МОДЕЛИРОВАНИЕ СИСТЕМЫ ИДЕНТИФИКАЦИИ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ НА БАЗЕ АРХИТЕКТУРЫ ЦИФРОВЫХ ОБЪЕКТОВ

М.С. Аль-Бахри[1], Р.В. Киричек[1], Д.Д. Сазонов[1*]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: dim-saz@yandex.ru

Информация о статье
УДК 004.7
Язык статьи – русский

Ссылка для цитирования: Аль-Бахри М.С., Киричек Р.В., Сазонов Д.Д. Моделирование системы идентификации устройств интернета вещей на базе архитектуры цифровых объектов // Труды учебных заведений связи. 2019. Т. 5. № 1. С. 42–47. DOI:10.31854/1813-324X-2019-5-1-42-47

Аннотация: *Проведен анализ возможности построения системы идентификации устройств интернета вещей на базе архитектуры цифровых объектов. Предложена модель системы резолюции идентификаторов цифровых объектов как системы массового обслуживания, на базе которой выполнен оптимизационный эксперимент и получена конфигурация системы резолюции, позволяющая сократить время на разрешение идентификатора устройства. Проведен анализ программного обеспечения существующей системы резолюции Handle System и предложены пути возможного улучшения алгоритмов с целью сокращения времени на разрешения идентификатора.*

Ключевые слова: *интернет вещей, архитектура цифровых объектов, идентификация цифровых объектов, Handle System, система массового обслуживания.*

Введение

В современном обществе значительную часть рынка технических систем занимает Интернет вещей. Данные устройства находят место во многих областях, начиная от простого бытового использования, медицины и заканчивая применением в военных целях. По приблизительным оценкам, количество устройств IoT (*от англ.* Internet of Things) составляет порядка 28 миллиардов и это цифра с каждым годом растет. Гигантское множество устройств интернета вещей взаимодействуют друг с другом ежедневно, что открывает широчайшие возможности по созданию приложений различного класса на базе данных «умных» систем. Очевидно, что для обеспечения корректной и быстрой работы с огромным потоком информации от таких устройств требуется наличие надежной системы адресации и идентификации, в связи с чем выделяется отдельная область задач – идентификация интернета вещей. Основной проблематикой данной области является присвоение уникальных идентификаторов и связанных с ними метаданных устройствам интернета вещей, позволяющих им обмениваться информацией с различными сущностями в сети Интернет [1–3].

В [3–6] авторами рассмотрены, а ниже обобщены основные особенности идентификации для интернета вещей, а именно: различный жизненный цикл устройств; взаимоотношение объектов интернета вещей с другими внесистемными сущностями; особые требования к контексту, в котором работают устройства; требования к обеспечению механизмов защиты; возможность расширения системы идентификации до огромного числа устройств; возможность эффективно работать для самых различных устройств; прозрачность системы адресации и независимость от сети; гибкий и эффективный механизм резолюции идентификаторов; безопасность и сохранность пользовательских данных и т. д.

На сегодняшний день существуют несколько подходов для построения системы идентификации устройств интернета вещей [7, 8]. Одним из возможных решений возникшей проблемы является использование архитектуры идентификации на базе архитектуры цифровых объектов DOA (*от англ.* Digital Object Architecture).

1. Общая концепция архитектуры цифровых объектов

Как было показано в статье [3], существующие системы управления информацией в сети основаны на классической клиент-серверной архитектуре. Сервер в такой системе представляется местом

хранения информации и обработки запросов от клиентов на работу с данной информацией. DOA, в отличие от такого подхода, стремится решить вопрос не о локализации, а о контексте цифрового объекта [1].

Цифровой объект в данной архитектуре характеризуется не только информацией о своем расположении. Помимо этого, существует возможность получать различные сведения о самом объекте: требования к доступу, аутентификации, информацию об авторе и прочее [9]. Вся эта информация вносится самим создателем цифрового объекта. Для этого в архитектуру DOA интегрирована специальная инфраструктура, обеспечивающая необходимое шифрование и верификацию доступа.

Основными структурными элементами DOA являются цифровой объект, система резолюции идентификатора (Handle System) и репозиторий и реестр цифровых объектов. Остановимся на принципах система резолюции подробнее.

Каждому цифровому объекту в описываемой архитектуре ставится в соответствие уникальный идентификатор – DOI (*от англ.* Digital Object Identificator). Данный идентификатор чем-то напоминает URL, на базе которого построен современный Интернет. Однако, в отличие от последнего, присваиваемые идентификаторы остаются постоянными и не зависят от состояния цифрового объекта. Именно система резолюции связывает идентификатор с информацией о текущем статусе цифрового объекта (местонахождение, доступ, информация об аутентичности) [10].

В классической архитектуре DOA система резолюции является двухуровневой [1, 2, 7]. Первым уровнем резолюции является глобальный реестр (GHR, *от англ.* Global Handle Registry); вторым уровнем – набор локальных реестров (LHR, *от англ.* Local Handle Registry) или локальных сервисов (LHS, *от англ.* Local Handle Service). Для разрешения идентификатора в данной подсистеме, вначале идет обращение к глобальному реестру GHR, который сообщает информацию о локальном реестре LHR, в котором содержится необходимая информация о цифровом объекте. Схематически данный процесс представлен на рисунке 1.

Сама структура идентификатора DOA также соответствует двухуровневой системе [11]. Например, рассмотрим идентификатор: 10.1000/123abc. Первая часть, расположенная до «/», носит названия префикса; вторая часть – суффикса. Префикс позволяет установить сведения о локальном реестре цифрового объекта LHR. Данное соответствие префикса и информации об администраторе хранится в глобальном реестре GHR. Суффикс же уже однозначно идентифицирует конкретный объект, и данная информация, связывающая суффикс с конкретным объектом, хранится в локальном реестре LHR.

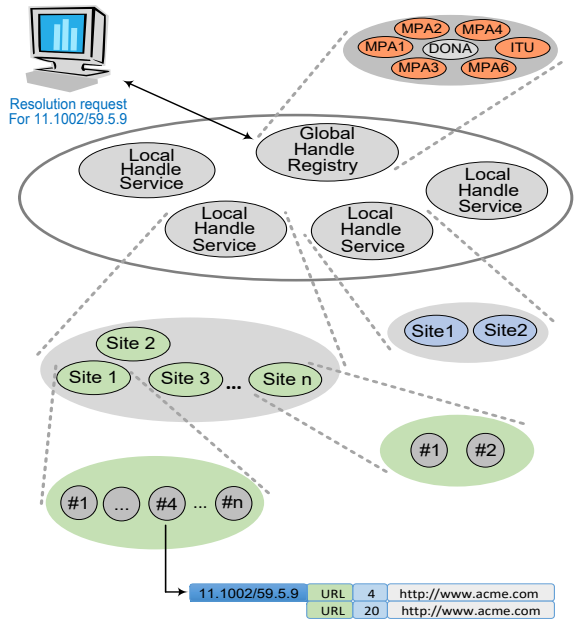


Рис. 1. Структура системы резолюции (Handle system)

2. Математическая модель системы резолюции

Как было описано выше, система резолюций состоит из двух типов реестров – GHR и LHR. Пусть группа реестров GHR определяется символом *Gj*, где *j* = 1, 2, 3...*N*, где *N* – общее число реестров GHR в системе. Каждый реестр GHR объединяет и контролирует определенный набор локальных реестров. Набор локальных реестров, подсоединенных к *j*-му GHR, обозначается символом *Lji*, где *i* = 1, 2, 3...*Mj*, где *Mj* – общее количество LHR, подсоединенных к *j*-му GHR. Переданные пакеты прибывают на сервер с определенной частотой, соответствующей Пуассоновскому процессу, формируя одиночную очередь на контроллере. Такая система может быть смоделирована на основе мульти-серверной модели массового обслуживания (M/M/s) [12].

Тогда среднее время ответа *Tj* реестра GHR *Gj* равно сумме времени в очереди и времени обработки, и может быть вычислено при помощи формулы Эрланга, как функция частоты поступления λ*i* запросов и частоты обслуживания μ:

$$T_j(\lambda) = \frac{f\left(s, \frac{\lambda_j}{\mu}\right)}{s\mu_j - \lambda_j} + \frac{1}{\mu}. \qquad (1)$$

Функция $f(s, \lambda/\mu)$ определяет вероятность того, что все серверы в системе используются, и любая из поступивших заявок попадет в очередь:

$$f\left(s, \frac{\lambda}{\mu}\right) = \frac{1}{1 + \left(\frac{1}{1-\gamma}\right)\left(\frac{s!}{(s\gamma)^s}\right)\sum_{k=0}^{s-1}\frac{(s\gamma)^k}{k!}}, \qquad (2)$$

$$\gamma = \frac{\lambda_j}{s\mu}. \qquad (3)$$

Функция γ показывает использование системы, что отражает также ее стабильность. Система ста-

бильно распределена только если показатель использования системы γ меньше единицы. Данная информация может быть корректно интерпретирована при помощи диаграммы состояний модели M/M/s. В случае, когда число заявок в очереди больше, чем на сервере контроллера, обработка будет происходить с той же частотой μ, при этом контроллер будет предельно заполнен.

Частота поступления заявок λ_j реестра GHR G_j рассчитывается как сумма средних частот поступления заявок на локальных реестрах, подсоединенных к реестру G_j:

$$\lambda_j = \sum_{L_i} \lambda_l. \quad (4)$$

Средняя нагрузка на сервер-посредник G_j рассчитывается как среднее число поступивших и обработанных запросов. При помощи формулы Эрланга рассчитывается средняя нагрузка L_j на реестрах GHR:

$$L_j(\lambda) = s\gamma + \frac{\gamma}{1-\gamma} f\left(s, \frac{\lambda_j}{\mu}\right). \quad (5)$$

3. Имитационная модель системы резолюции

Для того, чтобы охарактеризовать эффективность системы резолюции идентификаторов в архитектуре DOA при применении к задачам идентификации Интернета Вещей, рассмотрим систему резолюции как СМО (систему массового обслуживания).

В качестве системы СМО было решено взять модель M/M/n/m. Данная модель характеризует систему с экспоненциальным распределением времени обслуживания заявок и экспоненциальным распределением времени между поступлениями заявок [13]. Кроме того, модель удовлетворяет следующим важным условиям:

– наличие нескольких каналов обработки (в данной модели будем рассматривать серверы GHR как самостоятельную сущность, только лишь обрабатывающую приходящие в нее запросы);

– ограничение на длину буфера GHR отсутствует (каждый запрос, поступивший в систему, будет обслужен);

– нет приоритетности у поступающих запросов, каждый запрос обрабатывается в той последовательности, в которой поступил в систему.

Стоит заметить, что при анализе обработки трафика запросов на протяжении длительного периода времени (например, суток), выбранная модель уже не будет валидной [5]. Однако на коротких промежутках времени эту модель можно использовать. В качестве времени работы системы был выбран промежуток в 200 с.

Модель системы резолюции как СМО была построена путем анализа существующей реализации системы резолюции [1, 4, 7]. В существующей архитектуре используется не один GHR-сервер, а несколько, принадлежащих MPA (*от англ.* Multi-Primary Administrators), контролируемым DONA Foundation [1, 2, 8]. Каждый MPA-сервер представляет собой GHR, способный разрешать поступающие на него запросы. Путем анализа работы программного обеспечения, предоставляемого Handling.net [14], была установлена инфраструктура серверов глобальных регистров верхнего уровня и определена средняя задержка на разрешение запроса этими серверами. В данном программном обеспечении все MPA-серверы эквивалентны между собой и запрос на разрешение поступает последовательно на все серверы и анализируется ответ, который пришел первым. При этом не идет учет и анализ времени задержки до сервера. По сути система резолюции гарантирует, что если запрос на разрешение поступил в систему, то он обязательно будет выполнен, однако время, которое может потребоваться на это, четко не регламентировано [7, 9]. В таблице 1 представлены характеристики серверов MPA, используемых в качестве GHR в действующей архитектуре системы резолюции.

ТАБЛИЦА 1. Характеристики серверов MPA

MPA	IP-адрес	Средняя задержка на разрешение, мс
CNRI (Америка)	132.151.20.9; 38.100.138.153; 38.100.138.131; 132.151.20.9; 2001:550:100:6::138:153; 2001:550:100:6::4; 132.151.1.179	243.548
ITU (Швейцария)	156.106.193.160	71.33
Beijing Flash Newsletter Cas Telecommunication (Китай)	119.90.34.34	473.583
Alicloud (Китай)	47.90.103.77	410.693
ATI – Agence Tunisienne Internet (Тунис)	41.231.118.2	82.510
Gesellschaft Für Wissenschaftliche Datenverarbeitung Mbh Göttingen (Германия)	134.76.30.197	44.356
Communications And Information Technology Commission (Саудовская Аравия)	86.111.195.107	318.450
Liquid Telecommunications Operations Limited (Кения)	196.12.152.22	258.450

На рисунке 2 изображена основная диаграмма процесса обработки запроса системой массового обслуживания, в которой рассматривался процесс разрешения идентификатора (имитационное моделирование произведено в среде Anylogic).

Элемент clients соответствует источнику заявок на разрешение идентификаторов, поступающих от устройств. Далее идет разветвление на 8 каналов,

каждый из которых соответствует инфраструктуре определенного MPA. Вероятность выбора каждого из каналов в существующей системе одинакова. Каждый сервер MPA представляет собой набор из буфера заявок и сервера обработки идентификатора. При этом количество каналов в сервере обработки соответствует количеству серверов каждого конкретного MPA, приведенных в таблице 1. Буфер каждого из серверов MPA является гипотетически неограниченным, что обеспечивает свойство системы резолюции по гарантированному разрешению поступившего идентификатора.

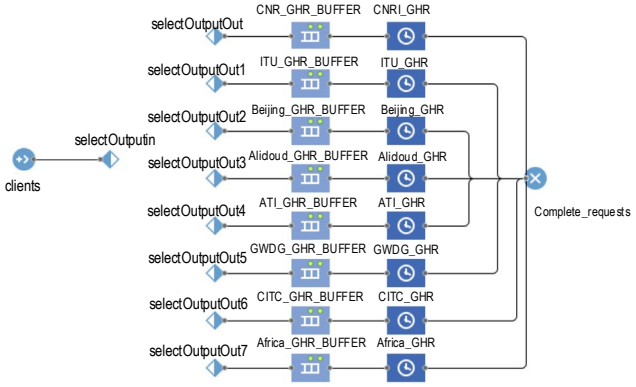


Рис. 2. Имитационная модель системы резолюции идентификатора цифровых объектов как СМО

Следует отметить, что анализ ограничивался только верхним уровнем GHR, и не анализировался следующий уровень работы системы с LHR. Взаимодействие с локальными серверами и анализ их конфигурации должен рассматриваться отдельно в рамках конкретной решаемой задачи.

4. Результаты моделирования

Так как система DOA строится на базе сетевой архитектуры, которая уже существует на данный момент для глобальной сети Интернет, то основными параметрами, влияющими на работу, будут величина сетевой задержки для поступающего запроса, скорость обработки запроса сервером, ответственным за резолюцию, и количество каналов обработки у каждого MPA.

Характеристикой системы резолюции, критичной для идентификации Интернета вещей, является среднее время обслуживания одного запроса. Данное время будет зависеть как от конфигурации системы, так и от интенсивности нагрузки.

На рисунке 3 (синяя линия) показана зависимость среднего времени разрешения идентификатора (сек.) от интенсивности поступающих запросов (Эрл.) при текущей конфигурации системы резолюции. Как видно из графика, с ростом интенсивности нагрузки увеличивается и среднее время разрешения одного идентификатора, причем при больших нагрузках это время доходит до 30 секунд, что достаточно много для реальных приложений, особенно если сравнивать с показателями системы DNS.

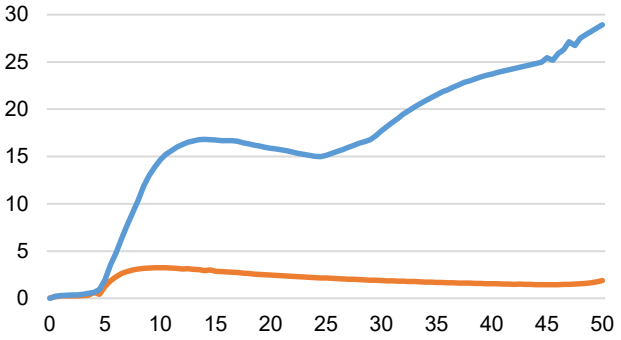


Рис. 3. Зависимость времени разрешения идентификаторов от интенсивности запросов при текущей (синяя линия) и оптимальной конфигурации (красная линия)

Используя возможности среды Anylogic, проведем оптимизационный эксперимент, направленный на установление наиболее подходящей инфраструктуры GHR-серверов при текущей конфигурации временных задержек с целью снизить среднее время разрешения идентификатора. Основным параметром для оптимизации будет количество GHR-серверов, используемым каждым из MPA. В качестве целевой функции будем стремится минимизировать время разрешения запроса. Установим время разрешения не более 1 секунды. Зададимся значением интенсивности в 50 Эрл.

Результаты оптимизационного эксперимента представлены в таблице 2, где: alfa – параметр интенсивности нагрузки; d1...d8 – количество серверов каждого из MPA.

ТАБЛИЦА 2. Результаты оптимизационного эксперимента

	Текущее	Лучшее
Итерация	500	60
Функционал	3.947	0.878
Параметры		
alfa	50	50
d1	7	7
d2	9	10
d3	4	1
d4	9	10
d5	8	10
d6	8	10
d7	10	10
d8	8	10

Процесс оптимизации заключается в последовательном запуске модели с варьированием параметров оптимизации (количества серверов GHR) для достижения установленной цели (времени разрешения идентификатора менее 1 сек.). В столбце «Текущее» представлены параметры оптимизируемой модели на текущем шаге итерации. Строка «Функционал» показывает значение оптимизационной функции на текущем шаге. В конце оптимизационного процесса мы получаем набор параметров (количество серверов GHR), наиболее близко

обеспечивающих результат времени разрешения идентификатора не более 1 сек. Для текущей конфигурации модели количество серверов составляет 7, 10, 1, 10, 10, 10, 10, 10 для каждого MPA из таблицы 1 соответственно, как показано столбце «Лучшее». Как видно из строки «Функционал», для лучшей итерации значение времени разрешения идентификатора составило 0.878 сек. По графику на рисунке 3 (красная линия) видно, что при конфигурации GHR-серверов, взятых по результатам оптимизационного эксперимента, разрешение идентификатора в системе происходит гораздо быстрее; прирост скорости в 15 раз достигается на максимальной интенсивности нагрузки.

Заключение

Основываясь на результатах моделирования системы, можно сделать выводы о том, что текущая инфраструктура системы резолюции требует дальнейшего масштабирования и распределения для того, чтобы быть способной выдерживать большие нагрузки и минимизировать время разрешения поступающих запросов. Особенно актуально это при использовании архитектуры DOA и системы резолюции в задачах, связанных с идентификацией устройств интернета вещей.

Помимо инфраструктурного расширения существующей системы, доработки нужно вести и в программной части. Как уже было упомянуто ранее, в результате анализа открытого исходного кода библиотеки, предоставляемой Handling.net [15] для построения собственных клиентских решений для взаимодействия с системой резолюции, было установлено, что при отправке запроса на разрешение идентификатора к серверам GHR не производится предварительного анализа времени сетевой задержки до каждого из серверов. Каждый сервер из списка, приведенного в таблице 1, опрашивается в случайной последовательности и анализируется первый полученный ответ. Такая реализация, несомненно, сказывается на общем времени разрешения идентификатора [16]. Поэтому требуется дальнейшая модификация исходного с целью создания функционала сортировки и приоритизации GHR-серверов в зависимости от сетевой задержки от клиентского устройства.

Список используемых источников

1. Аль-Бахри М.С., Киричек Р.В., Бородин А.С. Архитектура цифровых объектов как основа идентификации в эпоху цифровой экономики // Электросвязь. 2019. № 1. С. 12–21.
2. Белявский Д.М. и др. Цифровая идентификация объектов: технология и не только. М.: Научное обозрение, 2016. 228 с.
3. Kirichek R., Kulik V., Koucheryavy A. False clouds for Internet of Things and methods of protection // Proceedings of the 18th International Conference on Advanced Communication Technology (ICACT, Pyeongchang, South Korea, 31 January–3 February 2016). Piscataway, NJ: IEEE, 2016. PP. 201–205. DOI:10.1109/ICACT.2016.7423328
4. Al-Bahri M., Yankovsky A., Kirichek R., Borodin A. Smart System Based on DOA and IoT for Products Monitoring and Anti-Counterfeiting // Proceedings of the 4th MEC International Conference on Big Data and Smart City (ICBDSC, Muscat, Oman, 15–16 January 2019). Piscataway, NJ: IEEE, 2019. DOI:10.1109/ICBDSC.2019.8645610
5. Al-Bahri M., Yankovsky A., Borodin A., Kirichek R. Testbed for Identify IoT-Devices Based on Digital Object Architecture // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Proceedings of the 18th International Conference, NEW2AN, and the 11th Conference, ruSMART (27–29 August 2018, St. Petersburg, Russia). Lecture Notes in Computer Science. Cham: Springer, 2018. Vol. 11118. PP. 129–137. DOI:10.1007/978-3-030-01168-0_12
6. Albahri M., Kirichek R., Ateya A.A., Muthanna A., Borodin A. Combating Counterfeit for Io T System Based on DOA // Proceedings of the 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT, 5–9 November, 2018, Moscow, Russia). Piscataway, NJ: IEEE, 2018. DOI:10.1109/ICUMT.2018.8631257
7. Кучерявый А.Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.
8. Kahn R., Wilensky R. A framework for distributed digital object services // International Journal on Digital Libraries. 2006. Vol. 6. Iss. 2. PP. 115–123. DOI:10.1007/s00799-005-0128-x
9. Кучерявый А.Е., Прокопьев А.В., Кучерявый Е.А. Самоорганизующиеся сети. СПб.: Типография «Любавич», 2011. 312 с.
10. Тельтевская В.А., Зеленов В.В., Шустов Н.И., Кулик В.А., Киричек Р.В., Маколкина М.А. Идентификация устройств интернета вещей с помощью технологий дополненной реальности // Информационные технологии и телекоммуникации. 2017. Т. 5. № 4. С. 64–70.
11. Тхаи Н.З. Удаленные вычисления через Web-сервер MATLAB как система массового обслуживания // Вестник Иркутского государственного технического университета. 2012. № 4(63). С. 25–32.
12. Shortle J.F., Thompson J., Gross D., Harris C.M. Fundamentals of Queueing Theory. Hoboken: John Wiley & Sons., 2018. 576 p.
13. Handle.Net Registry. URL: http://www.handle.net/index.html (дата обращения 22.03.2019)
14. The Handle System // The DONA Foundation. URL: https://www.dona.net/handle-system (дата обращения 22.03.2019)
15. Balanis C.A. Antenna Theory: Analysis and Design. Hoboken: John Wiley & Sons, 2005.
16. Madhow U. Fundamentals of Digital Communication. New York: Cambridge University Press, 2008.

* * *

A DIGITAL OBJECT ARCHITECTURE BASED INTERNET OF THINGS DEVICES IDENTIFICATION SYSTEM MODELING

M.S. Al-Bahri[1], R. Kirichek[1], D. Sazonov[1]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Article info
Article in Russian

For citation: Al-Bahri M.S., Kirichek R., Sazonov D. A Digital Object Architecture Based Internet of Things Devices Identification System Modeling. *Proceedings of Telecommunication Universities*. 2019;5(1):42–47. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-1-42-47

Abstract: *The analysis of the possibility of building a system for identifying devices of the Internet of Things based on the Digital Object Architecture has been carried out. A model of the system of resolution handle system of Digital Object Identification as a queuing system is proposed. The analysis of the existing system Handling. Is proposed an identification system model based on digital object architecture. On the basis of the developed model of the queuing system, an optimization experiment was performed and the configuration of the resolution system was obtained, allowing to reduce the time for resolving the device identifier. The software of the existing Handle System resolution was analyzed and ways of improving the algorithms with the aim of reducing the time for identifier resolution were proposed.*

Keywords: *Internet of Things, Digital Object Architecture, Digital Object Identification, Handle System, queuing system.*

References

1. Al-Bahri M.S., Kirichek R.V., Borodin A.S. The digital object architecture as a basis for identification in the era of the digital economy. *Electrosvyaz*. 2019;1:12–21. (in Russ.)
2. Beliavskii D.M., et al. *Tsifrovaia identifikatsiia obieektov: tekhnologiia i ne tolko* [Digital Identification of Objects: Technology and Not Only]. Moscow: Scientific Review Publishing House; 2016. 228 p. (in Russ.)
3. Kirichek R., Kulik V., Koucheryavy A. False clouds for Internet of Things and methods of protection. *Proceedings of the 18th International Conference on Advanced Communication Technology (ICACT), 31 January–3 February 2016 Pyeongchang, South Korea.* Piscataway, NJ: IEEE; 2016. p.201–205. Available from: https://doi.org/10.1109/ICACT.2016.7423328
4. Al-Bahri M., Yankovsky A., Kirichek R., Borodin A. Smart System Based on DOA and IoT for Products Monitoring and Anti-Counterfeiting. *Proceedings of the 4th MEC International Conference on Big Data and Smart Citym, ICBDSC, 15–16 January 2019, Muscat, Oman*. Piscataway, NJ: IEEE, 2019. Available from: https://doi.org/10.1109/ICBDSC.2019.8645610
5. Al-Bahri M., Yankovsky A., Borodin A., Kirichek R. Testbed for Identify IoT-Devices Based on Digital Object Architecture. *Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Proceedings of the 18th International Conference, NEW2AN, and the 11th Conference, ruSMART, St. Petersburg, Russia, 27–29 August 2018. Lecture Notes in Computer Science*. Cham: Springer; 2018. Vol. 11118. p.129–137. Available from: https://doi.org/10.1007/978-3-030-01168-0_12
6. Albahri M., Kirichek R., Ateya A.A., Muthanna A., Borodin A. Combating Counterfeit for Io T System Based on DOA. *Proceedings of the 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT, Moscow, Russia, 5–9 November, 2018*. Piscataway, NJ: IEEE; 2018. Available from: https://doi.org/10.1109/ICUMT.2018. 8631257
7. Koucheryavy A.E. Internet Veshchei [Internet of Things]. *Electrosvyaz*. 2013;1:21–24. (in Russ.)
8. Kahn R., Wilensky R. A framework for distributed digital object services. *International Journal on Digital Libraries*. 2006;6(2):115–123. Available from: https://doi.org/10.1007/s00799-005-0128-x
9. Koucheryavy A.E., Prokopiev A.V., Koucheryavy Y.A. *Samoorganizuiushchiesia seti* [Self-organizing network]. St. Petersburg: Lyubavich Printing House; 2011. 312 p. (in Russ.)
10. Teltevskaya V., Zelenov V., Shustov N., Kulik V., Kirichek R., Makolkina M. Identification of the Internet of Things Devices with Augmented Reality Technologies. *Telecom IT*. 2017;5(4):64–70. (in Russ.)
11. Thai N.D. Remote Computing Through MATLAB Web-Server as Queueing System. *Proceedings of Irkutsk State Technical University*. 2012;4(63):25–32. (in Russ.)
12. Shortle J.F., Thompson J., Gross D., Harris C.M. *Fundamentals of Queueing Theory*. Hoboken: John Wiley & Sons.; 2018. 576 p.
13. Handle.Net Registry. Available from: http://www.handle.net/index.html [Accessed 22nd March 2019]
14. The DONA Foundation. *The Handle System*. Available from: https://www.dona.net/handle-system [Accessed 22nd March 2019]
15. Balanis C.A. *Antenna Theory: Analysis and Design*. Hoboken: John Wiley & Sons; 2005.
16. Madhow U. *Fundamentals of Digital Communication*. New York: Cambridge University Press; 2008.