10. **Novitzky S., Pender J., Rand R. H., Wesson E.** Nonlinear dynamics in queueing theory: Determining the size of oscillations in queues with delay. *SIAM J. Appl. Dyn. Syst.*, 2019, vol. 18, no. 1, pp. 279–311. doi:https://doi.org/10.1137/18M1170637
11. **Brannstrom N.** *A Queueing Theory Analysis of Wireless Radio Systems. Appllied to HS-DSCH*. Lulea University of Technology, 2004. 79 p.
12. **Myskja A.** An improved heuristic approximation for the GI/GI/1 queue with bursty arrivals. *Teletraffic and Datatraffic in a Period of Change (ITC-13)*, 1991, pp. 683–688.
13. **Алиев Т. И.** Аппроксимация вероятностных распределений в моделях массового обслуживания. *Научно-технический вестник информационных технологий, механики и оптики*, 2013, № 2(84), с. 88–93.
14. **Aras A. K., Chen X., Liu Y.** Many-server Gaussian limits for overloaded non-Markovian queues with customer abandonment. *Queueing Systems*, 2018, vol. 89, no. 1, pp. 81–125. https://doi.org/10.1007/s11134-018-9575-0
15. **Jennings O. B., Pender J.** Comparisons of ticket and standard queues. *Queueing Systems*, 2016, vol. 84, no. 1, pp. 145–202. https://doi.org/10.1007/s11134-016-9493-y

16. **Gromoll H. C., Terwilliger B., Zwart B.** Heavy traffic limit for a tandem queue with identical service times. *Queueing Systems*, 2018, vol. 89, no. 3, pp. 213–241. https://doi.org/10.1007/s11134-017-9560-z
17. **Legros B.** M/G/1 queue with event-dependent arrival rates. *Queueing Systems*, 2018, vol. 89, no. 3, pp. 269–301. https://doi.org/10.1007 /s11134-017-9557-7
18. **Bazhba M., Blanchet J., Rhee C. H.** Queue with heavy-tailed Weibull service times. *Queueing Systems*, 2019, vol. 93, no. 11, pp. 1–32. https://doi.org/10.1007/s11134-019-09640-z/
19. **Adan I., D'Auria B., Kella O.** Special volume on 'Recent Developments in Queueing Theory' of the third ECQT conference. *Queueing Systems*, 2019, vol. 93, pp. 1–2. https://doi.org/10.1007/s11134-019-09630-1
20. **Adan I., D'Auria B., Kella O.** Special volume on 'Recent Developments in Queueing Theory' of the third ECQT conference: part 2. *Queueing Systems*, 2020, pp. 1–2. https://doi.org/10.1007/s11134-019-09637-8
21. **Tibi D.** Martingales and buffer overflow for the symmetric shortest queue model. *Queueing Systems*, 2019, vol. 93, pp. 153–190. doi:10.1007/s11134-019-09628-9
22. **Jacobovic R., Kella O.** Asymptotic independence of regenerative processes with a special dependence structure. *Queueing Systems*, 2019, vol. 93, pp. 139–152. doi:10.1007/s11134-019-09606-1
23. **Wang L., Kulkarni V.** Fluid and diffusion models for a system of taxis and customers with delayed matching. *Queueing Systems*, 2020, vol. 96, pp. 101–131. doi:10.1007/s11134-020-09659-7

UDC 621.391.1:621.395
doi:10.31799/1684-8853-2024-3-24-31
EDN: QEGHLU

Controlling the characteristics of a queueing system through shifting distribution laws in the form of probabilistic mixtures

V. N. Tarasov[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-9318-0797, v.tarasov@psuti.ru
N. F. Bakhareva[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-9850-7752
[a]Povolzhskiy State University of Telecommunications and Informatics, 23, L'va Tolstogo St., 443010, Samara, Russian Federation

Introduction: The need to minimize waiting time in queues and the volume of data storage buffers in promising data transmission systems remains relevant and requires constant improvement. **Purpose:** To expand the class of queuing systems as systems with distribution laws subjected to a shift operation in the form of probabilistic mixtures to solve the problem posed. **Methods:** We use the method of spectral solution of the Lindley integral equation based on the Laplace transform theory. **Results:** We develop numerical-analytical and simulation models for two different systems with hyper-exponential and hyper-Erlang input distributions. We can identify that shifting the distribution laws to the right reduces the coefficients of variation, and they make the main contribution to the formation of the average waiting time for requests in the queue. Then, in systems with shifted distributions, there will be a manyfold decrease in waiting time depending on the value of the shift parameter. Considering the functional dependence of the main criteria of system efficiency on the average waiting time according to Little's formulas, we are convinced of the possibility of their regulation using the time shift parameter. This will make it possible to control the main characteristics of real data systems, which is important for the theory and practice of designing such systems. **Practical relevance:** The results obtained are of great interest for the theory and practice of data transmission and make it possible to regulate the basic parameters of data transmission systems. **Discussion:** For the development of the conducted research, it is important to implement the results of the proposed approach into the theory and practice of data transmission. To do this, it is necessary to obtain the results of operation of the experimental hardware and software complex which can confirm the data of numerical analytical and simulation models.

Keywords — systems with shifted distributions, Laplace transform, Lindley integral equation, spectral solution, discrete-event modeling, GPSS World.

For citation: Tarasov V. N., Bakhareva N. F. Controlling the characteristics of a queueing system through shifting distribution laws in the form of probabilistic mixtures. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 3, pp. 24–31 (In Russian). doi:10.31799/1684-8853-2024-3-24-31, EDN: QEGHLU

Reference

1. Kleinrock L. *Queueing Systems*. Vol. I. Wiley, 1974. 448 p.
2. Do T. V., Chakka R., Sztrik J. Spectral expansion solution methodology for QBD-M processes and applications in future internet engineering. *ICCSAMA*, 2016, pp. 131–142. doi:10.1007/978-3-319-00293-4-11
3. Ma X. A., Wang Y., Zhu X., Liu W., Lan Q., Xiao W. Spectral method for two-dimensional ocean acoustic propagation. *Sci. Eng.*, 2021, no. 9, pp. 1–19. doi:https://doi.org/ 10.3390/jmse9080892
4. Tarasov V. N., Bakhareva N. F. Controlling queuing system characteristics through shifting distribution laws. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 5, pp. 55–63 (In Russian). doi:10.31799/1684-8853-2023-5-55-63, EDN: IVEQJM
5. Tarasov V. N. Extension of the class of queueing systems with delay. *Automation and Remote Control*, 2018, vol. 79, no. 12, pp. 2147–2158. doi:10.1134/S0005117918120056
6. Tarasov V. N. Features of analytical modeling of QS with hyper-Erlang and Erlang distributions. *Information Technology*, 2023, vol. 29, no. 6, pp. 284–289 (In Russian). doi:10.17587/it.29.284-289
7. Tarasov V. Comparison of two queuing systems with ordinary and shifted Erlang distributions. *Proc. of the IEEE Intern. Scientific-Practical Conf. "Problems of I nfocommunications Science and Technology"* (*PIC S and T)*, 2019, pp. 899–902. doi:10.1109/PICST47496.2019.9061271
8. Tarasov V. N., Bakhareva N. F. Simulation modeling of queuing systems based on composite distributions — proba-

bilistic mixtures. *T-Comm*, 2023, vol. 17, no. 3, pp. 14–19 (In Russian). doi:10.36724/2072-8735-2023-17-3-14-19
9. Novitzky S., Pender J., Rand R. H., Wesson E. Limiting the oscillations in queues with delayed information through a novel type of delay announcement. *Queueing Systems*, 2020, vol. 95, pp. 281–330. doi:https://doi.org/10.1007/s11134-020-09657-9
10. Novitzky S., Pender J., Rand R. H., Wesson E. Nonlinear dynamics in queueing theory: Determining the size of oscillations in queues with delay. *SIAM J. Appl. Dyn. Syst.*, 2019, vol. 18, no. 1, pp. 279–311. doi:https://doi.org/10.1137/18M1170637
11. Brannstrom N. *A Queueing Theory Analysis of Wireless Radio Systems. Appllied to HS-DSCH*. Lulea University of Technology, 2004. 79 p.
12. Myskja A. An improved heuristic approximation for the GI/GI/1 queue with bursty arrivals. *Teletraffic and Datatraffic in a Period of Change (ITC-13)*, 1991, pp. 683–688.
13. Aliev T. I. Approximation of probability distributions in queuing models. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, vol. 84, no. 2, pp. 88–93 (In Russian).
14. Aras A. K., Chen X., Liu Y. Many-server Gaussian limits for overloaded non-Markovian queues with customer abandonment. *Queueing Systems*, 2018, vol. 89, no. 1, pp. 81–125. https://doi.org/10.1007/s11134-018-9575-0
15. Jennings O. B., Pender J. Comparisons of ticket and standard queues. *Queueing Systems*, 2016, vol. 84, no. 1, pp. 145–202. https://doi.org/10.1007/s11134-016-9493-y
16. Gromoll H. C., Terwilliger B., Zwart B. Heavy traffic limit for a tandem queue with identical service times. *Queueing Systems*, 2018, vol. 89, no. 3, pp. 213–241. https://doi.org/10.1007/s11134-017-9560-z
17. Legros B. M/G/1 queue with event-dependent arrival rates. *Queueing Systems*, 2018, vol. 89, no. 3, pp. 269–301. https://doi.org/10.1007 /s11134-017-9557-7
18. Bazhba M., Blanchet J., Rhee C. H. Queue with heavy-tailed Weibull service times. *Queueing Systems*, 2019, vol. 93, no. 11, pp. 1–32. https://doi.org/10.1007/s11134-019-09640-z/
19. Adan I., D'Auria B., Kella O**.** Special volume on 'Recent Developments in Queueing Theory' of the third ECQT conference. *Queueing Systems*, 2019, vol. 93, pp. 1–2. https://doi.org/10.1007/s11134-019-09630-1
20. Adan I., D'Auria B., Kella O. Special volume on 'Recent Developments in Queueing Theory' of the third ECQT conference: part 2. *Queueing Systems*, 2020, pp. 1–2. https://doi.org/10.1007/s11134-019-09637-8
21. Tibi D. Martingales and buffer overflow for the symmetric shortest queue model. *Queueing Systems*, 2019, vol. 93, pp. 153–190. doi:10.1007/s11134-019-09628-9
22. Jacobovic R., Kella O. Asymptotic independence of regenerative processes with a special dependence structure. *Queueing Systems*, 2019, vol. 93, pp. 139–152. doi:10.1007/s11134-019-09606-1
23. Wang L., Kulkarni V. Fluid and diffusion models for a system of taxis and customers with delayed matching. *Queueing Systems*, 2020, vol. 96, pp. 101–131. doi:10.1007/s11134-020-09659-7

УДК 004.056.55
doi:10.31799/1684-8853-2024-3-32-40
EDN: FNYMEW

Научные статьи
Articles

Распределенный протокол генерации псевдослучайных чисел на основе алгоритма проверяемой случайной функции

И. С. Величко[a], *аспирант, orcid.org/0009-0005-6662-5606*
А. В. Афанасьева[a], *старший преподаватель, orcid.org/0000-0003-3001-0990*
С. В. Беззатеев[a], *доктор техн. наук, профессор, orcid.org/0000-0002-0924-6221, bsv@vu.spb.ru*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *одним из решений, применяемых для генерации случайных чисел в области безопасности смарт-контрактов, является «проверяемая случайная функция». Сегодняшние централизованные решения, основанные на этом алгоритме, не предоставляют прозрачности участникам-клиентам системы генерации, что вызывает беспокойство по поводу безопасности.* ***Цель:*** *разработать протокол работы системы на основе проверяемой псевдослучайной функции для децентрализованной блокчейн-системы с высоким уровнем защиты данных от фальсификации.* ***Результаты:*** *для решения проблемы подделки начального входного значения предложен протокол, основанный на замене классической централизованной системы на основе единичного оракула на децентрализованную. Для обеспечения безопасности функционирования разработана система формирования общего распределенного секретного ключа, а также методы генерации псевдослучайных значений на основе полученного секрета. Данный протокол реализован с использованием алгоритма обмена ключами без участия дилера. Работа протокола описана в контексте абстрактной Ethereum-подобной блокчейн-модели с применением узлов, функционирующих в рамках консенсуса «доказательство активности», в целях повышения доступности и удобства рядовых пользователей.* ***Практическая значимость:*** *разработанный протокол предоставляет эффективное решение для защиты системы генерации псевдослучайных чисел от подделки входного значения, формируемого смарт-контрактом. Благодаря введению системы разделения секретов без дилера и возможности цикличности раундов регистрации участников повышаются безопасность, гибкость и масштабируемость системы.*

Ключевые слова *— проверяемая случайная функция, блокчейн, смарт-контракты, распределенные системы, электронная подпись, схема Шнорра, разделение секрета, алгоритмы генерации случайных (псевдослучайных) чисел.*

Для цитирования: Величко И. С., Афанасьева А. В., Беззатеев С. В. Распределенный протокол генерации псевдослучайных чисел на основе алгоритма проверяемой случайной функции. *Информационно-управляющие системы*, 2024, № 3, с. 32–40. doi:10.31799/1684-8853-2024-3-32-40, EDN: FNYMEW
For citation: Velichko I. S., Afanasieva A. V., Bezzateev S. V. Distributed pseudorandom generation protocol based on verifiable random function algorithm. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 3, pp. 32–40 (In Russian). doi:10.31799/1684-8853-2024-3-32-40, EDN: FNYMEW

Введение

Проблема безопасной генерации случайных чисел в области технологий распределенного учета является серьезным вызовом для разработчиков смарт-контрактов и вопросом доверия для пользователей. В настоящее время существует достаточное количество технологических решений [1, 2], которые в некоторой степени повышают уровень безопасности, создавая алгоритмы, усиленные открытым ключом или криптографией с задержкой по времени. Одним из представителей таких алгоритмов является «проверяемая случайная функция» (Verifiable Random Function, VRF) [3, 4]. VRF — криптографический алгоритм, который позволяет безопасно генерировать случайные числа с возможностью их верификации с использованием открытого ключа. В данной статье представлены стандартный алгоритм VRF, рассмотрены его плюсы и минусы, а также предложена усовершенствованная концепция системы генерации псевдослучайных чисел.

Классический протокол VRF

Verifiable Random Function позволяет создавать псевдослучайные числа, вовлекая стороннего участника вне блокчейна в процесс генерации [5]. Этот участник является обладателем секретного ключа, необходимого для создания псевдослучайного числа. Чтобы предотвратить манипуляции результатом со стороны участника вне цепи, в алгоритм передается некоторое псевдослучайное значение, предоставленное пользователем протокола. Это означает, что ответ (результат) любого участника вне цепи можно проверить на правдоподобие (т. е. на то, что алгоритм генерации был выполнен согласно общеизвестной схеме).

Терминология для дальнейшего описания проверяемой случайной функции:

B — генератор группы эллиптической кривой [6];

PK — открытый ключ VRF;

SK — секретный ключ VRF;

$Gamma$ — псевдослучайная точка;

$seed$ — псевдослучайное входное значение алгоритма;

q — порядок группы эллиптической кривой;

c — доказательство алгоритма;

s — подпись доказательства.

Работу протокола можно представить в виде схемы, куда входят три сущности.

— Потребитель — клиентский контракт. Расположен в сети блокчейна EVM (Ethereum Virtual Machine — виртуальная машина, позволяющая выполнять код смарт-контрактов) (например, Ethereum [7, 8]). В запросах на случайной генерации он указывает технические параметры, такие как открытый ключ внешнего сервиса и количество заказанных чисел.

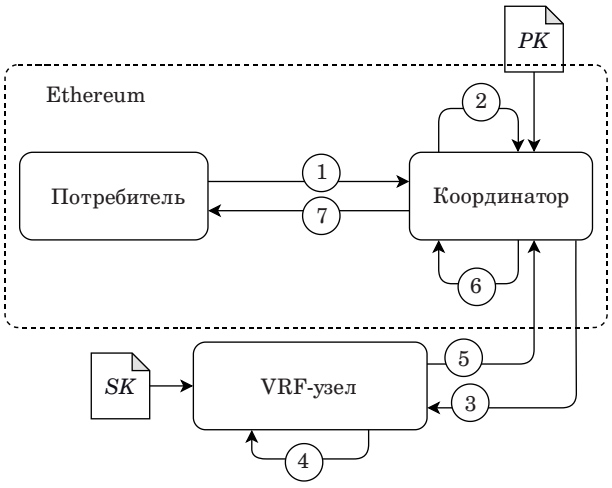
— Координатор — основной контракт. Координирует запросы к внешнему сервису и проверяет правильность результатов. Расположен в сети блокчейна EVM.

— Внешний сервис VRF — узел вне сети. Реализует генератор алгоритма VRF. Хранит секретный ключ SK на своей стороне.

Можно выделить семь основных шагов для описания полного цикла создания псевдослучайного значения. Схема протокола показана на рис. 1.

1. Запрос случайности. Вызов контракта координатора с параметрами PK и количеством запрошенных чисел.

2. Регистрация запроса в контракте координатора. Создание псевдослучайного входного значения $seed$ и регистрация запроса.



■ ***Рис. 1.*** Упрощенная схема VRF-протокола

■ ***Fig. 1.*** Simplified scheme of the VRF protocol

3. Запрос внешнего сервиса. Фактически внешний узел считывает информацию из координатора.

4. Генерация псевдослучайности. Генерация псевдослучайного значения и его доказательства с участием SK и $seed$. Результат алгоритма — это доказательство.

5. Возврат доказательства на контракт.

6. Проверка псевдослучайности.

7. Возврат результата в виде псевдослучайного числа.

Работа VRF представляет три основных шага.

1. Генерация $seed$. Операция создания псевдослучайного входного значения. Формирование значения происходит согласно определению

$$seed = hash(preSeed + blockHash),$$

где $preSeed$ — общедоступные хеш-значения пользователя, хранящиеся на контракте координатора; $blockHash$ — хеш выпущенного блока (блока, внутри которого хранится информация о запросе в службу VRF); $hash$ — операция хеширования конкатенированных значений.

2. Генерация $Gamma$. Операция создания псевдослучайного значения и его доказательств. Параметры алгоритма: входные — $seed$, SK; выходные — $Gamma$, c, s.

Опишем подробно алгоритм генерации псевдослучайности.

Функция $rand$ получает случайное число через специальное программное обеспечение, которое считывает шум с драйверов и других устройств:

$$nonce = rand(0...n);$$
$$sm \equiv nonce \bmod q.$$

Также подготавливаются ключи и псевдослучайный хеш для основного алгоритма:

$$sk \equiv SK \bmod q;$$
$$PK \equiv sk \cdot B.$$

Следующие формулы определены в рамках эллиптических кривых над конечным полем.

$$H = hashAndConvertToPnt(PK, seed), \qquad (1)$$

где $hashAndConvertToPnt$ — функция последовательного конкатенирования и создания хеш-значений переданных аргументов с последующей конвертацией в точку на кривой.

Псевдослучайное значение (псевдослучайная гамма-точка) формируется из секретного ключа и псевдослучайного хеша:

$$Gamma = sk \cdot H. \qquad (2)$$

Для контроля над *Gamma* и *PK* в процессе доказательства создаются вспомогательные переменные *U* и *V*:

$$U = sm \cdot B; \quad (3)$$

$$V = sm \cdot H. \quad (4)$$

Окончательное доказательство генерируется по следующему алгоритму:

$$c = concatAndHash\left(H, PK, Gamma, U, V\right), \quad (5)$$

где *concatAndHash* — функция последовательного конкатенирования и создания хеш-значений переданных аргументов. Вычисление функции выполняется следующим образом: для каждой точки берутся значения *x* и *y* в виде последовательностей байтов, данные последовательности объединяются. Все аргументы функции по очереди объединяются, после чего хеш вычисляется с помощью хеш-функции (в текущей версии обычно используется keccak256). Завершением работы алгоритма является создание подписи:

$$s \equiv \left(nonce + c \cdot sk\right) \bmod q. \quad (6)$$

3. Валидация *Gamma*, или проверка псевдослучайности. Параметры алгоритма: входные — *Gamma*, *c*, *s*; выходные — *true/false*.

Первым этапом проверки является проверка всех входных параметров на принадлежность к эллиптической кривой. Далее параметр *H* вычисляется таким же образом, как и в алгоритме генерации. Промежуточные значения *U′*, *V′* вычисляются как разность следующих произведений:

$$U' = s \cdot B - c \cdot PK =$$

$$= sm \cdot B + c \cdot sk \cdot B - c \cdot PK = U; \quad (7)$$

$$V' = s \cdot H - c \cdot Gamma =$$

$$= sm \cdot H + c \cdot sk \cdot H - c \cdot sk \cdot H = V. \quad (8)$$

Параметр *c′* вычисляется таким же образом, как и в алгоритме генерации. Проверка считается успешной, если параметры *c* и *c′* равны.

Уязвимости протокола

Несмотря на предполагаемую случайность и непредсказуемость результатов вычислений, для конечного пользователя классическая система генерации псевдослучайного числа имеет существенный недостаток, а именно централизацию вычислений и единый, явно хранимый, ключ.

Справочная информация: MEV (максимальное извлекаемое значение) — термин, используемый больше в экономической сфере, описывает способность майнера изменять последовательность выполняемых транзакций в блоке для выполнения различных видов арбитражных операций. Эта функция также имеет чисто техническое применение, а именно возможность влиять на значение хеша путем перестановки транзакций. В рамках консенсуса PoS (Proof of Stake — доказательство доли владения) влиять на значение хеша возможно за счет перестановки подписей в разделе тела блока.

Перечислим основные уязвимости.

Сговор потребителя VRF и автономного сервиса VRF. Все значения, участвующие в генерации исходных данных, являются общедоступными и предсказуемыми: идентификатор подписки, одноразовый номер и адрес пользователя, хеш блока. Единственным камнем преткновения в этом случае может быть хеш блока, но это значение априори криптографически слабо защищено от преждевременной компрометации или подделки. Проблема стоит особенно остро, учитывая использование MEV в блокчейне Ethereum. Использование mev-boost (сеть MEV-ботов) в качестве системы, основанной на доверии, создает потенциал для централизованных вычислений и взлома хеша блоков. Можно было бы сделать замечание, что выходное значение алгоритма VRF представляет собой 256-битный хеш, и в этом случае было бы довольно сложно перебирать всевозможные комбинации транзакций, чтобы сформировать правильный блочный хеш. Однако большинству пользователей VRF нужны числа меньшего размера, например, в лотерее Pancake (смарт-контракт платформы обмена криптовалют PancakeSwap, где пользователи могут приобретать билеты за основную валюту BNB для участия в ежедневном розыгрыше с целью выиграть денежный приз) используются билеты — числа от 1 000 000 до 1 999 999, что значительно увеличивает вероятность коллизий и упрощает выбор необходимых значений.

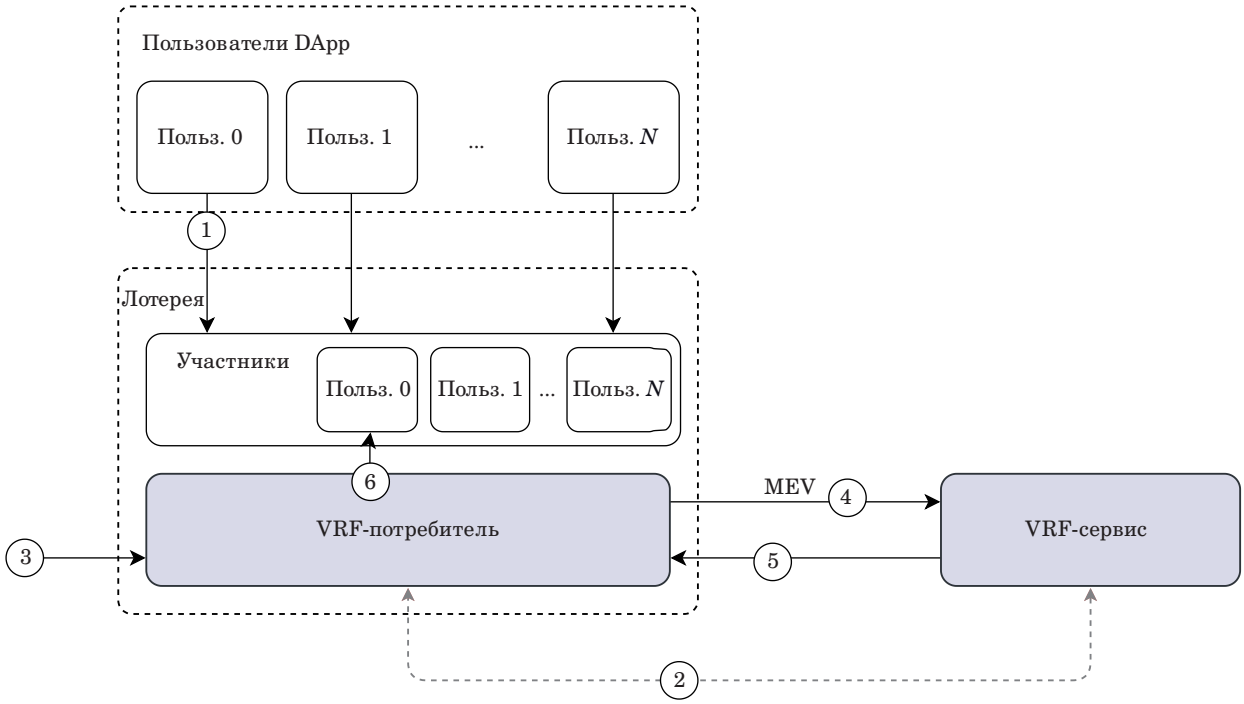
Приведем пошаговое описание схемы, показанной на рис. 2.

1. Регистрация пользователя DApp (Decentralized Application — децентрализованное приложение) или покупка пользователем лотерейного билета.

2. Сговор потребителя VRF (самой лотереи) со службой VRF по скрытому каналу связи. Потребитель должен предоставить идентификатор контракта, техническую информацию о подписке и временные характеристики (например, номер блока), в соответствии с которыми будет совершена транзакция.

3. Запуск процесса завершения лотереи.

4. Запрос на получение псевдослучайного числа. Аббревиатурой MEV обозначена возможность подделать хеш блока в момент выдачи запроса на генерацию псевдослучайного числа.

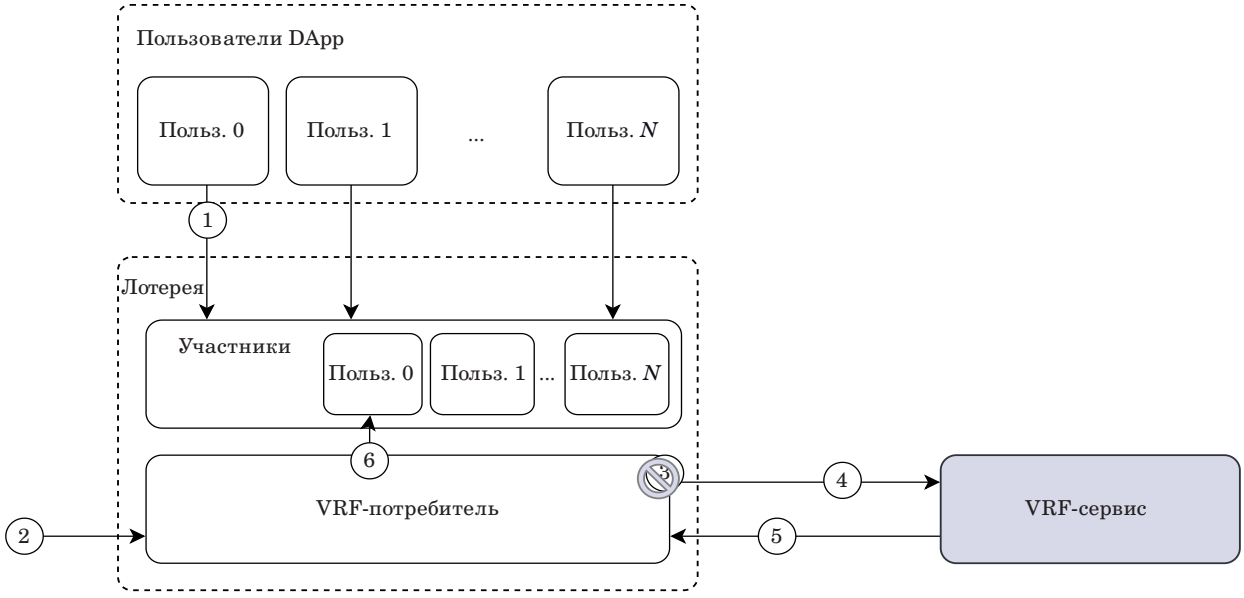


■ ***Рис. 2.*** Атака на протокол VRF через MEV (сговор VRF-потребителя и VRF-сервиса)
■ ***Fig. 2.*** Attack on the VRF protocol via MEV (collusion of the VRF of the Consumer and the VRF of the Service)

5. Возвращение псевдослучайного числа.
6. Выбор победителя.

Игнорирование транзакции. Другим возможным вектором атаки может быть игнорирование транзакции. Атака проста сама по себе: если сервис не удовлетворяет возможное число, полученное из хеша создаваемого блока, то эта транзакция просто не включается в блок и ожидает своей возможности быть обработанной в следующий раз. Символ ∅ на рис. 3 означает игнорирование транзакции.

Опишем пошагово схему, представленную на рис. 3.



■ ***Рис. 3.*** Атака на протокол VRF путем игнорирования транзакции
■ ***Fig. 3.*** Attacking the VRF protocol by ignoring the transaction

1. Регистрация пользователя/покупка лотерейного билета пользователем.

2. Начало процесса завершения лотереи.

3. Построение блока без учета выполненного вызова контракта. Игнорирование транзакции майнером.

4. Запрос псевдослучайного числа.

5. Возвращение псевдослучайного числа.

6. Выбор победителя.

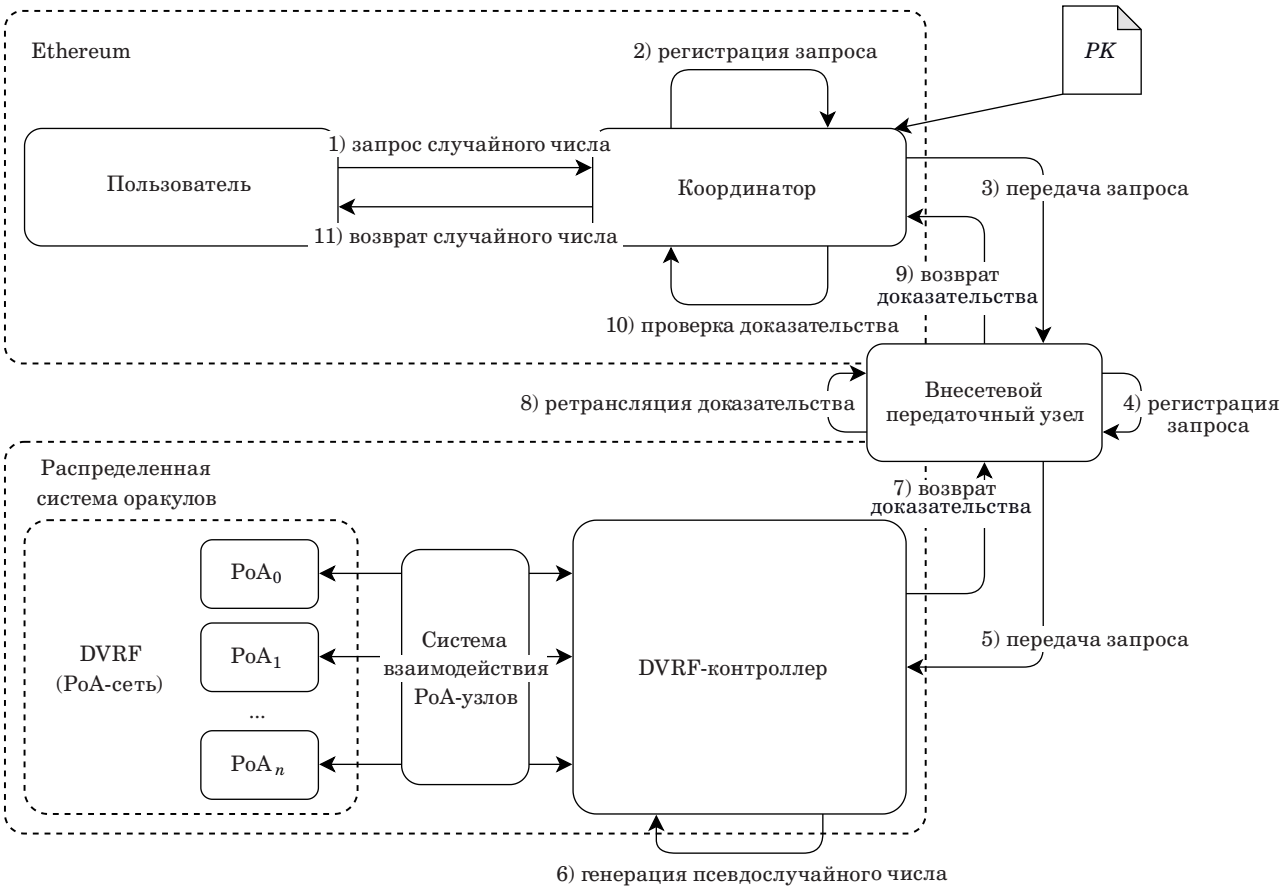
Как итог: проблема классического алгоритма заключается в том, что начальное входное значение хранится публично. Это обстоятельство предоставляет злоумышленникам возможность подделать секретное значение, поскольку доступ к начальному входному значению позволяет им воспроизвести или предсказать секретный ключ. Таким образом, отсутствие мер по защите начального входного значения существенно снижает безопасность всей системы.

Распределенный VRF-протокол

Если нет способа предотвратить подделку начального входного значения, то необходимо найти способ скрыть секрет *SK*. Изложенная выше проблема приводит к необходимости создания системы, в которой значение секретного ключа хранится не явно, а в виде отдельных проекций (точек на эллиптической кривой), совместно используемых между участниками. Мы воспользовались элементами схемы Шамира для обеспечения безопасного распределения секрета между участниками протокола [9]. В данной работе представлен вариант решения, основанный на алгоритме обмена ключами без участия дилера [10–14]. Работа протокола описана в соответствии с абстрактной Ethereum-подобной блокчейн-моделью. Поначалу предполагается использование узлов PoA (Proof of Activity) из-за большей распространенности и простоты использования обычными пользователями.

По сравнению с предыдущей версией системы (см. рис. 1) эта схема (рис. 4) вносит изменения в алгоритм генерации псевдослучайности путем создания протокола на основе готовой блокчейн-сети. Система разделена на три основных компонента:

1) алгоритм проверки псевдослучайных чисел по цепочке (предлагаемая хостинговая сеть Ethereum или другой EVM блокчейн);



■ ***Рис. 4.*** Абстрактное представление распределенного VRF-протокола (или DVRF)

■ ***Fig. 4.*** Abstract representation of the distributed VRF protocol (or DVRF)

2) встроенный алгоритм генерации псевдослучайных чисел;

3) автономный ретранслятор данных между двумя сетями.

На стороне генератора PoA-узлы участвуют в создании псевдослучайных чисел. Каждый узел имеет право «подать заявку на участие». Количество участников ограничено. На этапе регистрации каждый PoA участвует в раунде обмена проекциями секретного ключа, генерируя индивидуальные секретные ключи *SSK* и генерируя общий ключ *PK*. Принятие решения группой валидаторов PoA происходит в соответствии с заранее определенным пороговым значением в системе. Все взаимодействие узлов PoA осуществляется посредством обмена информацией по контракту с контроллером DVRF.

В качестве примера контракта с контроллером DVRF возьмем *VRFKeyCenter*, показанный на рис. 5, 6, он является представлением контракта координатора узлов PoA, расположенного во внешней сети.

Любые нарушения операций верификации (например, проверка порогового значения пользователей на рис. 5) приводят к прерыванию выполнения процессов, расположенных после условия, ниже по диаграмме.

Опишем основные функции распределенной системы генерации псевдослучайных чисел.

Регистрация свободных узлов PoA.

Для инициализации схемы необходимо не менее k участников с уникальным идентификатором, каждый из которых случайным образом формирует многочлен $f_i(x)$ над полем $GF(q)$ степени

$$deg\left(f_i(x)\right) = k-1,$$

где q — порядок группы точек эллиптической кривой. Узлы инициализируются в соответствии со схемой на рис. 5.

Распределенная генерация пары PK, SK.

1. Каждый из участников вычисляет значение своего многочлена $f_i(x)$ в $id_j = x,\ j = \{1, k\}$ и отправляет каждому участнику значение $f_i(id_j)$ по скрытому каналу связи.

2. Получив от всех k участников схемы набор значений k многочленов в точке $id_j = x$, каждый участник вычисляет значение своей проекции $sk_i = \sum_{j=1}^{k} f_j(id_i)$ секретного ключа *SK*. Результатом будет формирование $sk = \sum_{i=1}^{k} f_i(0)$, о котором ни у кого из участников протокола не будет никакой информации.

3. Для формирования *PK* каждый участник публикует свою собственную проекцию открытого ключа

$$PK_i = sk_i \cdot B,$$

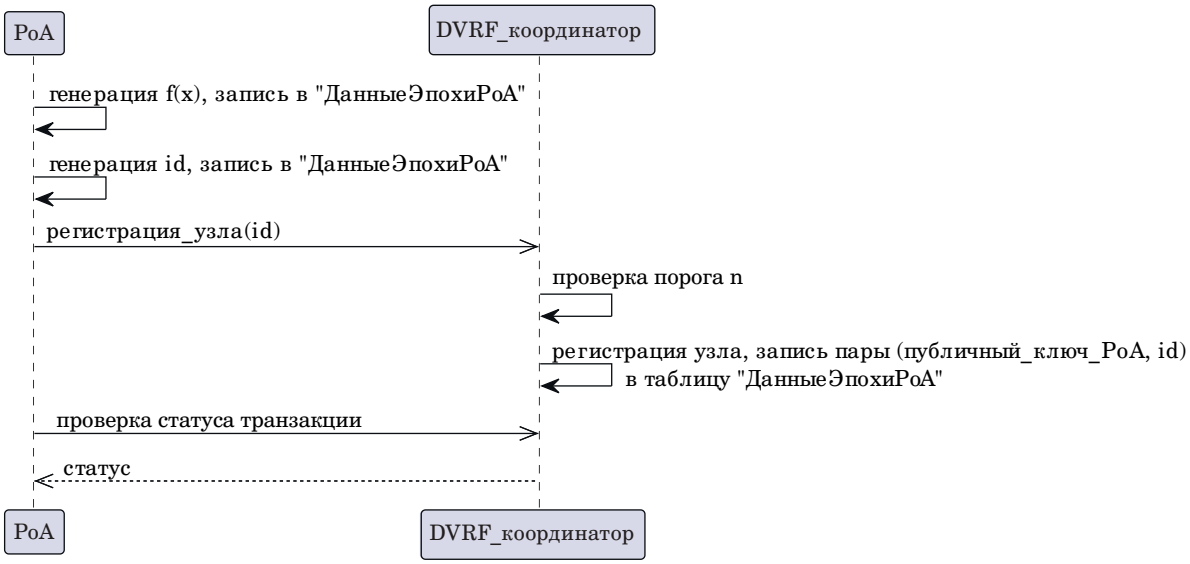
где B — генератор группы.

4. Открытый ключ собирается в соответствии с

$$PK = \sum_{i=1}^{k} \lambda_i \cdot PK_i = \sum_{i=1}^{k} \lambda_i \cdot sk_i \cdot B = sk \cdot B,$$

где λ_i — соответствующий множитель Лагранжа:

$$\lambda_i = \prod_{\substack{j=0 \\ j \neq i}}^{k} \frac{0 - id_j}{id_i - id_j}.$$



■ ***Рис. 5.*** Диаграмма регистрации PoA-узлов

■ ***Fig. 5.*** PoA node registration diagram

5. Чтобы сделать порог схемы k из n, после инициализации ключей первоначальные участники могут выдавать дополнительные проекции секрета другим участникам, вычисляя их многочлены $f_i(x)$ в новых точках id_j и отправляя по секретному каналу.

Все вышеперечисленные шаги представлены на рис. 6.

Генерация распределенного псевдослучайного числа.

Чтобы сгенерировать случайное число, каждый участник генерирует одноразовый номер и аналогично исходному алгоритму (1) параметр H:

$$nonce_i = rand(0...n);$$
$$sm_i \equiv nonce_i \bmod q.$$

Начальное значение формируется аналогично классической схеме VRF путем объединения и хеширования общедоступных значений пользователя протокола VRF:

$$Gamma_i = sk_i \cdot H;$$
$$U_i = sm_i \cdot B;$$
$$V_i = sm_i \cdot H.$$

Создание компонент U и V производится следующим образом:

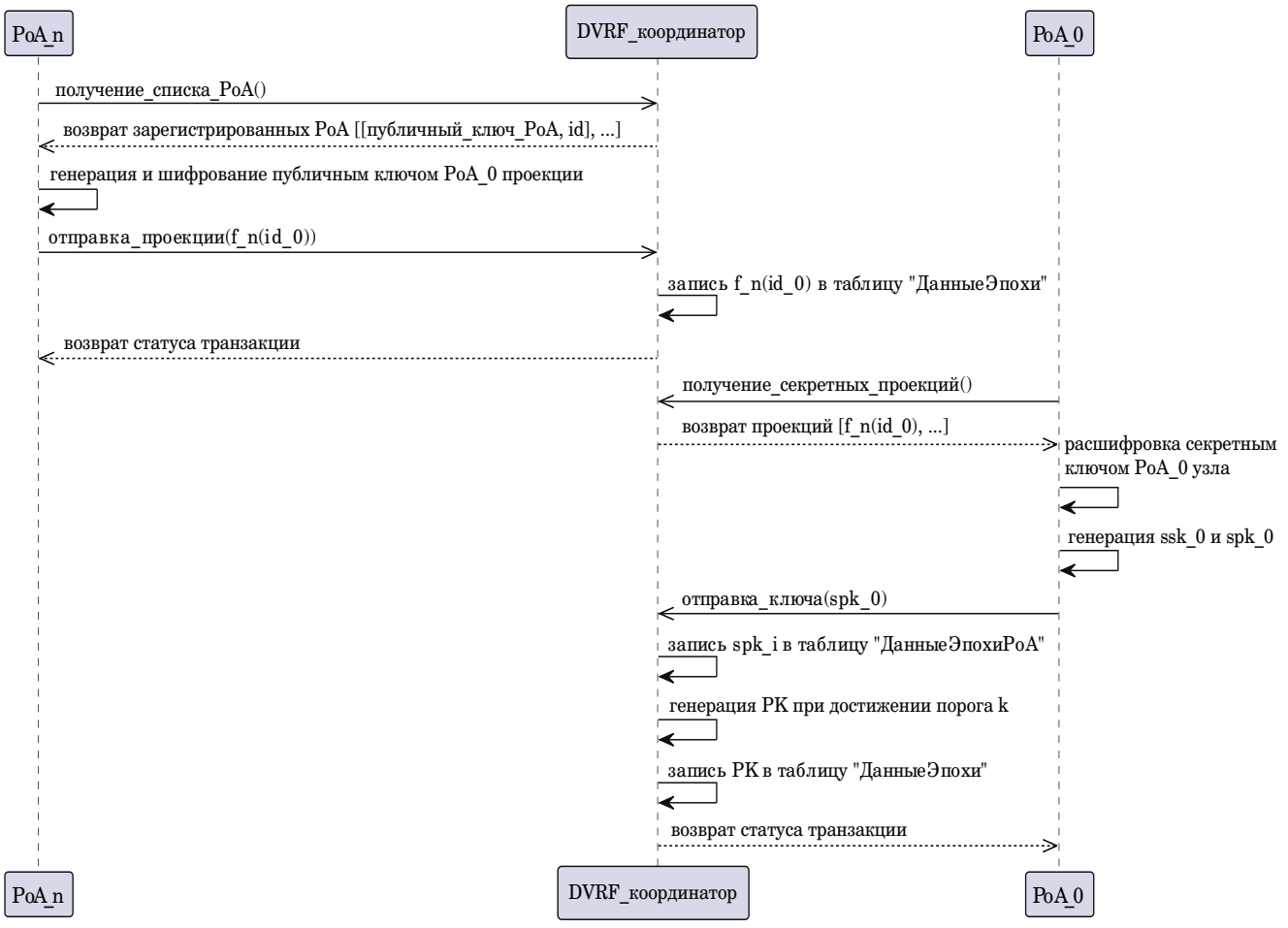
$$U = \sum_{i=1}^{k} \lambda_i \cdot U_i = \sum_{i=1}^{k} \lambda_i \cdot sm_i \cdot B = sm' \cdot B;$$
$$V = \sum_{i=1}^{k} \lambda_i \cdot V_i = \sum_{i=1}^{k} \lambda_i \cdot sm_i \cdot H = sm'H.$$

Далее выполняется формирование частичных подписей. Хеш-функция вычисляется аналогично исходной схеме по формуле (5). Проекция подписи формируется как

$$s_i \equiv \left(nonce_i + c \cdot sk_i\right) \bmod q. \quad (9)$$

Сборка подписи представлена формулой

$$s = \sum_{i=1}^{k} \lambda_i \cdot s_i = \sum_{i=1}^{k} \lambda_i \cdot sm_i + c \cdot \lambda_i \cdot sk_i =$$



■ ***Рис. 6.*** Диаграмма последовательности генерации распределенного ключа
■ ***Fig. 6.*** Diagram of the sequence of distributed key generation

$$= \sum_{i=1}^{k} \lambda_i \cdot sm_i + \sum_{i=1}^{k} c \cdot \lambda_i \cdot sk_i = sm' + c \cdot sk. \quad (10)$$

Проверка корректности приведенного псевдослучайного числа производится в соответствии с оригинальной схемой.

Заключение

По результатам работы можно сделать вывод, что на данный момент существующие решения генерации псевдослучайных чисел для блокчейн-систем имеют очевидные недостатки, связанные с вероятностью манипулирования техническими узлами самих систем. Предложенная и описанная выше система распределенных вычислений, основанная на алгоритме VRF, позволяет избежать уязвимостей классического протокола, а именно нивелировать возможность сговора с держателем секретного ключа централизованного VRF-сервиса. Хотя распределенный подход имеет собственные риски централизации при малых размерностях системы из-за сговора участников протокола, это определенно шаг вперед по сравнению с централизованным сервисом. С другой стороны, существует множество известных и зарекомендовавших себя схем, способных улучшить безопасность децентрализованных протоколов, вроде введения проверяемого разделения секрета Фельдмана или введение систем штрафов и поощрений [15–20]. Эти улучшения не рассматриваются в данной работе и должны быть обоснованы с учетом конкретных условий на практике.

Литература

1. **Boneh D., Waters B.** Constrained pseudorandom functions and their applications. *Lecture Notes in Computer Science*, 2013, vol. 7922, pp. 280–300. doi:10.1007/978-3-642-42045-0_15
2. **Micali S., Rabin M., Vadhan S.** Verifiable random functions. *Proc. 40th Int. Annual IEEE Symp. on Foundations of Computer Science*, New York, USA, 1999, pp. 120–130. doi:10.1109/SFFCS.1999.814584
3. *Verifiable Random Functions (VRFs).* https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-vrf (дата обращения: 05.03.2024).
4. **Dodis Y., Yampolskiy A.** A verifiable random function with short proofs and keys. *Proc. 8th Intern. Conf. on Theory and Practice of Public Key Cryptography*, Le Diableret, Switzerland, 2005, pp. 416–431. doi:10.1007/978-3-540-30580-4_28
5. *Pseudo-random Generators and Pseudo-random Functions: Cryptanalysis and Complexity Measures.* https://inria.hal.science/tel-01667124v1 (дата обращения: 23.05.2023).
6. *SEC 2: Recommended Elliptic Curve Domain Parameters.* https://www.secg.org/SEC2-Ver-1.0.pdf (дата обращения: 10.02.2023).
7. *Ethereum: A Secure Decentralised Generalised Transaction Ledger.* https://ethereum.github.io/yellowpaper/paper.pdf (дата обращения: 15.12.2023).
8. **David B., Gaži P., Kiayias A., Russell A.** Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. *Proc. 37th Annual Intern. Conf. on the Theory and Applications of Cryptographic Techniques*, Tel Aviv, Israel, 2018, pp. 66–98. doi:10.1007/978-3-319-78375-8_3
9. **Shamir A.** How to share a secret. *Communications of the ACM*, 1979, vol. 22, pp. 612–613. doi:10.1145/359168.359176
10. **Zhang Q., Zhihui L., Xiong L.** A verifiable secret sharing scheme without dealer in vector space. *Proc. 8th Intern. Conf. on Fuzzy Systems and Knowledge Discovery*, Shanghai, China, 2011. doi:10.1109/FSKD.2011.6019953
11. **Sun Y.** A completely fair secret sharing scheme without dealer. *Proc. 29th IEEE Intern. Conf. on Consumer Electronics-Taiwan*, Puli, Taiwan, 2016. doi:10.1109/ICCE-TW.2016.7520905
12. **Pedersen T.** A threshold cryptosystem without a trusted party. *Proc. 10th Intern. Conf. on the Theory and Application of Cryptographic Techniques*, Brighton, United Kingdom, 1991, pp. 522–526. doi:10.1007/3-540-46416-6_47
13. **Blundo C., De Santis A., Vaccaro U.** Randomness in distribution protocols. *Proc. 21th Intern. Colloquium on Automata, Languages and Programming*, Jerusalem, Israel, 1994. doi:10.1007/3-540-58201-0_99
14. **Popov S.** On a decentralized trustless pseudo-random number generation algorithm. *Journal of Mathematical Cryptology*, 2017, vol. 11, pp. 37–43. doi:10.1515/jmc-2016-0019
15. **Gennaro R., Rabin M. O., Rabin T.** Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. *Proc. 17th ACM SIGACT-SIGOPS Symp. on Principles of Distributed Computing*, Puerto Vallarta, Mexico, 1998, pp. 110–111. doi:10.1145/277697.277716
16. **Chor B., Goldwasser S., Micali S., Awerbuch B.** Verifiable secret sharing and achieving simultaneity in the presence of faults. *Proc. 26th Annual Symp. on Foundations of Computer Science*, Portland, USA, 1985, pp. 383–395. doi:10.1109/SFCS.1985.64
17. **Tomescu A., Chen R.** Towards scalable threshold cryptosystems. *Proc. 41th IEEE Symp. on Security and Privacy*, San Francisco, USA, 2020, pp. 877–893. doi:10.1109/SP40000.2020.00059
18. **Gueta G. G., Abraham I., Grossman S., Malkhi D.** SBFT: A scalable and decentralized trust infrastructure. *Proc. 49th Annual IEEE/IFIP Intern.Conf. on Dependable Systems and Networks*, Portland, USA, 2019, pp. 568–580. doi:10.1109/DSN.2019.00063

19. **Gilad Y., Hemo R., Micali C., Vlachos G., Zeldovich N.** Algorand: Scaling byzantine agreements for cryptocurrencies. *Proc. 26th Symp. on Operating Systems Principles*, Shanghai, China, 2017, pp. 51–68. doi:10.1145/3132747.3132757

20. **Papadopoulos D., Wessels D.** Can NSEC5 be practical for DNSSEC deployments? *IACR Cryptology ePrint Archive*, 2017, vol. 2017, pp. 99.

UDC 004.056.55
doi:10.31799/1684-8853-2024-3-32-40
EDN: FNYMEW

Distributed pseudorandom generation protocol based on verifiable random function algorithm

I. S. Velichko[a], Post-Graduate Student, orcid.org/0009-0005-6662-5606
A. V. Afanasieva[a], Senior Lecturer, orcid.org/0000-0003-3001-0990
S. V. Bezzateev[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-0924-6221, bsv@vu.spb.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Verifiable Random Function stands out as one of the solutions for generating random numbers within the realm of smart contract security. Current centralized solutions, relying on this algorithm, do not offer transparency to system participants, thereby raising security concerns. **Purpose:** To develop a protocol for a system based on a verifiable pseudorandom function for a decentralized blockchain system with a high level of data protection against falsification. **Results:** To address the issue of falsifying initial input values, we propose an approach that replaces the classical centralized system based on a single oracle with a decentralized one. To ensure secure operation, we have developed a system for generating a shared distributed secret key and methods for generating pseudorandom values based on the obtained secret. This method is implemented using a dealer-free key exchange algorithm. We describe the operation of the protocol in the context of an abstract Ethereum-like blockchain model, initially utilizing Proof of Activity nodes to enhance accessibility and user-friendliness. **Practical relevance:** The developed method offers an effective solution to protect the system for generating pseudorandom numbers from falsification of input values generated by smart contracts. The introduction of a secret-sharing system without a dealer and the option for cyclic rounds of participant registration enhance the security, flexibility, and scalability of the system.

Keywords — Verifiable Random Function, blockchain, smart contracts, distributed systems, electronic signature, Schnorr scheme, secret sharing, pseudorandom number generation algorithms.

For citation: Velichko I. S., Afanasieva A. V., Bezzateev S. V. Distributed pseudorandom generation protocol based on verifiable random function algorithm. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 3, pp. 32–40 (In Russian). doi:10.31799/1684-8853-2024-3-32-40, EDN: FNYMEW

References

1. Boneh D., Waters B. Constrained pseudorandom functions and their applications. *Lecture Notes in Computer Science*, 2013, vol. 7922, pp. 280–300. doi:10.1007/978-3-642-42045-0_15
2. Micali S., Rabin M., Vadhan S. Verifiable random functions. *Proc. 40th Intern. Annual IEEE Symp. on Foundations of Computer Science*, New York, USA, 1999, pp. 120–130. doi:10.1109/SFFCS.1999.814584
3. *Verifiable Random Functions (VRFs).* Available at: https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-vrf (accessed 05 March 2024).
4. Dodis Y., Yampolskiy A. A verifiable random function with short proofs and keys. *Proc. 8th Intern. Conf. on Theory and Practice of Public Key Cryptography*, Le Diableret, Switzerland, 2005, pp. 416–431. doi:10.1007/978-3-540-30580-4_28
5. *Pseudo-random Generators and Pseudo-random Functions: Cryptanalysis and Complexity Measures.* Available at: https://inria.hal.science/tel-01667124v1 (accessed 23 May 2023).
6. *SEC 2: Recommended Elliptic Curve Domain Parameters.* Available at: https://www.secg.org/SEC2-Ver-1.0.pdf (accessed 10 February 2023).
7. *Ethereum: A Secure Decentralised Generalised Transaction Ledger.* Available at: https://ethereum.github.io/yellowpaper/paper.pdf (accessed 15 December 2023).
8. David B., Gaži P., Kiayias A., Russell A. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. *Proc. 37th Annual Intern. Conf. on the Theory and Applications of Cryptographic Techniques*, Tel Aviv, Israel, 2018, pp. 66–98. doi:10.1007/978-3-319-78375-8_3
9. Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22, pp. 612–613. doi:10.1145/359168.359176
10. Zhang Q., Zhihui L., Xiong L. A verifiable secret sharing scheme without dealer in vector space. *Proc. 8th Intern. Conf. on Fuzzy Systems and Knowledge Discovery*, Shanghai, China, 2011. doi:10.1109/FSKD.2011.6019953
11. Sun Y. A completely fair secret sharing scheme without dealer. *Proc. 29th IEEE Intern. Conf. on Consumer Electronics-Taiwan*, Puli, Taiwan, 2016. doi:10.1109/ICCE-TW.2016.7520905
12. Pedersen T. A threshold cryptosystem without a trusted party. *Proc. 10th Intern. Conf. on the Theory and Application of Cryptographic Techniques*, Brighton, United Kingdom, 1991, pp. 522–526. doi:10.1007/3-540-46416-6_47
13. Blundo C., De Santis A., Vaccaro U. Randomness in distribution protocols. *Proc. 21th Intern. Colloquium on Automata, Languages and Programming*, Jerusalem, Israel, 1994. doi:10.1007/3-540-58201-0_99
14. Popov S. On a decentralized trustless pseudo-random number generation algorithm. *Journal of Mathematical Cryptology*, 2017, vol. 11, pp. 37–43. doi:10.1515/jmc-2016-0019
15. Gennaro R., Rabin M. O., Rabin T. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. *Proc. 17th ACM SIGACT-SIGOPS Symp. on Principles of Distributed Computing*, Puerto Vallarta, Mexico, 1998, pp. 110–111. doi:10.1145/277697.277716
16. Chor B., Goldwasser S., Micali S., Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults. *Proc. 26th Annual Symp. on Foundations of Computer Science*, Portland, USA, 1985, pp. 383–395. doi:10.1109/SFCS.1985.64
17. Tomescu A., Chen R. Towards scalable threshold cryptosystems. *Proc. 41th IEEE Symp. on Security and Privacy*, San Francisco, USA, 2020, pp. 877–893. doi:10.1109/SP40000.2020.00059
18. Gueta G. G., Abraham I., Grossman S., Malkhi D. SBFT: A scalable and decentralized trust infrastructure. *Proc. 49th Annual IEEE/IFIP Intern. Conf. on Dependable Systems and Networks*, Portland, USA, 2019, pp. 568–580. doi:10.1109/DSN.2019.00063
19. Gilad Y., Hemo R., Micali C., Vlachos G., Zeldovich N. Algorand: Scaling byzantine agreements for cryptocurrencies. *Proc. 26th Symp. on Operating Systems Principles*, Shanghai, China, 2017, pp. 51–68. doi:10.1145/3132747.3132757
20. Papadopoulos D., Wessels D. Can NSEC5 be practical for DNSSEC deployments? *IACR Cryptology ePrint Archive*, 2017, vol. 2017, pp. 99.

5-я Международная научно-техническая конференция «Современные сетевые технологии — MoNeTec-2024»

29–31 октября 2024 г., Москва, Россия
https://www.monetec.ru

Тематика и цель

5-я Международная научно-техническая конференция «Современные сетевые технологии» собирает представителей международного научного сообщества, исследовательских подразделений корпораций, стартапов, промышленности и бизнеса, институтов развития и органов государственной власти для обсуждения перспективных и актуальных технологий в сфере компьютерных сетей, виртуализации сетевых ресурсов и облачных вычислений, использования методов искусственного интеллекта.

Технологии передачи данных являются основой современной цивилизации. Области телекоммуникации вбирают в себя и постоянно порождают все новые и новые технологии, которые открывают новые возможности, повышают качество сервиса и безопасность в современных сетях. Технологии программного управления в сетях, виртуализации сервисов, периферийные облачные вычисления стали ключевыми элементами построения современных сетей передачи данных и информационных инфраструктур в целом. В настоящее время в мире (и в России в частности) начато их применение на практике. Однако творческая мысль не останавливается на достигнутом. Сегодня мы уже говорим о реконфигурируемых по требованию сетях (Intent Based Network), информационно-ориентированных сетях (Information Centric Network), контент-ориентированных сетях (Content Centric Network). Возникает много новых проблем и направлений для исследований.

На конференции планируются выступления с пленарными докладами ряда зарубежных и отечественных ученых по перспективным направлениям развития современных сетей передачи данных и их приложений. Программа конференции также предусматривает проведение нескольких школ по сетевым технологиям и применению отечественных решений по тематике конференции для молодых ученых, студентов старших курсов и аспирантов. Это будет способствовать расширению профессионального круга специалистов, способных поддерживать и развивать эти технологии и решения.

Направления работы MoNeTec-2024

- QoS control in data communication
- Resource management and control in cloud computing
- Edge computing
- Information security in SDN/cloud
- 5G/6G networks for wireless communication
- 6G radio access networks
- Coding theory applications in networking
- High-speed routing and switching
- Heterogeneous channel traffic modeling and analysis
- Large-scale network simulation: methods and tools
- Formal verification of network protocols and service
- AI-driven IoT sensing, interaction, and digitalization
- IIoT: Industrial Internet of Things
- Domain specific networks
- AI4net, AI for network and network for AI
- AIoT: Artificial Intelligence of Things
- Future networking

Программный комитет приветствует подачу докладов, посвященных применению методов искусственного интеллекта в указанных выше направлениях.

Организаторы конференции

- Московский государственный университет имени М. В. Ломоносова, факультет вычислительной математики и кибернетики
- Центр прикладных исследований компьютерных сетей

Программный комитет

В программный комитет входят 38 ученых из четырех стран, из них 17 состоят в IEEE. Список членов программного комитета MoNeTec-2024 доступен на официальном сайте по ссылке https://monetec.ru/committee

Организационный комитет

Список членов организационного комитета MoNeTec-2024 доступен на официальном сайте по ссылке https://monetec.ru/organizing_committee/

Контакты организационного комитета:

- e-mail: info@monetec.ru
- тел: +7 (495) 9394671

Подача докладов

Доклад должен представлять собой оригинальный, ранее не опубликованный результат. Информация о требованиях к докладам и процедуре подачи докладов размещена на сайте конференции https://www.monetec.ru

Материалы для публикации — доклады объемом до 12 страниц в формате pdf на английском языке — представляются через систему uConfy. Подробная информация о типах докладов представлена на сайте.

Для оформления статей необходимо использовать стандартный шаблон IEEE для материалов международных конференций (формат A4).

Для конференции запрошена техническая поддержка IEEE. Доклады на английском языке, успешно прошедшие отбор и представленные на конференции, будут поданы для публикации в библиотеке IEEE Xplore (индексация в Scopus).

Авторы могут подать доклад на русском языке. Такие доклады будут представлены на отдельной секции(ях) и опубликованы в сборнике трудов, индексируемом в РИНЦ.

По итогам выступлений авторам докладов может быть предложено доработать текст до полноформатной статьи, которая будет рекомендована для публикации в журналах из перечня ВАК и ядра РИНЦ.

Информация об оргвзносе для участников будет доступна на сайте конференции.

Стендовые доклады

Авторам докладов, отклоненных по итогам рецензирования, может быть предложено представить стендовый доклад. Докладчик предоставляет файл плаката; печать плаката (85×110 см) и размещение его на стенде выполняют организаторы конференции. Стендовые доклады **не** публикуются в сборнике трудов для IEEE Xplore, они будут опубликованы в сборнике, индексируемом в РИНЦ.

Школы по сетевым и облачным технологиям

Перед началом конференции планируется проведение нескольких школ по сетевым и облачным технологиям. Цель этих школ — познакомить слушателей с современными технологиями, показать их преимущества и возможности. Регистрация для участия в каждой школе будет открыта на сайте конференции. Количество мест в каждой из школ ограничено.

Важные даты

- Представление аннотаций (extended abstract) докладов: **до 1 мая 2024 г.**
- Результаты предварительного рецензирования: **до 15 мая 2024 г.**
- Представление докладов: **до 15 июня 2024 г.**
- Результаты рецензирования: **до 1 сентября 2024 г.**
- Предоставление финальной версии доклада, доработанного по результатам рецензирования: **до 20 сентября 2024 г.**
- Регистрация для участия в школе: **до 5 октября 2024 г.**
- Школы: **27–28 октября 2024 г.**
- Конференция: **29–31 октября 2024 г.**

Формат и место проведения

Формат конференции: смешанный (очный и дистанционный)

Место проведения: Московский государственный университет имени М. В. Ломоносова

Прошедшие конференции MoNeTec

Первая конференция MoNeTec-2014 (27–29 октября 2014 г.)

Место проведения: МГУ имени М. В. Ломоносова

Труды конференции: https://ieeexplore.ieee.org/xpl/conhome/8555058/proceeding

Вторая конференция MoNeTec-2018 (25–26 октября 2018 г.)
Место проведения: Сколтех (Москва)
Труды конференции: https://ieeexplore.ieee.org/xpl/conhome/8555058/proceeding

Третья конференция MoNeTec-2020 (27–29 октября 2020 г.)
Место проведения: online
Презентации и видеоконференции: https://monetec.ru/2020/reports

Труды конференции: https://ieeexplore.ieee.org/xpl/conhome/9257984/proceeding

Четвертая конференция MoNeTec-2022 (27–29 октября 2022 г.)
Место проведения: МТУСИ
Труды конференции: https://ieeexplore.ieee.org/xpl/conhome/9960711/proceeding

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.

СВЕДЕНИЯ ОБ АВТОРАХ

АФАНАСЬЕВА Александра Валентиновна

Старший преподаватель кафедры информационной безопасности Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2003 году с отличием окончила магистратуру Санкт-Петербургского государственного университета аэрокосмического приборостроения.
Является автором более 30 научных публикаций и десяти российских и международных патентов на изобретения.
Область научных интересов — криптографические алгоритмы и распределенные протоколы, доказательная безопасность и верификация криптографических протоколов.
Эл. адрес: alra@k36.org

БЕЗЗАТЕЕВ Сергей Валентинович

Заведующий кафедрой технологий защиты информации и техносферной безопасности Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1980 году окончил Ленинградский институт авиационного приборостроения по специальности «Автоматизированные системы управления».
В 2011 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 40 научных публикаций.
Область научных интересов — теория информации, теория кодирования, системы информационной безопасности.
Эл. адрес: bsv@aanet.ru

КРЫЛОВ Даниил Романович

Магистрант Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2022 году окончил бакалавриат Санкт-Петербургского государственного университета аэрокосмического приборостроения по специальности «Инфокоммуникационные технологии и системы связи».
Является автором одной научной публикации.
Область научных интересов — системы хранения данных, оптимизационные алгоритмы.
Эл. адрес: daniil12244892@mail.ru

БАХАРЕВА Надежда Федоровна

Профессор, заведующая кафедрой информатики и вычислительной техники Поволжского государственного университета телекоммуникаций и информатики, Самара.
В 1978 году окончила Оренбургский политехнический институт по специальности «Электрические машины».
В 2011 году защитила диссертацию на соискание ученой степени доктора технических наук.
Является автором более 150 научных публикаций.
Область научных интересов — вычислительные системы и сети.
Эл. адрес: n.bakhareva@psuti.ru

ВЕЛИЧКО Иван Сергеевич

Ассистент кафедры информационной безопасности Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2023 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Информационная безопасность автоматизированных систем».
Область научных интересов — криптография, методы проектирования распределенных систем, информационная безопасность.
Эл. адрес: wwr0ngn4m3@yandex.ru

ПОЙМАНОВА Екатерина Дмитриевна

Доцент кафедры инфокоммуникационных технологий и систем связи Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2005 году окончила Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича по специальности «Информационные системы в области связи».
В 2020 году защитила диссертацию на соискание ученой степени кандидата технических наук.
Является автором 64 научных публикаций.
Область научных интересов — информационные системы, системы хранения данных, базы данных.
Эл. адрес: e.d.poymanova@guap.ru

СОЛОДУХА Роман Александрович

Доцент кафедры информационных технологий, моделирования и управления Воронежского государственного университета инженерных технологий.
В 1998 году окончил Воронежскую высшую школу МВД России по специальности «Радиотехника».
В 2001 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 100 научных публикаций, 27 учебно-методических работ, десяти патентов на программы для ЭВМ.
Область научных интересов — стеганоанализ.
Эл. адрес: standartal@list.ru

ТЮРЛИКОВ Андрей Михайлович

Профессор, заведующий кафедрой инфокоммуникационных технологий и систем связи Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1980 году окончил Ленинградский институт авиационного приборостроения по специальности «Информационные системы управления».
В 2011 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 150 научных публикаций.
Область научных интересов — многоабонентные системы связи, системы дистанционного обучения, протоколы передачи данных в реальном масштабе времени, алгоритмы сжатия видеоинформации.
Эл. адрес: turlikov@guap.ru

ТАРАСОВ Вениамин Николаевич

Профессор, заведующий кафедрой управления в технических системах Поволжского государственного университета телекоммуникаций и информатики, заслуженный работник высшей школы РФ, Самара.
В 1975 году окончил Ордена Трудового Красного Знамени Уральский государственный университет им. А. М. Горького по специальности «Механика».
В 2003 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 250 научных публикаций.
Область научных интересов — вычислительные системы и сети.
Эл. адрес: v.tarasov@psuti.ru

Уважаемые авторы!

При подготовке рукописей статей необходимо руководствоваться следующими рекомендациями.

Статьи должны содержать изложение новых научных результатов. Название статьи должно быть кратким, но информативным. В названии недопустимо использование сокращений, кроме самых общепринятых (РАН, РФ, САПР и т. п.).

Текст рукописи должен быть оригинальным, а цитирование и самоцитирование корректно оформлено.

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 20 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала Word шрифтом Times New Roman размером 13, поля не менее двух сантиметров.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание (при отсутствии — должность), полное название организации, аннотация и ключевые слова на русском и английском языках, ORCID и электронный адрес одного из авторов. При написании аннотации не используйте аббревиатур и не делайте ссылок на источники в списке литературы. Предоставляйте подрисуночные подписи и названия таблиц на русском и английском языках.

Статьи авторов, не имеющих ученой степени, рекомендуется публиковать в соавторстве с научным руководителем, наличие подписи научного руководителя на рукописи обязательно; в случае самостоятельной публикации обязательно предоставляйте заверенную по месту работы рекомендацию научного руководителя с указанием его фамилии, имени, отчества, места работы, должности, ученого звания, ученой степени.

Простые **формулы** набирайте в Word, сложные с помощью редактора Mathtype или Equation. Для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта в Mathtype никогда не пользуйтесь вкладкой Other, Smaller, Larger, используйте заводские установки редактора, не подгоняйте размер символов в формулах под размер шрифта в тексте статьи, не растягивайте и не сжимайте мышью формулы, вставленные в текст; пробелы в формуле ставьте только после запятых при перечислении с помощью Ctrl+Shift+Space (пробел); не отделяйте пробелами знаки: + = – ×, а также пространство внутри скобок; для выделения греческих символов в Mathtype полужирным начертанием используйте Style → Other → bold.

Для набора формул в Word никогда не используйте вкладки: «Уравнение», «Конструктор», «Формула» (на верхней панели: «Вставка» — «Уравнение»), так как этот ресурс предназначен только для внутреннего использования в Word и не поддерживается программами, предназначенными для изготовления оригинал-макета журнала.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Подробнее см. http://i-us.ru/index.php/ius/author-guide

Иллюстрации:

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio (*.vsd, *.vsdx); Adobe Illustrator (*.ai); Coreldraw (*.cdr, версия не выше 15); Excel (*.xls); Word (*.docx); AutoCad, Matlab (экспорт в PDF, EPS, SVG, WMF, EMF); Компас (экспорт в PDF); веб-портал DRAW.IO (экспорт в PDF); Inkscape (экспорт в PDF);

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей и названий таблиц на русском и английском языках обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png, *.jpg с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40×55 мм;

— экспертное заключение;

— экспортное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц, doi;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц, doi;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта и дату обращения.

Список литературы оформляйте двумя отдельными блоками по образцам lit.dot на сайте журнала (http://i-us.ru/paperrules): Литература и References.

Более подробно правила подготовки текста с образцами изложены на нашем сайте в разделе «Руководство для авторов» – http://i-us.ru/index.php/ius/author-guide.

Контакты

Куда: 190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А, ГУАП, РИЦ
Кому: Редакция журнала «Информационно-управляющие системы»
Тел.: (812) 494-70-02
Эл. почта: ius.spb@gmail.com
Сайт: www.i-us.ru