Научная статья
УДК 004.056.5; DOI: 10.61260/2218-13X-2025-3-30-41

МОДЕЛИРОВАНИЕ И АНАЛИЗ ЗАЩИЩЕННЫХ САМООРГАНИЗУЮЩИХСЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

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

Аннотация. В связи с развитием и совершенствованием беспроводных сенсорных сетей и их распространением в различных практических областях возникает потребность в большем динамизме и изменчивости таких сетей. Наблюдается все возрастающая тенденция к повышению самоорганизуемости и децентрализации таких сетей, и такие сети становятся более настраиваемыми под нужды конкретного потребителя и адаптивными в зависимости от текущих условий функционирования. Появляются и совершенствуются протоколы распределенного управления такими сетями со все большим внедрением сетей с ячеистой токологией (mesh-сетей). В рамках таких сетей узлы могут менять свое географическое положение, выстраивать новые коммуникационные каналы в зависимости от текущей пропускной способности и надежности соединения, выполнять различные служебные и прикладные функции. Однако, такое развитие беспроводных сенсорных сетей формирует новые угрозы информационной безопасности, непосредственно связанные со злонамеренной эксплуатацией свойств самоорганизации и децентрализации. Потенциальный атакующий оказывается способным осуществлять атаки подмены и модификации данных от сенсоров, flooding-воздействия, атаки истощения энергоресурсов, атаки нарушения процессов маршрутизации в сети и др. с большей вариативностью и потенциально более высоким эффектом. Настоящая работа ориентирована на моделирование и анализ такого вида атак, и основной акцент сделан на исследование возможностей имитационного моделирования с учетом влияния свойств самоорганизации и децентрализации сетей и атак, эксплуатирующих эти свойства. В статье предлагается подход к имитационному моделированию самоорганизующихся беспроводных сенсорных сетей с ролевым управлением. Проведенные эксперименты на модели фрагмента беспроводных сенсорных сетей для системы взаимосвязанных беспилотных летательных аппаратов подтверждают корректность данного подхода и его выполнимость на практике.

Ключевые слова: беспроводная сенсорная сеть, моделирование, безопасность, атака

Для цитирования: Десницкий В.А. Моделирование и анализ защищенных самоорганизующихся беспроводных сенсорных сетей // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2025. № 3. С. 30–41. DOI: 10.61260/2218-13X-2025-3-30-41.

Scientific article

MODELING AND ANALYSIS OF SECURE SELF-ORGANIZED WIRELESS SENSOR NETWORKS

✉**Desnitsky Vasily A.**
St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg, Russia
✉***desnitsky@comsec.spb.ru***

Abstract. Due to the development and improvement of wireless sensor networks and their active implementation in various areas, there is a need to increase the dynamics and variability of such networks. Today, there is a clear trend towards an increase in the level of self-organization and decentralization, due to which networks adapt to user needs and operating conditions.

For this purpose, distributed control protocols are created and improved, networks with a cellular topology (mesh networks) are actively introduced. Nodes of such networks are able to move, create new data transmission paths based on the current state of communication channels and device resources, and perform various auxiliary and applied tasks. However, the progress of wireless sensor networks gives rise to additional information security risks associated with the use of self-organization and decentralization features by intruders. Attacks on such infrastructure include manipulation of sensor data, flood attacks that deplete equipment resources, failures in signal transmission routes, and other impacts that are characterized by increased variability and efficiency. This article comprises modeling and studying this type of threats, with special attention paid to simulation analysis methods taking into account the specificity properties of self-organization and decentralization of networks and attacks that exploit them. The proposed approach is built on role-based management in the simulation modeling of self-organizing wireless sensor networks. The results of experiments on a model of a network fragment for a group of connected unmanned aerial vehicles confirmed the validity and practicality of the proposed method.

Keywords: wireless sensor network, modeling, security, attack

For citation: Desnitsky V.A. Modeling and analysis of secure self-organized wireless sensor networks // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 3. P. 30–41. DOI: 10.61260/2218-13X-2025-3-30-41.

Введение

В настоящее время все большее распространение получают беспроводные сенсорные сети (БСС), являющиеся элементами различных промышленных, транспортных и других инфраструктур, в том числе в рамках индустриального интернета вещей. В общем случае БСС представляет собой множество взаимосвязанных маломощных сенсоров и узлов, объединённых посредством беспроводных каналов связи и предназначенных для сбора и передачи данных об окружающей среде или некотором контролируемом процессе на централизованные сетевые хосты или облачные структуры. При этом, как правило, узлы БСС характеризуются достаточно малыми физическими размерами, автономностью узлов и их низким энергопотреблением, в том числе от возобновляемых батарей. Наблюдается стремительный рост числа устройств, собирающих данные при помощи физических сенсоров и имеющих подключения к глобальной сети Интернет с использованием беспроводных технологий. Также благодаря беспроводным сетям становится возможным получать данные в режиме реального времени от устройств, связанных с различными технологическими процессами крупного предприятия. Это позволяет улучшить контроль качества продукции, сократить использование критически важных ресурсов и финансовых затрат.

При этом все большую роль в рамках индустриальных инфраструктур играют самоорганизация и децентрализация таких сетей. Самоорганизация представляет способность сети самостоятельно адаптироваться и организовывать свою структуру с минимальным централизованным управлением и заранее задаваемым конфигурационными настройками [1]. Самоорганизующаяся сеть предполагает динамический состав узлов и изменяемую во времени сетевую топологию. В частности, в процессе функционирования возможны спонтанный уход из сети или добавление некоторого нового узла, а также установление соответствующих беспроводных сетевых каналов в зависимости от ряда значимых факторов. К таким факторам можно отнести пространственное расположение узлов, мощность их передатчиков, наличие препятствий распространения сигнала, наличие шумов, загруженность уже имеющихся каналов БСС, разновидности узлов, режимы их работы и др.

Децентрализация в БСС предполагает отсутствие или минимизацию обязанностей единого центра управления и обработки данных. Вместе с тем появляется возможность

наложения части служебных и прикладных функций, которые обычно выполняются централизовано, на отдельные заранее не фиксированные узлы сети. В частности, перераспределяться могут, как функции сбора первичных данных в сети, так и функции их агрегации, обработки и последующего анализа, а также функции принятия операционных решений в сети [2]. В частности за счет самоорганизации оказывается возможным выстраивание такого распределения функций по узлам, чтобы оптимизировать сбор и накопление нужных данных с учетом связей между соседними узлами.

Конкретными примерами таких сетей являются самоорганизующиеся беспроводные сенсорные сети на основе протокола ZigBee, в том числе в рамках следующих систем:

– системы умных домов для управления климатическими характеристиками, освещением, управлением бытовой техникой и др., как например, устройства серий IKEA Trådfri [3], Xiaomi Mi Home [4] и др., использующие протокол ZigBee. Преимущества в использовании самоорганизации и децентрализации в таких сетях включают не фиксированность точек установки узлов сети, включая возможность перемещения встраиваемых в умную мебель узлов и сенсоров с возможностью динамического выстраивания новых каналов связи между узлами. Преимуществами также являются универсальность и независимость от конкретного сервис-провайдера, легкая масштабируемость и переносимость всей инфраструктуры в другие помещения;

– системы контроля потребления энергоресурсов, включающие умные счетчики электричества, воды, газа, подключающиеся к единому хабу на этаже или в частном доме для дальнейшей передачи компаниям-поставщикам [5]. Преимущества в использовании самоорганизации и децентрализации в таких сетях включают также возможность легкой замены узлов и резервирования узлов для контроля согласованности показаний;

– автоматизированные системы мониторинга защищенности и диагностики оборудования, дистанционного управления производственными станками и роботами на промышленных предприятиях [6]. Преимущества в использовании самоорганизации и децентрализации в таких сетях включают повышение надежности и отказоустойчивости в таких инфраструктурах за счет возможности динамической передачи функций узла со сбоем на другие доступные узлы сети. Выход из строя узла, выполняющего определенную роль, не приведет к полной потере управляемости сети и выполнению возложенных на нее задач. При гибкой настройке режимов работы узлов возможно также повышение энергоэффективности оперативного автоматического высвобождения узлов, наиболее уязвимых с точки зрения возобновления их энергоресурса;

– распределенные транспортные системы, в том числе системы управления беспилотными транспортными средствами [7]. К преимуществам в использовании самоорганизации и децентрализации в таких сетях можно отнести возможности по снижению энергопотребления и повышению отказоустойчивости, в том числе продолжение миссии в целом в условиях потери части средств и с учетом изменяющейся окружающей обстановки.

Таким образом, все три упомянутых области применения подтверждают актуальность накладываемых требований к самоорганизации и децентрализации беспроводных сенсорных сетей в отличающихся прикладных задачах.

Анализ литературы

В работе [8] анализируется свойство самоорганизации, которое присуще распределенным информационным системам, где компоненты системы управляются при помощи локальных правил, обеспечивающих желаемое глобальное поведение всей системы. В частности, такое управление может способствовать улучшению процессов обработки информации и коммуникации в таких сетях, улучшению энергопотребления и плотности покрытия сети, снижению задержек и устранению конфликтов и сбоев в работе устройств [9]. В работе [1] рассматривают самоорганизацию БСС в связке с интеллектуальностью,

автономностью, адаптивностью и узловой кооперацией для решения задач мониторинга нагрузки сети, энергопотребления и эффективности передачи данных. В контексте обеспечения информационной безопасности таких самоорганизующихся и самоконфигурирующихся сетей в работе [10] авторы предлагают концепцию для обнаружения вторжений на основе репутационной системы и распределенных агентов, в том числе с поддержкой самовосстановления за счет идентификации и изоляции узлов с выявленными отклонениями в сетевом и функциональном поведении.

Что касается вопросов децентрализации применительно к БСС, то в существующей литературе децентрализация в контексте киберфизической безопасности исследуется в основном в части децентрализованных механизмов обнаружения атак в БСС [11–12]. В частности, в работе [11] в сеть вводится специальный узел-монитор, который предназначен для сбора сообщений от других узлов сети, в том числе его соседей, и последующего их анализа с использованием семи сформулированных правил. Кроме того, применяются специализированные механизмы повышения информационной безопасности за счет децентрализации, как, например, исследование децентрализованной аутентификации в БСС [13] и децентрализованного механизма восстановления сети после атаки [14].

В отличие от существующих опубликованных работ в данной предметной области предлагаемое в настоящей работе моделирование ориентировано на возможность исследования и анализ атак, эксплуатирующих свойства самоорганизации и децентрализации сети с учетом ролей узлов, участвующих в процессе сбора и обработки данных, что необходимо для обнаружения атак. Кроме того, в рамках предлагаемого решения отсутствует необходимость интеграции с какой-либо внешней специализированной средой моделирования, что определяет повышенную настраиваимость процесса моделирования атак и оптимизации ресурсов узлов сети.

В результате того, что БСС получает свойства самоорганизации и децентрализации, она оказывается подверженной дополнительным атакам, непосредственно связанным с эксплуатацией этих свойств нарушителем. Например, отсутствие фиксированного распределения обязанностей между узами может привести к тому, что атакующий, злоупотребляя особенностями процесса такого распределения, может форсированно перетянуть некоторую важную роль на контролируемый им узел. В частности, в случае принятия им, к примеру, роли по логированию событий в сети, узел способен собирать всю полноту информации о функционировании сети и использовать ее как основу для последующих атак. Отметим, что в случае, если сеть не является самоорганизующейся и децентрализованной, такая атака была бы крайне трудно осуществимой.

К настоящему времени опубликовано обилие работ, исследующих атаки на стационарные БСС и другие виды сетей без учета этих свойств. К таким атакам относится известные виды атак на БСС, направленные на нарушение процессов маршрутизации трафика и идентификации узлов. Примерами таких атак являются wormhole-атаки [15–16], sinkhole-атаки [17], атаки типа hello-flood [18], vampire-атаки [19], Sybil-атаки [20] и др. Вместе с тем атаки, относящиеся к данным разновидностям, но учитывающие и эксплуатирующие свойства самоорганизации и децентрализации, оказываются мало изучены. Однако в общем случае подобные усовершенствованные атаки могут быть особенно опасными, поскольку эксплуатация самоорганизации и децентрализации позволяет нарушителю повысить скрытность атаки и ее эффект, а также, возможно, затрачиваемые на ее осуществление ресурсы.

Например, в случае БСС в области мониторинга объектов умного промышленного предприятия атака по внедрению нарушителем нового ложного узла для сбора данных и/или спуфинга в условиях фиксированной сетевой топологии и фиксированного состава узлов с большой вероятностью будет обнаружена на основе системы обнаружения вторжений с простой системой правил, как минимум, в качестве аномалии. Тогда как в условиях самоорганизации и децентрализации сети, например, в случае БСС в рамках роя беспилотных транспортных средств, когда изменение состава узлов и каналов связи легитимным образом

меняется в процессе функционирования, для обнаружения такой атаки нужно было бы учитывать значительно больше специфичных данных и событий из трафика. Предположительно, в последнем случае качество обнаружения такой атаки не будет настолько высоким, как в случае стационарной сети. Кроме того, такие модифицированные атаки обладают большей вариативностью и могут быть более быстрыми.

Поэтому возникает проблема повышения эффективности обнаружения атак, учитывающих и эксплуатирующих свойства самоорганизации и децентрализации. В особенности это касается прикладных сценариев, отличающихся повышенным динамизмом, как на уровне структуры БСС, так и в части программного поведения. Ввиду организационно-технической сложности моделирования и проведения экспериментов по обнаружению таких атак и оценки качества их обнаружения на реальных сетях с использованием полноценного физического оборудования возникает потребность в альтернативных способах моделирования, позволяющих снизить такую сложность. Поэтому в данной работе предлагается подход к имитационному моделированию самоорганизующихся децентрализованных БСС, позволяющий обнаруживать такие атаки более эффективно.

Основной вклад данной статьи включает подход к построению имитационной модели [21–22] самоорганизующейся децентрализованной БСС и атак, эксплуатирующих свойства самоорганизации и децентрализации, а также апробацию подхода на примере модели сети беспилотных транспортных средств. К элементам новизны данной работы, отличающей ее от альтернативных подходов и решений в данной предметной области, во-первых, относятся использование комбинированного подхода к моделированию на основе полнофункционального моделирования на физических узлах сети и имитационной компоненты при помощи скриптов на языке Python, оптимизируемых под ограничения программно-аппаратной платформы узлов. Во-вторых, новизна включает возможность моделирования атак, учитывающих ролевое представление узлов, участвующих в процессе обеспечения функций обнаружения атак.

Подход к моделированию

В рамках предложенного подхода самоорганизующаяся децентрализованная БСС представляется в виде кортежа $\left\{\left(n_i, \left\{r_i^k\right\}_{k\in K}\right)\right\}_{i\in I}$, где $n_i \in N$, N – множество узлов БСС, $r_i^k \in R$, R – множество ролей узлов, I – множество индексов узлов сети, $K \subseteq 2^R$, K – подмножество множества всех ролей R. Значения множества R задаются в соответствии с табл. 1.

Таблица 1

Роли узлов самоорганизующейся децентрализованной БСС

Роль узла	Функции роли узла
Сборщик данных	Узел осуществляет сбор данных со своих сенсоров, а также некоторых операционных данных своего функционирования, в том числе различные статистические показатели сенсоров, ретрансляций сообщений, периодов пребывания в режиме сна и бодрствования, активности узлов-соседей и т.п. Узел способен проводить их небольшую, не требующую значительных вычислительных ресурсов предобработку. Кроме того, узел может выборочно передавать собранные им данные на узел с ролью хранитель, а также по запросу от других узлов, в том числе узлов-соседей
Хранитель данных	Узел ответственен за получение данных от других узлов для их сохранения в рамках модуля защищенного хранения. В общем случае фактическое хранение может быть распределено между несколькими узлами, тогда как узел-хранитель отвечает за организацию такого распределенного хранилища и обеспечение согласованности данных в нем. В частности, хранитель поддерживает инфраструктуру локального блокчейна, во-первых, для обеспечения неизменности данных сети и, во-вторых, для предоставления возможности запрашиваемых данных от некоторого узла с предоставлением доказательства их целостности и неизменности

Роль узла	Функции роли узла
Обработчик данных	Узел обработчик данных в сети ответственен за преобразования данных, необходимых для обнаружения атак и аномалий, в том числе за нормализацию, фильтрацию и агрегацию данных. В общем случае обрабатываемые данные берутся из хранилища, и результаты обработки помещаются обратно в хранилище
Анализатор данных	Анализатор данных в первую очередь предназначен для выявления атак и аномалий в БСС на основе доступных данных о функционировании сети. В частности, применяются методы обнаружения на основе правил, статистик, а также облегченных методах машинного обучения и нейронных сетях, заранее обученных и валидированных на тестовых выборках данных

Автор отмечает, что каждый из узлов может одновременно принимать на себя одну или несколько ролей, каждая из которых предполагает выполнение им определенных функций по сбору, обработке, хранению данных в сети и их анализу. Блокчейн, обеспечивающий защищенное хранение прикладных и системных данных, включает использование смарт-контрактов. Смарт-контракты позволяют автоматизировать процессы взаимодействия между узлами сети и повысить уровень защищенности процессов функционирования БСС. В табл. 2 приведены использования смарт-контрактов для каждого типа узлов сети.

Таблица 2

Использование смарт-контрактов для различных типов узлов БСС

Роль узла	Использование смарт-контрактов
Сборщик данных	– проверка узлом-сборщиком отправляемых данных на аномальность. Перед передачей другим участникам сети, в том числе на узел-хранитель при помощи контракта, возможно проверить согласованность данных от сенсора с другими имеющимися в сети сенсорами, к примеру, применяя машинное обучение; – регистрация действий и событий узлов с учетом совместного формирования таких логов несколькими узлами сети; – возможность обеспечения конфиденциальности данных за счет их шифрования перед сохранением, которое осуществляется узлами-источниками этих данных
Хранитель данных	– возможность обеспечения конфиденциальности данных за счет их шифрования перед сохранением, которое осуществляется узлами-источниками этих данных
Обработчик данных	– с использованием смарт-контрактов осуществляется совместное согласование и подтверждение завершения операций обработки данных в сети. Успешное завершение обработки сопровождается соответствующей записью в блокчейне
Анализатор данных	– совместное управление процессами обнаружения атак и аномалий в данных и событиях от нескольких узлов сети – совместное и согласованное реагирование на найденные атаки и аномалии

В рамках имитационного моделирования для каждого узла декларативно задаются стартовые значения параметров моделирования, которые включают (T_i, T_i^d) – периодичность опроса датчиков в форме математического ожидания и дисперсии в соответствии с нормальным распределением. Аналогичным образом задается способ генерации сообщений для каждого узла сети. При этом выбор узла для коммуникации на очередном шаге работы модели производится псевдослучайным образом из имеющихся узлов-соседей, находящихся в настоящий момент в пределах видимости радиосигнала следующим образом:

$$p_i(n_j) = \frac{\sqrt{d(n_i, n_j)}}{\sum_{n_k \in N} \sqrt{d(n_i, n_k)}},$$

где функция d задает линейное расстояние между двумя узлами (n_i и n_j), множество N_i задает множество текущих соседей узла n_i, тогда как $p_i(n_j)$ позволяет задать вероятность выбора узлом n_i конкретного узла n_j для коммуникации.

Максимальная дальность связи между двумя узлами задается с учетом пространственного расположения узлов моделируемой сети с использованием двумерного равномерного распределения для непрерывной случайной величины по следующей формуле:

$$(\frac{1}{x_1 - x_0}, \frac{1}{y_1 - y_0}),$$

где векторы (x_0, y_0) и (x_1, y_1) задают верхнюю левую и нижнюю правую точки прямоугольника, в рамках которого производится моделирование.

Реализация и дискуссия

Моделирование проводится на примере фрагмента БСС, состоящем из четырех основных узлов, имеющих роли сборщика данных, хранителя, обработчика и анализатора данных соответственно. Каждый узел представляет устройство в рамках спонтанно формируемой системы взаимодействующих беспилотных летательных аппаратов (БПЛА), способных обмениваться сообщениями в целях выполнения совместных миссий и избегания коллизий и конфликтов. Примером миссий является осуществление мониторинга физических параметров воздушной среды. Схема моделируемой сети приведена на рисунке – показана сетевая топологи БСС с узлами n(..), носителями которых являются БПЛА UAV_1, UAV_2, UAV_3 и UAV_4, и ролями: c – сборщик данных, k – хранитель данных, p – обработчик данных, a – анализатор данных, осуществляющим выявление аномалий и атак. К узлам прикреплены сенсоры c_1, c_2, c_3 и c_4, а также компонент предварительной обработки PreC, компонент организации блокчейна BC для защищенного хранения данных, компонент обработки PC, а также компонент анализа данных AD.

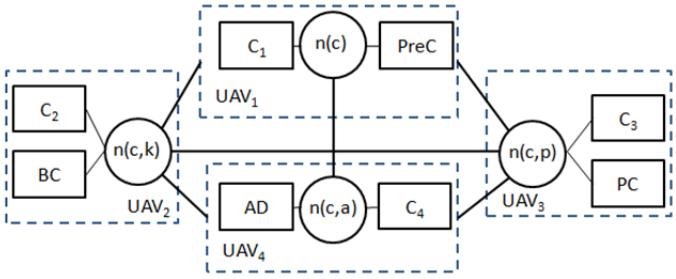

Рис. **Схема моделируемой самоорганизующейся децентрализованной БСС в рамках системы взаимодействующих БПЛА**

Реализация имитационной модели осуществляется на основе четыре скриптов на языке Python, а также конфигурационного файла в формате JSON, определяющего стартовые параметры узлов и данные эксперимента, включая продолжительность моделирования, интенсивность потока сообщений, измерений сенсоров и команд. Каждый скрипт ответственен за работу узла с определенной ролью. В качестве сенсоров, устанавливаемых на узлах, задается комбинированный сенсор влажности и температуры окружающего пространства. Данные снабжаются метками времени регистрации такого события. В рамках данной реализации нормальная активность узлов ограничивается, действиями, представленными в табл. 3.

Таблица 3

Роли узлов самоорганизующейся децентрализованной БСС

Роль узла	Реализуемая активность
Сборщик данных	– сбор данных о местоположении БПЛА, являющегося носителем узла БСС; – сбор данных о влажности и температуре среды, снабженных метками времени; – сбор данных потока команд, направляемых БПЛА оператором; – сбор прикладных сообщений, поступающих от других узлов БСС
Хранитель данных	– реализация локального приватного блокчейна [23], включающего четыре узла БСС и учитывающего ограничения вычислительной мощности узлов, энергоресурсов и пропускной способности каналов связи
Обработчик данных	– для удобства и универсальности представления показаний сенсоров применяется нормализация на основе метода оценки z-scores; – рамках текущей реализации сбор команд и сообщений от других узлов осуществляется на основе идентификаторов конкретных команд без использования численных значений их аргументов (как, например, координат точки, в которую БПЛА должен переместиться)
Анализатор данных	– реализуемые функции безопасности ограничиваются применение метода трех сигм для проверки согласованности и аномальности данных от сенсоров. Согласованность поступающих команд проверяется на основе валидации блоков блокчейна, включающих команды и логи от устройств-источников и устройств-получателей; – применяется также анализ корреляционных зависимостей между сенсорами от разных узлов с течением времени. В данной реализации фактически это парные сравнения серий показаний от двух близлежащих узлов за заданный промежуток времени; – при выявлении отклонения генерируется инцидент об аномальности анализируемых данных

В рамках эксперимента проведено моделирование атаки перехвата роли (role hijacking), включающей несанкционированное получение скомпрометированным узлом некоторой роли, например, роли обработчика. В случае перехвата роли обработчика конечной целью атаки является внесение модификаций в обрабатываемые данные, например, сокрытие следов других атак из обрабатываемых логов и внесение изменений в показания сенсоров сети. Особенностью такой атаки является то, что она включает эксплуатацию свойства самоорганизации сети, когда решение о передаче некоторой роли другому узлу применяется на основе оптимизации показателей функционирования сети, в том числе для снижения среднего суммарного числа хопов пакетов данных, проходящих по сети за заданный промежуток времени. Злонамеренное использованием свойств децентрализации БСС позволяет перехватить атакующим нужную роль, получив от предыдущего узла соответствующий программный контекст и продолжить ее выполнение под своим контролем.

Проведенный эксперимент по моделированию нормальной активности сети, а также атаки перехвата роли узла-обработчика, подтверждают выполнимость данного подхода и его практическую реализуемость. Кроме того, эксперимент подтвердил возможность моделирования атаки на примере атаки перехвата роли и возможность ее обнаружения в качестве аномалии при помощи выявления отклонений в показаниях сенсоров.

К ограничениям используемого имитационного моделирования относится то, что при генерации сообщения узлами сети осуществляются лишь базовые операции по считыванию данных с сенсоров, их передачи по сети, обработке, хранению и анализу на предмет выявления аномалий. Также к ограничениям модели можно отнести то, что, несмотря на трехмерный характер моделируемого перемещения БПЛА, для простоты локализация местоположения узлов сети ограничиваются только двухмерными векторами координат узла

в проекции на поверхность земли. Еще одним ограничением текущей реализации модели является то, что роли хранителя, обработчика и анализатора данных представлены в виде одного узла для каждого из ролей, тогда как роль сборщика данных параллельно выполняют все четыре узла сети.

Заключение

В работе представлен подход к имитационному моделированию самоорганизующихся децентрализованных БСС с ролевым управлением, ориентированный на моделирование и анализ атак, эксплуатирующих свойства самоорганизации и децентрализации сети. Подход апробирован на примере модели фрагмента БСС в области взаимосвязанных беспилотных транспортных средств с четырьмя узлами и моделированием атаки перехвата роли. Результаты экспериментов подтвердили корректность и выполнимость подхода на практике. В качестве дальнейших исследований по данному направлению предполагаются моделирование и эксперименты по сравнению других видов атак на такие сети, а также ранжирование атак по степени их критичности для целевой системы.

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

Список источников

1. Li N., Liu X. Research on Self-Organization and Adaptive Strategy of the Internet of Things Sensor Networks // IEEE Access. 2024. Vol. 12. P. 66569–66579. DOI: 10.1109/ACCESS.2024.3399537.

2. Aldawsari H. A blockchain-based approach for secure energy-efficient IoT-based Wireless Sensor Networks for smart cities // Alexandria Engineering Journal. 2025. Vol. 126. P. 1–7. DOI: 10.1016/j.aej.2025.04.052.

3. Sultanow E., Chircu A. A Review of IoT Technologies, Standards, Tools, Frameworks and Platforms // The Internet of Things in the Industrial Sector: Security and Device Connectivity, Smart Environments, and Industry 4.0. 2019. P. 3–34. DOI: 10.1007/978-3-030-24892-5_1.

4. Forensic Analysis of the Xiaomi Mi Smart Sensor Set / J.M. Castelo Gómez [et al.] // Forensic Science International: Digital Investigation. 2022. Vol. 42–43. P. 301451. DOI: 10.1016/j.fsidi.2022.301451.

5. Abdalzaher M.S., Fouda M.M., Ibrahem M.I. Data Privacy Preservation and Security in Smart Metering Systems // Energies. 2022. Vol. 15. № 19. P. 7419. DOI: 10.3390/en15197419.

6. Sharma R. Enhancing Industrial Automation and Safety Through Real-Time Monitoring and Control Systems // International Journal on Smart & Sustainable Intelligent Computing. 2024. Vol. 1. № 2. P. 1–20. DOI: 10.63503/j.ijssic.2024.30.

7. Data Communication for Wireless Mobile Nodes in Intelligent Transportation Systems / K.N. Qureshi [et al.] // Microprocessors and Microsystems. 2022. Vol. 90. P. 104501. DOI: 10.1016/j.micpro.2022.104501.

8. Mills K. A Brief Survey of Self-Organization in Wireless Sensor Networks: Research Articles // Wireless Communications and Mobile Computing. 2007. Vol. 7. P. 823–834. DOI: 10.1002/wcm.499.

9. Khanna R. Evolutionary Approach to Efficient Provisioning and Self-organization in Wireless Sensor Networks (WSN). Oregon State University, 2016.

10. Improving Security in WMNs With Reputation Systems and Self-Organizing Maps / Z. Bankovic [et al.] // Journal of Network and Computer Applications. 2011. Vol. 34. Iss. 2. P. 455–463. DOI: 10.1016/j.jnca.2010.03.023.

11. Decentralized Intrusion Detection in Wireless Sensor Networks / A.P. Silva [et al.] // Proceedings. 2005. P. 16–23. DOI: 10.1145/1089761.1089765.

12. Chatzigiannakis I., Strikos A. A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks // 2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007), Patras, Greece. 2007. P. 1408–1411. DOI: 10.1109/EFTA.2007.4416949.

13. Blockchain-powered defense: Securing WSN against DDoS attacks with decentralized authentication / A. Suman [et al.] // Wireless Ad-hoc and Sensor Networks. CRC Press. 2024. P. 318–339.

14. Lee C., Suzuki J. SWAT: A Decentralized Self-Healing Mechanism for Wormhole Attacks in Wireless Sensor Networks // Handbook on Sensor Networks. World Scientific Publishing Co., 2010. P. 511–532. DOI: 10.1142/9789812837318_0021.

15. Energy Optimized Security Against Wormhole Attack in IoT-Based Wireless Sensor Networks / H. Shahid [et al.] // Computers, Materials and Continua. 2021. Vol. 68. Iss. 2. P. 1967–1981. DOI: 10.32604/cmc.2021.015259.

16. Wormhole Attack Mitigation Strategies and Their Impact on Wireless Sensor Network Performance: A Literature Survey / H. Shahid [et al.] // International Journal of Communication Systems. 2022. Vol. 35. DOI: 10.1002/dac.5311.

17. An Efficient Intrusion Detection Framework for Mitigating Blackhole and Sinkhole Attacks in Healthcare Wireless Sensor Networks / J.L. Webber [et al.] // Computers and Electrical Engineering. 2023. Vol. 111, Part B. P. 108964. DOI: 10.1016/j.compeleceng.2023.108964.

18. Detection of Hello Flood Attacks Using Fuzzy-Based Energy-Efficient Clustering Algorithm for Wireless Sensor Networks / S. Radhika [et al.] // Electronics. 2023. Vol. 12. № 1. P. 123. DOI: 10.3390/electronics12010123.

19. Arunachalam R., Ruby Kanmani E.D. Detection and Mitigation of Vampire Attacks with Secure Routing in WSN Using Weighted RNN and Optimal Path Selection // Computers & Security. 2024. Vol. 145. P. 103991. DOI: 10.1016/j.cose.2024.103991.

20. Almesaeed R., Al-Salem E. Sybil Attack Detection Scheme Based on Channel Profile and Power Regulations in Wireless Sensor Networks // Wireless Networks. 2022. Vol. 28. P. 1361–1374. DOI: 10.1007/s11276-021-02871-0.

21. Nayyar A., Singh R. A Comprehensive Review of Simulation Tools for Wireless Sensor Networks (WSNs) // Journal of Wireless Networking and Communications. 2015. Vol. 5. № 1. P. 19–47. DOI: 10.5923/j.jwnc.20150501.03.

22. Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey / G.H. Adday [et al.] // IEEE Access. 2024. Vol. 12. P. 22938–22977. DOI: 10.1109/ACCESS.2024.3362889.

23. A Secure Framework for Data Sharing in Private Blockchain-Based WBANs / L. Xiao [et al.] // IEEE Access. 2020. Vol. 8. P. 153956–153968. DOI: 10.1109/ACCESS.2020.3018119.

References

1. Li N., Liu X. Research on Self-Organization and Adaptive Strategy of the Internet of Things Sensor Networks // IEEE Access. 2024. Vol. 12. P. 66569–66579. DOI: 10.1109/ACCESS.2024.3399537.

2. Aldawsari H. A blockchain-based approach for secure energy-efficient IoT-based Wireless Sensor Networks for smart cities // Alexandria Engineering Journal. 2025. Vol. 126. P. 1–7. DOI: 10.1016/j.aej.2025.04.052.

3. Sultanow E., Chircu A. A Review of IoT Technologies, Standards, Tools, Frameworks and Platforms // The Internet of Things in the Industrial Sector: Security and Device Connectivity, Smart Environments, and Industry 4.0. 2019. P. 3–34. DOI: 10.1007/978-3-030-24892-5_1.

4. Forensic Analysis of the Xiaomi Mi Smart Sensor Set / J.M. Castelo Gómez [et al.] // Forensic Science International: Digital Investigation. 2022. Vol. 42–43. P. 301451. DOI: 10.1016/j.fsidi.2022.301451.

5. Abdalzaher M.S., Fouda M.M., Ibrahem M.I. Data Privacy Preservation and Security in Smart Metering Systems // Energies. 2022. Vol. 15. № 19. P. 7419. DOI: 10.3390/en15197419.

6. Sharma R. Enhancing Industrial Automation and Safety Through Real-Time Monitoring and Control Systems // International Journal on Smart & Sustainable Intelligent Computing. 2024. Vol. 1. № 2. P. 1–20. DOI: 10.63503/j.ijssic.2024.30.

7. Data Communication for Wireless Mobile Nodes in Intelligent Transportation Systems / K.N. Qureshi [et al.] // Microprocessors and Microsystems. 2022. Vol. 90. P. 104501. DOI: 10.1016/j.micpro.2022.104501.

8. Mills K. A Brief Survey of Self-Organization in Wireless Sensor Networks: Research Articles // Wireless Communications and Mobile Computing. 2007. Vol. 7. P. 823–834. DOI: 10.1002/wcm.499.

9. Khanna R. Evolutionary Approach to Efficient Provisioning and Self-organization in Wireless Sensor Networks (WSN). Oregon State University, 2016.

10. Improving Security in WMNs With Reputation Systems and Self-Organizing Maps / Z. Bankovic [et al.] // Journal of Network and Computer Applications. 2011. Vol. 34. Iss. 2. P. 455–463. DOI: 10.1016/j.jnca.2010.03.023.

11. Decentralized Intrusion Detection in Wireless Sensor Networks / A.P. Silva [et al.] // Proceedings. 2005. P. 16–23. DOI: 10.1145/1089761.1089765.

12. Chatzigiannakis I., Strikos A. A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks // 2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007), Patras, Greece. 2007. P. 1408–1411. DOI: 10.1109/EFTA.2007.4416949.

13. Blockchain-powered defense: Securing WSN against DDoS attacks with decentralized authentication / A. Suman [et al.] // Wireless Ad-hoc and Sensor Networks. CRC Press. 2024. P. 318–339.

14. Lee C., Suzuki J. SWAT: A Decentralized Self-Healing Mechanism for Wormhole Attacks in Wireless Sensor Networks // Handbook on Sensor Networks. World Scientific Publishing Co., 2010. P. 511–532. DOI: 10.1142/9789812837318_0021.

15. Energy Optimized Security Against Wormhole Attack in IoT-Based Wireless Sensor Networks / H. Shahid [et al.] // Computers, Materials and Continua. 2021. Vol. 68. Iss. 2. P. 1967–1981. DOI: 10.32604/cmc.2021.015259.

16. Wormhole Attack Mitigation Strategies and Their Impact on Wireless Sensor Network Performance: A Literature Survey / H. Shahid [et al.] // International Journal of Communication Systems. 2022. Vol. 35. DOI: 10.1002/dac.5311.

17. An Efficient Intrusion Detection Framework for Mitigating Blackhole and Sinkhole Attacks in Healthcare Wireless Sensor Networks / J.L. Webber [et al.] // Computers and Electrical Engineering. 2023. Vol. 111, Part B. P. 108964. DOI: 10.1016/j.compeleceng.2023.108964.

18. Detection of Hello Flood Attacks Using Fuzzy-Based Energy-Efficient Clustering Algorithm for Wireless Sensor Networks / S. Radhika [et al.] // Electronics. 2023. Vol. 12. № 1. P. 123. DOI: 10.3390/electronics12010123.

19. Arunachalam R., Ruby Kanmani E.D. Detection and Mitigation of Vampire Attacks with Secure Routing in WSN Using Weighted RNN and Optimal Path Selection // Computers & Security. 2024. Vol. 145. P. 103991. DOI: 10.1016/j.cose.2024.103991.

20. Almesaeed R., Al-Salem E. Sybil Attack Detection Scheme Based on Channel Profile and Power Regulations in Wireless Sensor Networks // Wireless Networks. 2022. Vol. 28. P. 1361–1374. DOI: 10.1007/s11276-021-02871-0.

21. Nayyar A., Singh R. A Comprehensive Review of Simulation Tools for Wireless Sensor Networks (WSNs) // Journal of Wireless Networking and Communications. 2015. Vol. 5. № 1. P. 19–47. DOI: 10.5923/j.jwnc.20150501.03.

22. Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey / G.H. Adday [et al.] // IEEE Access. 2024. Vol. 12. P. 22938–22977. DOI: 10.1109/ACCESS.2024.3362889.

23. A Secure Framework for Data Sharing in Private Blockchain-Based WBANs / L. Xiao [et al.] // IEEE Access. 2020. Vol. 8. P. 153956–153968. DOI: 10.1109/ACCESS.2020.3018119.

Информация о статье:
Статья поступила в редакцию: 05.08.2025; одобрена после рецензирования: 28.08.2025;
принята к публикации: 01.09.2025
Information about the article:
The article was submitted to the editorial office: 05.08.2025; approved after review: 28.08.2025;
accepted for publication: 01.09.2025

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

Information about authors:
Desnitsky Vasily A., senior researcher of St. Petersburg Federal Research Center of the Russian Academy of Sciences (199178, Saint-Petersburg, 14th line of Vasilyevsky Island, 39), candidate of technical sciences, associate professor, e-mail: desnitsky@comsec.spb.ru, https://orcid.org/0000-0002-3748-5414