УДК 004.057.4
DOI 10.17513/snt.39941

ПРОТОКОЛ ОРГАНИЗАЦИИ ДЕЦЕНТРАЛИЗОВАННОЙ БЕСПРОВОДНОЙ СЕТИ СВЯЗИ ДЛЯ ОБЕСПЕЧЕНИЯ ВЗАИМОДЕЙСТВИЯ СОЦИОКИБЕРФИЗИЧЕСКИХ СИСТЕМ

[1]Земцов А.Н., [1]Садек Сажжад, [2]Чан Зунг Хань

[1]ФГБОУ ВО «Волгоградский государственный технический университет», Волгоград, e-mail: ecmsys@yandex.ru

[2]Национальный экономический университет, Ханой, e-mail: ecmsys@yandex.ru

Аннотация. В статье рассматриваются вопросы модификации дистанционно-векторного протокола маршрутной информации для использования его в децентрализованной беспроводной сети связи социокиберфизических систем. Интеллектуальные сети социокиберфизических систем характеризуются большим количеством узлов. Протоколы маршрутизации состояния связей основаны на вычислительно сложных алгоритмах поиска кратчайших путей, таких как алгоритм Дейкстры, что негативно сказывается на взаимодействии большого количества узлов, поэтому предпочтительными для использования в интеллектуальной сети социокиберфизических систем являются дистанционно-векторные протоколы. Основной проблемой применения протокола маршрутной информации в децентрализованной беспроводной сети связи является возможность появления циклов маршрутизации, которые могут существовать произвольное время, из-за чего в дистанционно-векторных методах маршрутизации искусственно ограничивается максимально возможное расстояние между узлами. Проблемы сетевого взаимодействия узлов децентрализованной беспроводной сети связи особенно негативно сказываются на приложениях передачи трафика реального времени, а также организации скрытых каналов связи. Для достижения поставленной цели необходим механизм, позволяющий избежать ограничения на максимально возможное расстояние между узлами. Предлагается использовать комбинацию механизма триггерных обновлений и номеров последовательности. Приводится обоснование эффективности предотвращения образования циклов маршрутизации.

Ключевые слова: децентрализованная самоорганизующаяся сеть, беспроводная сеть, маршрутизация, протокол, стеганография, скрытие данных, цифровой водяной знак, защита информации

PROTOCOL FOR AD-HOC NETWORK FOR INTERACTION OF SOCIO-CYBER-PHYSICAL SYSTEMS

[1]Zemtsov A.N., [1]Sadiq Sajjad, [2]Tran Dung Khanh

[1]Volgograd State Technical University, Volgograd, e-mail: ecmsys@yandex.ru

[2]National Economics University, Hanoi, e-mail: ecmsys@yandex.ru

Annotation. The issues of modifying the distance vector routing information protocol for its use in a decentralized wireless communication network of socio-cyberphysical systems are considered. Intelligent networks of socio-cyberphysical systems are characterized by a large number of nodes. Link state routing protocols are based on computationally complex algorithms for finding shortest paths, such as Dijkstra's algorithm, which negatively affects the interaction of a large number of nodes, therefore distance vector protocols are more preferable for use in an intelligent network of socio-cyberphysical systems. The main problem of using the routing information protocol in a decentralized wireless communication network is the possibility of routing cycles that can exist for an arbitrary time, which is why distance vector routing methods artificially limit the maximum possible distance between nodes. Problems of network interaction between nodes of a decentralized wireless communication network have a particularly negative impact on applications of real-time traffic transmission, as well as the organization of covert communication channels. To achieve this goal, a mechanism is needed to avoid the limitation on the maximum possible distance between nodes. It is proposed to use a combination of triggered update mechanism and sequence numbers. A justification is given for the effectiveness of preventing the formation of routing loops.

Keywords: ad-hoc network, wireless network, routing, protocol, steganography, data hiding, digital watermark, information security

В последние годы разработка интеллектуальных методов многомодального взаимодействия социокиберфизических систем является активной областью исследований, которые дополнительно стимулируются значительными достижениями в области технологий беспроводных сетей связи LTE Direct, LTE-A, LTE-A Pro, 5G NR, миниатюризации и снижения стоимости цифровых устройств. Следствием являются ориентация на мобильность, увеличение активности взаимодействия большого количества социокиберфизических систем в составе интеллектуальной сети. Для интеллектуальных медицинских систем уже разработан широкий спектр средств мониторинга состояния и диагностики пациентов. В исследовании [1] приводятся результаты, демонстрирующие, что к 2025 году будет использоваться около 200 миллионов медицинских социокиберфизических систем. С увеличением количества социокиберфизических систем

в составе интеллектуальной сети предъявляются более строгие требования к безопасности [2] и отказоустойчивости их взаимодействия [3, 4]. Подобные статистические данные приводятся и для других отраслей народного хозяйства [5–9]. Интеллектуальные транспортные системы на основе автомобильных самоорганизующихся сетей характеризуются множеством практически неограниченно движущихся в любом направлении с различной скоростью узлов сети. Многомодальное взаимодействие подобных социокиберфизических систем, использующееся, например, для повышения эффективности обеспечения информационной безопасности за счет применения стеганографических методов защиты трафика [10] или служб транспортной безопасности [11], описанных в группе стандартов IEEE 1609 [12], предполагает наличие трафика высокой интенсивности между различными элементами интеллектуальной сети социокиберфизических систем. Как следствие, особенно важным показателем является вероятность доставки пакета между исходным и целевым узлами [13]. Невозможность доставки пакета от исходного узла к целевому может порождать ситуацию отключения узлов и повторного установления соединения между ними. Процесс отключения приводит к поиску нового маршрута между узлами и последующему повторному установлению соединения, что существенно снижает производительность сети в целом вследствие снижения пропускной способности, увеличения задержки и джиттера. Особенно остро эта проблема стоит при организации скрытых каналов связи и передаче трафика реального времени [14], например трафика систем городского видеонаблюдения. Эта проблема ставит перед исследователями новые актуальные задачи по усовершенствованию протоколов маршрутизации, средств обеспечения безопасности, а также качества обслуживания в интеллектуальной сети социокиберфизических систем. Протокол маршрутной информации является привлекательным для его применения в интеллектуальных сетях социокиберфизических систем, поскольку имеет линейную сложность, но его использование невозможно из-за жесткого ограничения на количество узлов. Цель исследования заключается в модификации дистанционно-векторного протокола маршрутной информации для использования его в интеллектуальной сети социокиберфизических систем.

Методы маршрутизации

В одношаговых методах маршрутизации, когда при определении в соответствии с критерием оптимальности маршрута задействуется только смежный узел маршрутизатор, а не полная последовательность маршрутизаторов от начального до конечного узла, различают статическую и адаптивную (динамическую) маршрутизацию. В случае адаптивной маршрутизации изменения конфигурации сети автоматически отображаются в специальных таблицах протоколами маршрутизации. На рисунке 1 показана упрощенная классификация протоколов маршрутизации.

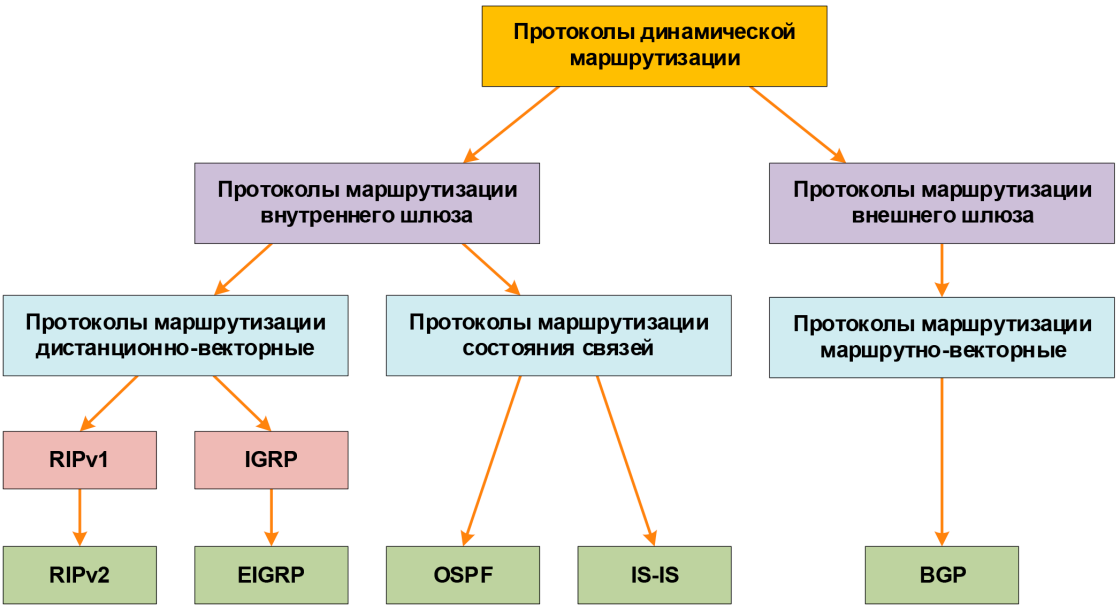

Рис. 1. Классификация протоколов маршрутизации

В зависимости от типа интеллектуальной сети могут использоваться другие классификационные признаки. Например, протоколы маршрутизации в автомобильных самоорганизующихся сетях делят на: топологические, проактивные, реактивные, широковещательные, кластерные и др.

В методах, оценивающих состояния связей, все узлы имеют сведения о полной топологии сети и расстояниях между узлами. Интеллектуальные сети социокиберфизических систем характеризуются большим количеством узлов. К сожалению, протоколы маршрутизации состояния связей [15] предполагают использование вычислительно сложных алгоритмов поиска кратчайших путей для формирования базы данных топологии, таких как алгоритм Дейкстры [16], что негативно сказывается на взаимодействии большого количества узлов, поэтому более предпочтительными для использования в интеллектуальной сети социокиберфизических систем являются дистанционно-векторные протоколы.

Проблема дистанционно-векторных методов

В дистанционно-векторных методах маршрутизации каждый узел взаимодействует, принимая, обрабатывая и передавая векторы, только со смежными узлами. Дистанционно-векторные методы основаны на алгоритме из семейства алгоритмов Беллмана–Форда и характеризуются простотой работы, что обусловливает высокую скорость их работы при взаимодействии большого количества узлов [17]. Здесь возникает проблема обеспечения достоверности информации, содержащейся в принимаемых векторах. Следствием этой проблемы могут стать маршрутные петли.

Таблица 1

Согласованные таблицы маршрутизации

R1			R3			R4			R5		
Dest	GW	Metric	Dest	GW	Metric	Dest	GW	Metric	Dest	GW	Metric
R1	R1	0	R1	R2	2	R1	R1	1	R1	R1	1
R2	R2	1	R2	R2	1	R2	R3	2	R2	R1	2
R3	R2	2	R3	R3	0	R3	R3	1	R3	R1	3
R4	R4	1	R4	R4	1	R4	R4	0	R4	R1	2
R5	R5	1	R5	R2	3	R5	R1	2	R5	R5	0

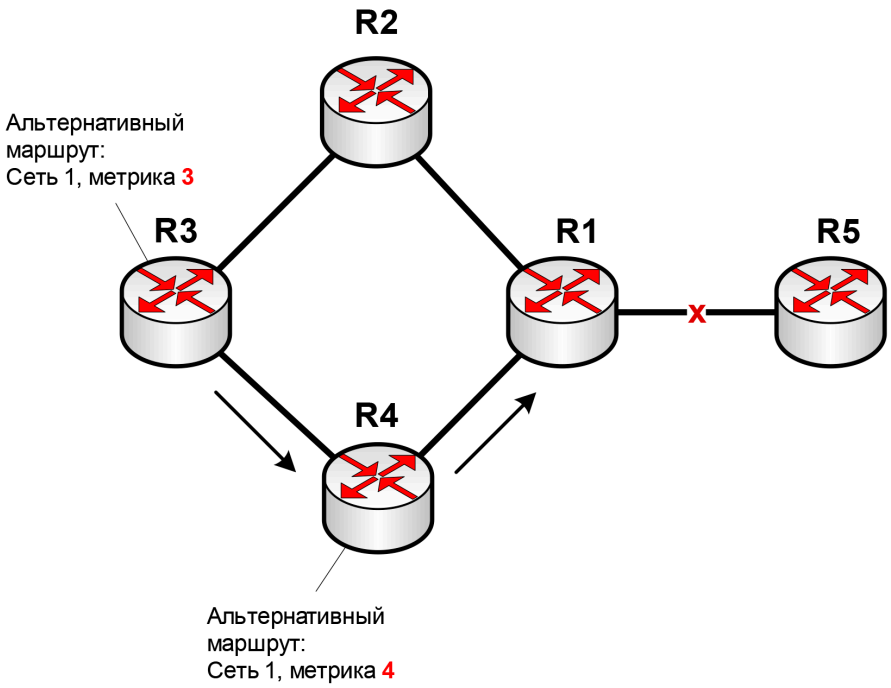

Рис. 2. Проблема достоверности информации в векторах

Для пояснения подобной ситуации рассмотрим пример на рисунке 2, когда непосредственно перед отказом канала связи между узлом R1 и узлом R5 узлы R1-R5 имеют согласованные (табл. 1) и корректные таблицы маршрутизации.

Предположим, что для узла R3 наилучший маршрут к узлу R5 проходит через узел R2 и что в своей таблице маршрутизации узел R3 имеет сведения о расстоянии до узла R5, равном 3.

В случае когда канал связи между узлами R1 и R5 переходит в состояние отказа (табл. 2), узел R1 прекращает направлять пакеты узлу R5, в отличие от узлов R1, R3 и R4, поскольку они еще не получили соответствующий вектор с информацией об отказе.

На следующем этапе узел R1 отправляет вектор с информацией об отказе смежным узлам R2 и R4, которые прекращают направлять пакеты узлу R5 (табл. 3). В этот момент времени узел R3 еще не имеет сведений об отказе канала связи между узлами R1 и R5.

В случае когда узел R3 не успел получить вектор с информацией об отказе, но истек тайм-аут до очередной периодической рассылки векторов согласно алгоритму работы дистанционно-векторных протоколов маршрутизации, узел R3 посылает свои векторы узлу R4, указывая, что у него имеется маршрут до узла R5 через узел R2.

Узел R4 изменяет свою таблицу маршрутизации в соответствии со сведениями, содержащимися в полученном от узла R2 векторе, и формирует соответствующий вектор для узла R1. В свою очередь, узел R1 распространяет информацию о доступности R5 узлу R2. В результате любой пакет к R5 будет передаваться узлами сети по циклу R3–R2–R1–R4–R3 (табл. 4).

Таблица 2

Таблицы маршрутизации при отказе канала связи между узлами R1 и R5

R1			R2			R3			R4		
Dest	GW	Metric	Dest	GW	Metric	Dest	GW	Metric	Dest	GW	Metric
R1	R1	0	R1	R2	2	R1	R2	2	R1	R1	1
R2	R2	1	R2	R2	1	R2	R2	1	R2	R3	2
R3	R2	2	R3	R3	0	R3	R3	0	R3	R3	1
R4	R4	1	R4	R4	1	R4	R4	1	R4	R4	0
R5	R5	∞	R5	R2	3	R5	R2	3	R5	R1	2

Таблица 3

Уведомление смежных узлов об отказе

R1			R2			R3			R4		
Dest	GW	Metric	Dest	GW	Metric	Dest	GW	Metric	Dest	GW	Metric
R1	R1	0	R1	R2	2	R1	R2	2	R1	R1	1
R2	R2	1	R2	R2	1	R2	R2	1	R2	R3	2
R3	R2	2	R3	R3	0	R3	R3	0	R3	R3	1
R4	R4	1	R4	R4	1	R4	R4	1	R4	R4	0
R5	R5	∞	R5	R2	∞	R5	R2	3	R5	R1	∞

Таблица 4

Появление цикла маршрутизации

R1			R2			R3			R4		
Dest	GW	Metric	Dest	GW	Metric	Dest	GW	Metric	Dest	GW	Metric
R1	R1	0	R1	R2	2	R1	R2	2	R1	R1	1
R2	R2	1	R2	R2	1	R2	R2	1	R2	R3	2
R3	R2	2	R3	R3	0	R3	R3	0	R3	R3	1
R4	R4	1	R4	R4	1	R4	R4	1	R4	R4	0
R5	R4	5	R5	R1	6	R5	R2	3	R5	R3	4

Предлагаемые решения проблемы

Для уменьшения вероятности возникновения циклов могут использоваться различные механизмы: расщепление горизонта, таймеры удержания состояния, отправление маршрута [18]. Необходимо отметить, что некорректная информация в векторах дает возможность циклу существовать бесконечное время. В связи с тем, что ни один из механизмов не позволяет предотвратить появление цикла и цикл может существовать продолжительное время, в дистанционно-векторных методах маршрутизации искусственно ограничивается максимально возможное расстояние между узлами. Кроме того, перечисленные механизмы слабо подходят для использования их в децентрализованной беспроводной сети связи (например, механизм расщепления горизонта неэффективен на топологиях, содержащих циклы).

Протокол маршрутной информации имеет линейную сложность $O(n)$, где n – количество узлов сети, в то время как протоколы состояния связи имеют сложность $O(n^2)$, и их применение затруднительно в сетях с большим количеством узлов [19], к которым относятся сети киберфизических систем. Для достижения поставленной цели необходим механизм, позволяющий избежать ограничения на максимально возможное расстояние между узлами.

В протоколе маршрутной информации векторы, содержащие маршрутную информацию, штатно передаются смежным узлам периодически. Механизм триггерных обновлений предполагает осуществление передачи векторов с маршрутной информацией, касающейся обнаруженных изменений топологии сети социокиберфизических систем, смежным узлам незамедлительно. Триггерные обновления генерирует узел, обнаруживший изменения топологии сети, при этом используется волновой принцип доставки векторов. Смежные узлы, получившие векторы с маршрутной информацией, в свою очередь, также генерируют триггерные обновления, таймеры периодической рассылки сбрасываются. В примере, показанном на рисунке 2, узел R1 генерирует триггерные обновления для узлов R2 и R4, информируя их об отказе канала связи между узлом R1 и узлом R5. После получения векторов с обновленной информацией об изменении топологии сети узлы R2 и R4 извещают об этом изменении смежный узел R3.

Для адаптации протокола маршрутной информации в целях использования в децентрализованной беспроводной сети связи добавим новый атрибут – номер последовательности к каждой записи таблицы маршрутов. Этот атрибут позволяет предотвратить образование циклов маршрутизации. В процессе подготовки векторов с маршрутной информацией узел помечает каждый вектор монотонно возрастающим номером последовательности обновления, позволяющим отличить устаревшие векторы от актуальных.

Таким образом, если узел получает вектор от другого узла, номер последовательности обновления должен быть больше или равен номеру последовательности узла, уже присутствующего в его таблице маршрутизации. Если это условие не выполняется, то полученный вектор в пакете обновления является неактуальным, и его следует отбросить. Если номер последовательности в полученном векторе обновления информации о маршрутизации совпадает с соответствующим номером последовательности в таблице маршрутизации узла, то в результате сравнения метрик в таблицу устанавливается маршрут с лучшим значением (табл. 5).

Перемещение или отключение мобильных узлов в децентрализованной беспроводной сети связи приводят к изменению топологии сети. Отсутствие соединения может быть диагностировано аппаратным обеспечением узла связи или самим протоколом, если от определенного узла в течение заданного тайм-аута не было получено соответствующего вектора.

Таблица 5

Модифицированные таблицы маршрутизации

R1				R3				R4			
Dest	GW	Metric	Seq	Dest	GW	Metric	Seq	Dest	GW	Metric	Seq
R1	R1	0	124:R1	R1	R2	2	124:R1	R1	R1	1	124:R1
R2	R2	1	402:R2	R2	R2	1	402:R2	R2	R3	2	402:R2
R3	R2	2	528:R3	R3	R3	0	528:R3	R3	R3	1	528:R3
R4	R4	1	712:R4	R4	R4	1	712:R4	R4	R4	0	712:R4
R5	R5	1	160:R5	R5	R2	3	160:R5	R5	R1	2	160:R5

Таблица 6

Предотвращение цикла маршрутизации

R1				R3				R4			
Dest	GW	Metric	Seq	Dest	GW	Metric	Seq	Dest	GW	Metric	Seq
R1	R1	0	124:R1	R1	R2	2	124:R1	R1	R1	1	124:R1
R2	R2	1	402:R2	R2	R2	1	402:R2	R2	R3	2	402:R2
R3	R2	2	528:R3	R3	R3	0	528:R3	R3	R3	1	528:R3
R4	R4	1	712:R4	R4	R4	1	712:R4	R4	R4	0	712:R4
R5	R5	∞	161:R5	R5	R2	3	160:R5	R5	R1	2	160:R5

В случае обнаружения отказа маршруту через этот узел присваивается метрика, равная бесконечности, номер последовательности обновления инкрементируется. Отключение мобильного узла квалифицируется как существенное изменение топологии сети, в связи с чем узел, обнаруживший изменение, должен осуществить триггерное обновление.

В случае отказа канала связи между узлом R1 и узлом R5 узел R1 изменяет значение метрики в таблице маршрутизации и номер последовательности на 161, что гарантирует отсутствие возможности возникновения цикла маршрутизации. Таким образом, запись об узле R5 не будет чувствительной к получаемым узлом R1 от узлов R2 и R4 векторам, поскольку номера последовательности в их таблицах имеют меньшие значения. Далее узел R1 рассылает триггерное обновление узлам R2 и R4 с номером последовательности, равным 161 (табл. 6).

Маршруты к узлу R5 будут рассчитаны заново, когда узел R5 установит соединение с каким-либо узлом сети и отправит сообщение обновления с тем же или более поздним номером последовательности.

Заключение

В настоящей работе предложена модификация дистанционно-векторного протокола маршрутной информации для использования его в интеллектуальной сети социокиберфизических систем. Интеллектуальные сети социокиберфизических систем характеризуются высоким уровнем активности взаимодействия большого количества узлов, что обусловливает дополнительные требования отказоустойчивости и обеспечения требуемого уровня качества обслуживания. Особенно важным показателем является вероятность доставки пакета между исходным и целевым узлами. Невозможность доставки пакета приводит к отключению узлов и повторному установлению соединения между ними, что существенно снижает производительность сети в целом вследствие снижения пропускной способности, увеличения задержки и джиттера. Особенно остро эта проблема стоит при передаче трафика реального времени и организации скрытых каналов связи. Кроме того, топология сети постоянно изменяется, поскольку узлы сети характеризуются высоким уровнем мобильности. Таблица маршрутизации включает минимальный набор параметров: адрес каждого узла, адрес шлюза, метрика маршрута, номер последовательности. Рассылка векторов штатно осуществляется периодически, иначе используются триггерные обновления. В таблицу маршрутизации устанавливаются маршруты с большим по значению номером последовательности. Если номера последовательности идентичны, в таблицу маршрутизации устанавливается маршрут с меньшей метрикой.

Список литературы

1. Statista. Global estimated healthcare IoT device installations 2015 to 2020. [Электронный ресурс]. URL: www.statista.com/statistics/735810/healthcare-iot-installations-global-estimate/ (дата обращения: 14.02.2024).

2. Бабенко Л.К., Шумилин А.С., Алексеев Д.М. Алгоритм обеспечения безопасности конфиденциальных данных медицинской информационной системы хранения и обработки результатов обследований // Известия ЮФУ. Технические науки. 2020. № 5(215). С. 6-16.

3. Bradley W.C. Handbook of Data Center Management. Auerbach Publications CRC Press. 2018. 816 p.

4. Zemtsov A. Performance Evaluation of First Hop Redundancy Protocols for a Computer Networks of an Industrial Enterprise // 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). 2019. P. 1-5. DOI: 10.1109/FarEastCon.2019.8934315.

5. Duo W., Zhou M., Abusorrah A. A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges // IEEE/CAA Journal of Automatica Sinica. 2022. Vol. 9(5). P. 784-800. DOI: 10.1109/JAS.2022.105548.

6. Progoulakis I., Rohmeyer P., Nikitakos N. Cyber Physical Systems Security for Maritime Assets // Journal of Marine Science and Engineering. 2021. Vol. 9(12). P.1384. DOI: 10.3390/jmse9121384.

7. Wang Z., Liu X. Cyber security of railway cyber-physical system – A risk management methodology // Communications in Transportation Research. 2022. Vol. 2. P. 100078. DOI: 10.1016/j.commtr.2022.100078.

8. Мясникова О.В. Теоретико-концептуальные подходы к формированию производственно-логистической системы умного производства как социокиберфизической системы // Экономика. Управление. Инновации. 2020. № 1(7). С. 29-35.

9. Serodio C. Software and Architecture Orchestration for Process Control in Industry 4.0 Enabled by Cyber-Physical Systems Technologies // Applied Sciences. 2024. Vol. 14(5). P. 2160. DOI: 10.3390/app14052160.

10. Земцов А.Н., Садек С. Защита графической информации в системе управления городским движением от неправомерного использования // Инженерный вестник Дона. 2023. № 12(108). С. 207-216.

11. Земцов А.Н., Кузнецов М.А., Садек С., Попов В.К., Ступницкий П.С. Автоматическое распознавание автомобильных номерных знаков в автомобильной самоорганизующейся сети // Инженерный вестник Дона. 2023. № 12(108). URL: http://www.ivdon.ru/ru/magazine/archive/n12y2023/8880 (дата обращения: 04.02.2024).

12. IEEE Standard for Wireless Access in Vehicular Environments // IEEE Std. 1609.12-2019. 2019. [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/8877516 (дата обращения: 11.02.2024). DOI: 10.1109/IEEESTD.2019.8877516.

13. Земцов А.Н., Чан З.Х. Анализ эффективности алгоритмов планирования передачи пакета в сетях LTE // Инженерный вестник Дона. 2019. № 4(55). URL: http://www.ivdon.ru/ru/magazine/archive/n4y2019/5840 (дата обращения: 08.02.2024).

14. Антоненко А.С. Оценка параметров QoS для бесперебойной работы IPTV // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14, № 10. С. 33-38.

15. Изотова Т.Ю. Обзор алгоритмов поиска кратчайшего пути в графе // Новые информационные технологии в автоматизированных системах. 2016. № 19. С. 341-344.

16. Барыбин Д.А., Кофман Е.Ю., Шульгин М.С. Сравнение алгоритмов Дейкстры и Беллмана-Форда при решении задачи о поиске кратчайшего пути в протоколах маршрутизации // Символ науки. 2021. № 6. С. 27-31.

17. Кирьянов В.А., Буторин К.А., Сухов А.А. Анализ использования протоколов внутренней динамической маршрутизации RIP и OSPF в современных сетевых инфраструктурах // Наукосфера. 2023. № 12-2. С. 177-181.

18. Almutairi H., Zhang N. A Survey on Routing Solutions for Low-Power and Lossy Networks: Toward a Reliable Path-Finding Approach // Network. 2024. Vol. 4(1). P. 1-32. DOI: 10.3390/network4010001.

19. Tsochev G. A Comparative Study by Simulation of OSPF and EIGRP Routing Protocols // Informatics and Automation. 2022. Vol. 21(6). P. 1240-1264. DOI: 10.15622/ia.21.6.6.