Научная статья
УДК 004.056.5; DOI: 10.61260/2218-13X-2024-3-35-44

ПОДХОД К РАЗРАБОТКЕ ПРОТОКОЛА ДЕЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

✉**Десницкий Василий Алексеевич.**
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Россия
✉***desnitsky@comsec.spb.ru***

Аннотация. Статья посвящена вопросам построения и оценки протокола децентрализованного управления в самоорганизующейся децентрализованной беспроводной сенсорной сети в рамках индустриального Интернета вещей. Протокол ориентирован на организацию и поддержку функционирования и мониторинг информационной безопасности сети в целях сбора, обработки, хранения и анализа данных с узлов беспроводной сенсорной сети в условиях высокого динамизма и изменчивости структуры такой сети, состава ее узлов, их физического месторасположения в пространстве, поведения узлов и объемов их доступных ресурсов. В настоящей статье основное внимание уделяется двум предлагаемым алгоритмам организации многосторонней сессии узлов беспроводной сенсорной сети, лежащим в основе данного протокола с использованием ролевой модели узлов. Формируемый протокол предназначен для решения задач мониторинга информационной безопасности самоорганизующейся децентрализованной беспроводной сенсорной сети и обнаружения атак, эксплуатирующих, в том числе, свойства самоорганизации и децентрализации сети.

Ключевые слова: беспроводная сенсорная сеть, децентрализованное управление, протокол

Для цитирования: Десницкий В.А. Подход к разработке протокола децентрализованного управления в беспроводных сенсорных сетях // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 35–44. DOI: 10.61260/2218-13X-2024-3-35-44.

Scientific article

APPROACH TO CONSTRUCTION OF DECENTRALIZED CONTROL PROTOCOL IN WIRELESS SENSOR NETWORKS

✉**Desnitskiy Vasiliy A.**
Saint-Petersburg Federal research center of the Russian academy of sciences,
Saint-Petersburg, Russia
✉***desnitsky@comsec.spb.ru***

Abstract. The article encompasses development and assessment issues of the decentralized control protocol in mesh decentralized wireless sensor networks within the industrial Internet of things. The protocol is used to ensure the operation of the network, including functions of gathering, processing and analyzing data received from network nodes to solve the problem of monitoring information security, given the variability of the network composition and its topology, the spatial placement of nodes, as well as the volumes of their resources. In this article, the main attention is paid to the proposed two algorithms for organizing a multilateral session of wireless sensor networks nodes, which form the basis of this protocol, using a role model of nodes. The formed protocol is focused on solving the issues of monitoring the information security of a mesh decentralized wireless sensor network and revealing attacks that exploit, among other things, the properties of wireless sensor networks self-organization and decentralization.

Keywords: wireless sensor network, decentralized control, protocol

For citation: Desnitskiy V.A. Approach to construction of decentralized control protocol in wireless sensor networks // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 3. P. 35–44. DOI: 10.61260/2218-13X-2024-3-35-44.

Введение

В настоящее время все большее распространение получают беспроводные сенсорные сети (БСС), функционирующие в рамках различных индустриальных киберфизических инфраструктур на транспорте, в промышленном производстве, в электроэнергетике, в рамках инфраструктур умных городов, интеллектуальных систем управления и реагирования в чрезвычайных ситуациях [1]. При этом возникает все большая потребность в средствах распределенного взаимодействия, обмена и хранения информации, непосредственно интегрируемых с узлами таких сетей.

Характерным примером подобных БСС являются системы соединенных дронов (connected drones), в которых спонтанно собираемые из отдельных узлов сети под конкретные прикладные задачи способны повышать эффективность целевых процессов за счет согласованных и защищенных процессов сбора, обработки, хранения и анализа данных в условиях функционирования в недоверенной среде [2, 3]. Поэтому разработка и обеспечение защищенности протоколов управления такими БСС представляется в настоящее время особенно важной [4, 5].

Разрабатываемый протокол децентрализованного управления нацелен на обеспечение связности узлов БСС, надежности и бесперебойности функций коммуникации в сети с учетом особенностей регулярной или спонтанной смены функциональных ролей узлов сети. В частности, предлагаемый протокол использует усовершенствованный механизм распределенных реестров – блокчейн, гарантирующий неизменность собираемых и хранимых в рамках периметра сети данных [6, 7]. К отличительным особенностям протокола в целом можно отнести возможность гибкой настройки используемого механизма блокчейна, обеспечивающей децентрализованное дублирование формируемых блоков по имеющимся в текущий момент времени узлам БСС в автоматическом режиме. Помимо бесперебойности процессов сбора, обработки, хранения и анализа целевых данных БСС предлагаемый протокол обеспечивает также возможность валидации данных, хранимых на узлах распределенным образом, – в целях гарантии неизменности данных [8].

Вкладом данной статьи являются два альтернативных алгоритма, позволяющих организовать многостороннюю сессию для надежного и защищенного обмена данными между узлами БСС, а также результаты аналитического сравнения обоих алгоритмов. В качестве дополнения отметим, что обеспечение целостности прикладных и служебных данных, формируемых на узлах сети, предполагается за счет использования облегченного блокчейна. При этом блокчейн разворачивается на узлах сети и обеспечивает распределенное защищенное хранение наиболее важных данных с допустимыми затратами на хранение этих данных. Также проводится анализ полученных в работе результатов.

Построение протокола децентрализованного управления

Разрабатываемый протокол включает средства функционирования узлов самоорганизующейся децентрализованной БСС с ролевой моделью узлов сети. Выделяются следующие основные роли: сборщик данных, обработчик данных, хранитель, анализатор данных и событий [9]. В данном разделе представлены два следующих алгоритма, формирующих протокол децентрализованного управления в БСС.

Алгоритм для установления многосторонней сессии предназначен для поиска узлов БСС, находящихся в зоне действия беспроводного сигнала, использующих общий сетевой идентификатор PAN ID и намеревающихся установить логическую сессию или присоединиться к уже существующей сессии. Такая сеть формируется в рамках прикладного

уровня коммуникаций для решения задач защищенного сбора данных, обмена данными между узлами и анализа данных в интересах оперативного управления и мониторинга информационной безопасности сети [10].

Входным для данного алгоритма является параметр n, определяющий минимальное количество участников (узлов БСС), которые необходимы для инициации многосторонней сессии и задаваемый организаторами сети. Также на вход подается значение параметра Δ, формирующее резерв для снижения вероятности того, что из-за спонтанно отсоединившихся от сети узлов, число функционирующих узлов опустится ниже установленного значения n. На рис. 1 в виде диаграммы последовательностей приведена схема работы данного алгоритма для случая линейного фрагмента БСС с узлами $A \leftrightarrow B \leftrightarrow C$. Далее приведены пояснения работы основных шагов данного алгоритма.

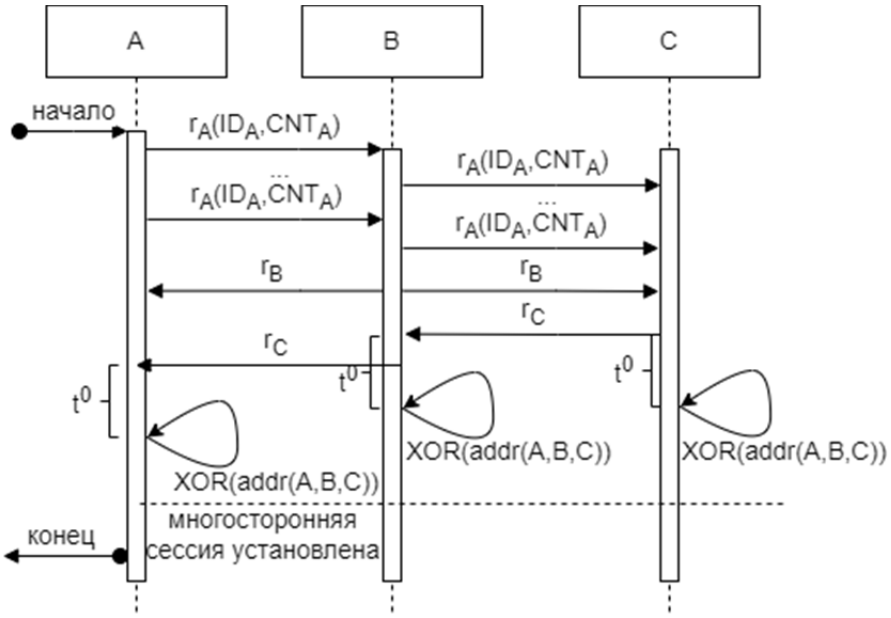

Рис. 1. **Схема работы алгоритма на примере фрагмента БСС с тремя узлами**

Первоначально любой узел, функционирующий в рамках текущего коммуникационно-вычислительного окружения узлов и намеревающийся войти в формируемую логическую сессию, транслирует в сеть свою готовность при помощи широковещательных команд r_A, отправляемых с заданной частотой (например, один раз в секунду). Такие команды отправляются в рамках используемого сетевого протокола ZigBee [11]. Каждая такая команда содержит, во-первых, уникальный идентификатор самого узла ID_A и, во-вторых, уникальное значение счетчика команд демонстрации готовности узла присоединиться к формируемой многосторонней сессии CNT_A. Первый идентификатор представляет собой уникальный физический (MAC) адрес ZigBee-модуля, тогда как второй идентификатор изначально инициализируется нулевым значением, а после каждой такой команды это значение увеличивается на единицу.

Далее каждый узел сети, находящийся в состоянии готовности, сам ретранслирует на все соседние с ним узлы поступившие ему команды готовности, за исключением узла, с которого такая команда поступила на этот узел. В случае если некоторый экземпляр команды на данный узел уже поступал и пересылался в сеть, то эта команда игнорируется. При этом каждый узел собирает и постоянно актуализирует данные о состоянии узлов, находящихся в текущий момент времени в состоянии готовности.

При достижении на узле сведений о том, что $(n+\Delta)$ узел находится в состоянии готовности, этот узел широковещательной командой отправляет команду на создание логической сессии и также начинает повторять команду с заданной периодичностью

(например, один раз в секунду). Кроме того, узел ждет аналогичных команд от других узлов, выразивших готовность – то есть от узлов из своего списка. Данный узел собирает таблицу таких подтверждений от всех $(n+\Delta)$ узлов. Отметим, что когда узел получает подтверждение от всех $(n+\Delta)$ узлов, он прекращает трансляцию своих широковещательных команд.

Далее узел ожидает константное время t^O, необходимое для доставки всех оставшихся широковещательных команд по сети. Если за этот промежуток времени никто из участников не прислал свою команду, то это означает, что все участники информационного обмена фактически «договорились» о составе участников, и сессию можно начинать. Иначе ожидание продлевается еще на величину интервала t^O.

Каждый узел, зная физические адреса каждого участника информационного обмена устанавливаемой сессии, вычисляет единый, общий для всех (разделяемый) идентификатор сессии при помощи битовой операции «исключающего ИЛИ» бинарных представлений всех адресов. Отметим, что в силу коммутативности данной операции, порядок ее применения неважен, и результирующее значение будет одинаковым на всех узлах. Опциональным завершающим шагом может быть многосторонний обмен данным идентификатором в качестве дополнительного подтверждения корректности получения всеми участниками сессии. Размер идентификатора сессии будет равен размеру физического адреса узла. Отметим также, что идентификатор будет отличаться в зависимости от состава узлов, которые решили такую сессию организовать. Идентификатор сессии будет однозначно определять текущую сетевую сессии. При этом на идентификатор сессии не накладывается требование секретности по отношению к каким-либо оставшимся узлам БСС.

К отличительным особенностям данного алгоритма можно отнести использование принципа многостороннего рукопожатия как средства для уточнения состава узлов многосторонней сессии и выработки единого уникального идентификатора сессии, на основе которого будет происходить дальнейшая коммуникация узлов. При этом данный алгоритм является в достаточной степени масштабируемым, позволяя организовывать многосторонние сессии на большом наборе узлов БСС, взаимодействующих на сетевом уровне. Кроме того, отметим, что данный алгоритм не требует значительного расходования коммуникационно-вычислительных ресурсов узлов БСС и поэтому может использоваться, в том числе, в ZigBee-сетях в условиях маломощных микроконтроллеров или одноплатных компьютеров, в качестве программно-аппаратной платформы узлов сети. Вместе с тем обильное использование широковещательных сообщений в процессе установления сессии, тем не менее создает дополнительный трафик, эффект от которого может сказываться негативно на выполнении прикладных сценариев БСС.

Алгоритм для установления многосторонней сессии на основе кластеризации узлов является альтернативным к представленному выше алгоритму организации многосторонней сессии. Суть второго алгоритма сводится к последовательной попарной кластеризации узлов, когда два узла, намеревающихся войти в организуемую многостороннюю сессию, связываются друг с другом, образуя базовый кластер [12]. После этого образованный кластер рекурсивно продолжает поиск других узлов, также готовых связаться с его узлами. Таким образом, формируемые кластеры последовательно укрупняются, каждый раз формируя новый уникальный идентификатор, разделяемый узлами, уже находящимися в рамках данного кластера. На конечном этапе процесса организации сессии некоторый кластер объединяется с другим подобным кластером или отдельным узлом, и они образуют единственный объединенный кластер с выработкой единого уникального идентификатора сессии. На рис. 2 в виде диаграммы последовательностей приведена обобщенная схема работы данного алгоритма на примере фрагмента БСС, состоящего из четырех узлов. Далее приведены пояснения работы основных шагов данного алгоритма.

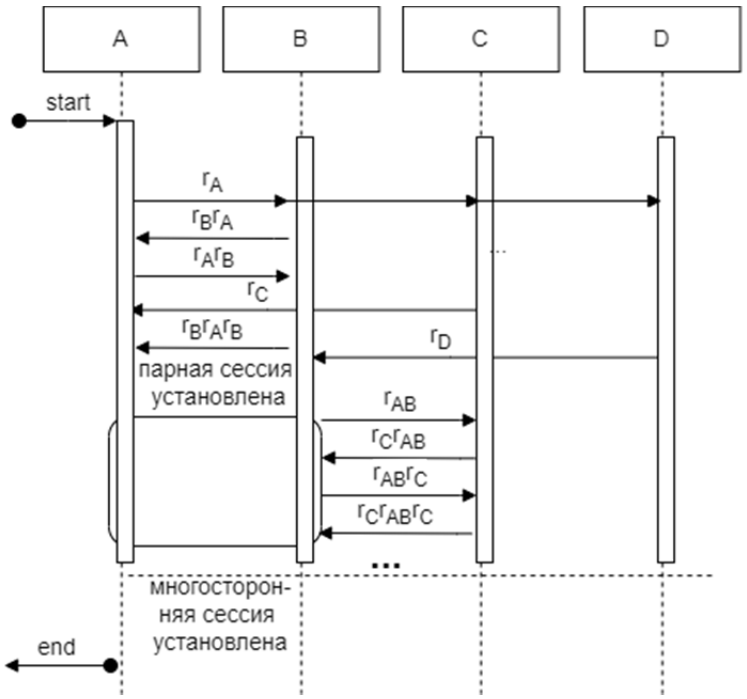

Рис. 2. **Схема работы алгоритма для установления многосторонней сессии на основе кластеризации узлов**

Первоначально каждый из узлов, желающий участвовать в организации многосторонней сессии в рамках БСС, отправляет широковещательный запрос. Так, узел *A* отправляет запрос r_A всем узлам, находящимся в пределах зоны действия беспроводного сигнала и обладающих заданным значением идентификатора PAN ID. Идентификатор r_A включает в свой состав физический адрес узла *A*. В ответ на данный запрос узел *B* сформирует и отправит команду $r_B r_A$, подтверждая тем самым согласие образовать парную связь с узлом *A*. Для идентификации того, на какой запрос выполнен данный ответ, ответное сообщение включает, в частности, повтор идентификатора r_A, а также идентификатор r_B, включающий физический адрес узла *B*.

После получения ответа на первоначальный запрос, узел *A* выбирает один из узлов в качестве узла для образования парной связи и в качестве своего подтверждения отправляет узлу *B* подтверждение в виде инверсированного сообщения $r_A r_B$. В соответствии с данным протоколом выбор конкретного узла, который узел *A* принимает в качестве текущего узла-партнера, делегируется непосредственно узлу *A*. Среди возможных кандидатов может быть выбран тот узел, ответ о готовности от которого пришел раньше ответов от других узлов. Отметим также, что на рис. 2 запрос r_C от узла *C* игнорируется, поскольку к моменту его прихода парная связь между узлами *A* и *B* уже в процессе установления.

Финальное подтверждение в виде команды $r_B r_A r_B$ отправляется от узла *B* к узлу *A*. После этого парная сессия между этими двумя узлами считается установленной. Далее, в рамках рассматриваемого протокола узлы *A* и *B* представляют одну единицу взаимодействия для установления парных сессий с другими узлами или группами узлов, образуя тем самым итеративно многостороннюю сессию между всеми узлами данной БСС, которые находятся в зоне видимости беспроводного сигнала, имеют общий идентификатор сети PAN ID и выразили готовность участвовать в данной многосторонней сессии. Таким образом, алгоритм завершает свою работу по факту формирования такой многосторонней сессии.

К отличительным особенностям данного алгоритма можно отнести итеративный характер алгоритма, причем процесс кластеризации имеет признаки иерархичности – процесс образования и укрупнения кластеров может быть растянут во времени. Например, в случае если в некоторый момент времени не удалось вовлечь в организуемую сессию

требуемые *(n+Δ)* узлов, то процесс формирования сессии может быть переведен в режим ожидания до момента появления узлов с необходимым PAN ID и их готовности войти в данную сессию. Поэтому к преимуществу использования данного алгоритма организации сессии можно отнести его ориентированность на ситуации с нестабильным сетевым покрытием, помехами беспроводного сигнала, сложным рельефом местности с преградами или приемо-передающими интерфейсами пониженной мощности. Вместе с тем необходимость парного связывания узлов на протяжении установления многосторонней сессии обуславливает большее число пересылок команд, что может значительно удлинять фактическое время формирования сессии.

Анализ результатов

В работе проводится программная реализация предложенных алгоритмов, представленных выше с использованием имитационного моделирования и языка программирования Java. Моделируемая БСС, по сути, представляется при помощи многоагентной системы, разворачиваемой в рамках виртуальной машины JVM. Каждый узел БСС представляется при помощи некоторого специально созданного процесса операционной системы, управляемого с использованием данной виртуальной машины. При этом изолированность процессов обеспечивает автономность моделируемых узлов БСС и значительную ограниченность представления узлов о текущем состоянии других узлов сети. Также децентрализованный характер моделируемой БСС обеспечивается за счет возможности создании, удаления и управления неограниченным числом процессов операционной системы.

Для проведения моделирования используется инициализирующий конфигурационный файл с начальными параметрами моделирования, включающими, в частности, начальные количества и состав узлов моделируемой сети, характеристики программного и аппаратного обеспечения узлов и др. Используется иерархическая структура Java-классов с наследованием для различных ролей узлов БСС. Технологическая гибкость такой структуры позволяет с минимальными вычислительными затратами организовать достаточно безопасную и надежную передачу ролей между узлами БСС путем сериализации текущего состояния соответствующего экземпляра класса, а также бесшовную передачу на новый узел. После чего, десериализовав данный экземпляр, узел-получатель оказывается способным к дальнейшему использованию этой роли в сети. Кроме того, в процессе имитационного моделирования это позволяет использовать единый интерфейс для доступа к объектам классов ролей узлов и единым образом манипулировать этими объектами.

Ниже приведены результаты аналитического расчета и сравнения коммуникационной сложности алгоритма предложенного установления многосторонней сессии (A_H) и альтернативного алгоритма на основе кластеризации узлов (A_{CL}) [13, 14]. Данный показатель определяет сетевую нагрузку на коммуникационные каналы БСС в целом при формировании многосторонней сессии. Пусть величина *c* обозначает количество узлов БСС, участвующих в формировании многосторонней сессии. В расчетах величина *c* всегда превышает единицу. Показатель сложности *Compl* определяется количеством пересылок сообщений, непосредственно связанных с процессом установления многосторонней сессии.

При задании значений показателя *Compl* учитываются экземпляры сообщений, пересылаемые между двумя конкретными адресатами – узлом-отправителем и узлом-получателем. В общем случае ввиду непредопределенности сетевой топологии БСС и возможным наличием непрямых пересылок между двумя адресатами – пересылок в несколько хопов («прыжков») – каждая такая пересылка считается за одну пересылку вне зависимости от числа промежуточных узлов, участвующих в процессе пересылки. Поэтому для понимания реального числа хопов таких сообщений в сети в результирующих оценках коммуникационной сложности алгоритма необходимо вводить дополнительные

коэффициенты на основе среднего числа хопов на пересылку одного сообщения между узлом отправителем и узлом-получателем.

В качестве допущения принимаем тот факт, что в рамках моделирования оба анализируемых алгоритма работают в условиях стартовой активности всех узлов и их готовности организовать многостороннюю сессию. Также для большей корректности оценки широковещательные сообщения учитываются как аналогичные соответствующие множества однонаправленных сообщений, отправленных всем узлам сети. Кроме того, оценка производится в условиях однократного информационного обмена без каких-либо сбоев, задержек, ошибок и пропусков реакций на полученные сообщения. Отметим, что указанные допущения упрощают процедуру оценки алгоритмов, но не оказывают существенного влияния на результирующие оценки.

В соответствии со схемой алгоритма A_H, приведенной на рис. 1, его сложность вычисляется как $Compl(A_H) = 2 \cdot c \cdot (c-1)$, и поэтому сложность алгоритма является квадратичной и в асимптотическом выражении принимается равной $O(c^2)$. В соответствии со схемой на рис. 2 сложность алгоритма A_{CL} вычисляется как $Compl(A_{CL}) = 2 \cdot c^2 + 2 \cdot c - 4$, в результате чего в асимптотическом выражении она оказывается также равной $O(c^2)$. Таким образом, несмотря на сходный предельный характер коммуникационных расходов, тем не менее при ограниченном числе узлов, участвующих в создании многосторонней сессии в условиях дефицита коммуникационного ресурса или недостаточной стабильности беспроводных каналов, использование алгоритма A_H оказывается более предпочтительным.

Отметим, что помимо теоретического обоснования корректности и проверки работоспособности предложенных в работе алгоритмов, проведенной с использованием программной симуляции БСС в целях полноценного использования алгоритмов на практике, необходимо проведение комплексного всестороннего их анализа, тестирования и апробации. В частности, в дальнейшей работе необходимо запланировать эмпирическую проверку устойчивости работы предложенных алгоритмов в части не злонамеренных ошибок и сбоев, которые могут возникать в процессе установления многосторонней сессии между узами. В качестве примеров подобных тестов выделим следующие: внезапная потеря связи с одним из узлов в процессе установления сессии и потеря одного или нескольких подтверждений в процессе установления.

В целом подобные не являющиеся намеренными ошибки и сбои могут возникать в основном следствие коммуникационных проблем на сетевом уровне. Вместе с тем подобные ситуации могут являться результатом также и преднамеренных легитимных действий узлов БСС. Например, узлу может внезапно потребоваться отключиться от сети для проведения профилактики или перенастройки своего оборудования в сервисном режиме. Также узел может покинуть зону действия беспроводного сигнала из-за особенностей прикладных задач, на него наложенных. Альтернативной причиной может также быть потребность узла сменить свой идентификатор PAN ID и при необходимости присоединиться к другой БСС, функционирующей параллельно.

Кроме того, разработанные алгоритмы необходимо дополнительно тестировать на предмет фактического отсутствия тупиковых ситуаций, связанных с потерей синхронизации действий участников информационного обмена. На уровне теоретического анализа предложенных алгоритмов отсутствие подобных ситуаций проверено аналитически, однако эмпирическое оценивание позволит также подтвердить корректность программных реализаций этих алгоритмов. В частности, целесообразно применять метод проверки на модели (model checking), который позволяет сделать направленный автоматизированный перебор различных входных данных с проигрыванием различных вариантов состояний и цепочек действий узлов БСС [15].

Отметим также, что целесообразность применения метода проверки на модели обуславливается в особенности тем, что коммуникационный процесс, включающий вовлечение узлов, располагающихся в рамках заранее неизвестной сетевой топологии и несинхронизированных между собой по времени, формирует существенный недетерминизм

процесса управления сетью. И поэтому без перебора и проигрывания значительного числа тестовых сценариев с применением средств автоматизации это было бы затруднительно и не слишком эффективно с точки зрения результата такого тестирования и вовлекаемых ресурсов.

Заключение

В статье предложены два алгоритма для организации многосторонних сессий в самоорганизующихся БСС с ролевым управлением. Указанные алгоритмы служат основой формируемого в работе протокола децентрализованного управления БСС. В качестве дальнейших шагов в данном направлении предполагается исследование возможных уязвимостей и атак данного протокола, а также построение наборов логов функционирования на примере конкретной БСС с целью разработки программных средств обнаружения актуальных видов атак на такие виды сетей.

Исследование выполнено за счет гранта Российского научного фонда № 24-21-00486. URL: https://rscf.ru/project/24-21-00486/.

Список источников

1. Kaur S., Sharma S. Role of the Internet of Things in Smart Cities: A Review // 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). Greater Noida, India. 2023. P. 686–689. DOI: 10.1109/ICACITE57410.2023.10182986.

2. Singh H., Verma D. Approaches for Data Analysis in WSN // 11th International Conference on System Modeling & Advancement in Research Trends (SMART). Moradabad, India. 2022. P. 521–527. DOI: 10.1109/SMART55829.2022.10046819.

3. Eltahlawy A.M., Azer M.A. Using Blockchain Technology for the Internet Of Vehicles // International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC). Cairo, Egypt. 2021. P. 54–61. DOI: 10.1109/MIUCC52538.2021.9447622.

4. Sharma M., Gebali F., Elmiligi H., Rahman M. Network Security Evaluation Scheme for WSN in Cyber-physical Systems // IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). Vancouver, BC, Canada. 2018. P. 1145–1151. DOI: 10.1109/IEMCON.2018.8615051.

5. Ji S., Pei Q., Zeng Y., Yang C., Bu S.-p. An Automated Black-box Testing Approach for WSN Security Protocols // 2011 Seventh International Conference on Computational Intelligence and Security. Sanya, China. 2011. P. 693–697. DOI: 10.1109/CIS.2011.158.

6. Singh T., Vaid R., Sharma A. Security Issues in Blockchain Integrated WSN: Challenges and Concerns // International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES). Chennai, India. 2022. P. 1–5. DOI: 10.1109/ICSES55317.2022.9914006.

7. Badri N., Nasraoui L., Saidane L.A. Blockchain for WSN and IoT Applications // IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT). Hammamet, Tunisia. 2022. P. 543–548. DOI: 10.1109/SETIT54465.2022.9875746.

8. Aleksieva V., Valchanov H., Haka A., Dinev D. Model of Controlled Environment based on Blockchain and IoT // 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES). Plovdiv, Bulgaria. 2023. P. 1–4. DOI: 10.1109/CIEES58940.2023.10378795.

9. Desnitsky V., Meleshko A. Modeling and Analysis of Secure Blockchain-driven Self-organized Decentralized Wireless Sensor Networks for Attack Detection // International Russian Automation Conference (RusAutoCon). Sochi, Russian Federation. 2024.

10. Harsha K.M., James D. A Novel Approach to Aggregate and Secure Data in Wireless Sensor Networks // International Conference on Communication and Electronics Systems (ICCES). Coimbatore, India. 2019. P. 1665–1670. DOI: 10.1109/ICCES45898.2019.9002418.

11. Wang W., He G., Wan J. Research on Zigbee wireless communication technology // International Conference on Electrical and Control Engineering. Yichang, China. 2011. P. 1245–1249. DOI: 10.1109/ICECENG.2011.6057961.

12. Wang Z., Wen Q., Sun Y., Zhang H. A Fault Detection Scheme Based on Self-Clustering Nodes Sets for Wireless Sensor Networks // IEEE 12th International Conference on Computer and Information Technology. Chengdu, China. 2012. P. 921–925. DOI: 10.1109/CIT.2012.190.

13. Roughgarden T. Communication Complexity (for Algorithm Designers) // Foundations and Trends in Theoretical Computer Science Journal. 2016. Vol. 11. Number 3–4. P. 217–404. DOI: 10.1561/0400000076.

14. Kushilevitz E. Communication Complexity // Advances in Computers. Elsevier. 1997. Vol. 44. P. 331–360. DOI: 10.1016/S0065-2458(08)60342-3.

15. Chen W., Xiao W. Model checking and analyzing the security protocol for wireless sensor networks // Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. Harbin, China. 2011. P. 4093–4096. DOI: 10.1109/EMEIT.2011.6023953.

References

1. Kaur S., Sharma S. Role of the Internet of Things in Smart Cities: A Review // 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). Greater Noida, India. 2023. P. 686–689. DOI: 10.1109/ICACITE57410.2023.10182986.

2. Singh H., Verma D. Approaches for Data Analysis in WSN // 11th International Conference on System Modeling & Advancement in Research Trends (SMART). Moradabad, India. 2022. P. 521–527. DOI: 10.1109/SMART55829.2022.10046819.

3. Eltahlawy A.M., Azer M.A. Using Blockchain Technology for the Internet Of Vehicles // International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC). Cairo, Egypt. 2021. P. 54–61. DOI: 10.1109/MIUCC52538.2021.9447622.

4. Sharma M., Gebali F., Elmiligi H., Rahman M. Network Security Evaluation Scheme for WSN in Cyber-physical Systems // IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). Vancouver, BC, Canada. 2018. P. 1145–1151. DOI: 10.1109/IEMCON.2018.8615051.

5. Ji S., Pei Q., Zeng Y., Yang C., Bu S.-p. An Automated Black-box Testing Approach for WSN Security Protocols // 2011 Seventh International Conference on Computational Intelligence and Security. Sanya, China. 2011. P. 693–697. DOI: 10.1109/CIS.2011.158.

6. Singh T., Vaid R., Sharma A. Security Issues in Blockchain Integrated WSN: Challenges and Concerns // International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES). Chennai, India. 2022. P. 1–5. DOI: 10.1109/ICSES55317.2022.9914006.

7. Badri N., Nasraoui L., Saidane L.A. Blockchain for WSN and IoT Applications // IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT). Hammamet, Tunisia. 2022. P. 543–548. DOI: 10.1109/SETIT54465.2022.9875746.

8. Aleksieva V., Valchanov H., Haka A., Dinev D. Model of Controlled Environment based on Blockchain and IoT // 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES). Plovdiv, Bulgaria. 2023. P. 1–4. DOI: 10.1109/CIEES58940.2023.10378795.

9. Desnitsky V., Meleshko A. Modeling and Analysis of Secure Blockchain-driven Self-organized Decentralized Wireless Sensor Networks for Attack Detection // International Russian Automation Conference (RusAutoCon). Sochi, Russian Federation. 2024.

10. Harsha K.M., James D. A Novel Approach to Aggregate and Secure Data in Wireless Sensor Networks // International Conference on Communication and Electronics Systems (ICCES). Coimbatore, India. 2019. P. 1665–1670. DOI: 10.1109/ICCES45898.2019.9002418.

11. Wang W., He G., Wan J. Research on Zigbee wireless communication technology // International Conference on Electrical and Control Engineering. Yichang, China. 2011. P. 1245–1249. DOI: 10.1109/ICECENG.2011.6057961.

12. Wang Z., Wen Q., Sun Y., Zhang H. A Fault Detection Scheme Based on Self-Clustering Nodes Sets for Wireless Sensor Networks // IEEE 12th International Conference on Computer and Information Technology. Chengdu, China. 2012. P. 921–925. DOI: 10.1109/CIT.2012.190.

13. Roughgarden T. Communication Complexity (for Algorithm Designers) // Foundations and Trends in Theoretical Computer Science Journal. 2016. Vol. 11. Number 3–4. P. 217–404. DOI: 10.1561/0400000076.

14. Kushilevitz E. Communication Complexity // Advances in Computers. Elsevier. 1997. Vol. 44. P. 331–360. DOI: 10.1016/S0065-2458(08)60342-3.

15. Chen W., Xiao W. Model checking and analyzing the security protocol for wireless sensor networks // Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. Harbin, China. 2011. P. 4093–4096. DOI: 10.1109/EMEIT.2011.6023953.

Информация о статье:
Статья поступила в редакцию: 24.08.2024; одобрена после рецензирования: 24.09.2024;
принята к публикации: 30.09.2024
Information about the article:
The article was submitted to the editorial office: 24.08.2024; approved after review: 24.09.2024;
accepted for publication: 30.09.2024

Информация об авторе:
Десницкий Василий Алексеевич, старший научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук (199178, Санкт-Петербург, 14-я линия Васильевского о-ва, д. 39), кандидат технических наук, доцент, e-mail: desnitsky@comsec.spb.ru, https://orcid.org/0000-0002-3748-5414, SPIN-код: 6526-5812

Information about the authors:
Desnitsky Vasily A., senior researcher at the Saint-Petersburg Federal research center of the Russian academy of sciences (199178, Saint-Petersburg, 14 line of Vasilievsky island, 39), candidate of technical sciences, associate professor, e-mail: desnitsky@comsec.spb.ru, https://orcid.org/0000-0002-3748-5414, SPIN: 6526-5812