Научная статья
УДК 004. 056.5; DOI: 10.61260/2218-13X-2023-3-63-74

МЕТОДИКА ОБНАРУЖЕНИЯ АТАК В САМООРГАНИЗУЮЩИХСЯ ДЕЦЕНТРАЛИЗОВАННЫХ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

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

Аннотация. Работа посвящена разработке модели атак и методики обнаружения атак в самоорганизующихся децентрализованных беспроводных сенсорных сетях. Предложенная модель описывает возможные виды атак и их характеристики с учетом свойств самоорганизации и децентрализации. Методика ориентирована на защиту оперативно разворачиваемых на местности беспроводных сенсорных сетей, применяемых для реагирования в чрезвычайных ситуациях, и описывает этапы процесса построения и настройки механизма обнаружения атак на основе алгоритмов сбора данных в беспроводных сенсорных сетях и применения методов машинного обучения. Проведен анализ возможных видов данных, которые необходимо собирать на узлах беспроводных сенсорных сетей для обнаружения атак. К отличительным особенностям предлагаемой методики можно отнести используемые наборы признаков, характеризующих конкретные виды атакующих воздействий и позволяющих обнаруживать атаки с высокими значениями показателя качества обнаружения. На используемом в работе фрагменте программно-аппаратного прототипа беспроводных сенсорных сетей со встроенным в него механизмом обнаружения атак проведен эксперимент по проверке качества обнаружения атак, подтверждающий корректность предложенной методики.

Ключевые слова: беспроводные сенсорные сети, обнаружение атак, методика обнаружения атак

Для цитирования: Мелешко А.В., Десницкий В.А. Методика обнаружения атак в самоорганизующихся децентрализованных беспроводных сенсорных сетях // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2023. № 3. С. 63–74. DOI: 10.61260/2218-13X-2023-3-63-74.

Scientific article

TECHNIQUE OF ATTACK DETECTION IN SELF-ORGANIZING DECENTRALIZED WIRELESS SENSOR NETWORKS

Meleshko Aleksey V.;
✉**Desnitsky Vasily A.**
Saint-Petersburg Federal research center of the Russian academy of sciences, Saint-Petersburg, Russia
✉***desnitsky@comsec.spb.ru***

Abstract. The work is devoted to the development of an attack model and a technique for detecting attacks in self-organizing decentralized wireless sensor networks. The proposed model describes possible types of attacks and their characteristics, taking into account the properties of self-organization and decentralization. The methodology is focused on the protection of wireless sensor networks deployed on the ground, used for emergency response, and describes the stages

of the process of building and configuring an attack detection mechanism based on data collection algorithms in wireless sensor networks and the use of machine learning methods. The analysis of possible types of data that need to be collected at the nodes of wireless sensor networks to detect attacks is carried out. The distinctive features of the proposed technique include the sets of features used that characterize specific types of attacking influences and allow detecting attacks with high values of the detection quality indicator. On the fragment of the hardware-software prototype of wireless sensor networks used in the work with an attack detection mechanism built into it, an experiment was conducted to check the quality of attack detection, confirming the correctness of the proposed technique.

Keywords: wireless sensor networks, attack detection, attack detection technique

For citation: Meleshko A.V., Desnitsky V.A. Technique of attack detection in self-organizing decentralized wireless sensor networks // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2023. № 3. P. 63–74. DOI: 10.61260/2218-13X-2023-3-63-74.

Введение

Проблематика информационной безопасности беспроводных сенсорных сетей (БСС) и обнаружения атак в них становится все более актуальной во многих областях приложения, включающих электроэнергетику, транспортные системы, имплантируемые медицинские устройства и др. Все большее распространение получают самоорганизующиеся децентрализованные БСС, причем самоорганизация представляет возможности динамического изменения состава узлов сети и ситуационного выстраивания сетевой топологии. Децентрализация предполагает возможности распределения функций управляющего узла БСС на несколько узлов с различными ролями, назначаемыми и переопределяемыми узлам сети в процессе ее работы. Конкретная роль узла определяется набором назначаемых ему целевых и обеспечивающих функций, например, функций сбора данных или их хранения и обработки. Характерным примером таких БСС является система антикризисного реагирования в чрезвычайных ситуациях, оперативно разворачиваемая на местности и обеспечивающая сетевую связность и коммуникации в сети разнородных устройств, относящихся к различным службам спасения, а также обеспечивающая автономность работы отдельных узлов в условиях недостатка энергоресурсов. Ввиду критически важного характера подобных систем вопросы защищенности БСС и предоставляемых ими сервисов от действий атакующих приобретают особенно важное значение.

Механизмы самоорганизации и децентрализации обеспечивают динамический характер работы сети, перераспределение функций между устройствами сети на протяжении ее работы и возможности ее масштабирования. Но в то же время данные механизмы формируют уязвимости, эксплуатация которых позволяет нарушить корректное функционирование БСС. Например, злонамеренно используя механизм самоорганизации, атакующий способен внедрить ложный узел в сеть и искажать фактические данные об оперативной обстановке информационного и физического окружения сети. Поэтому вопросы моделирования атак в самоорганизующихся децентрализованных БСС и обнаружения атак, эксплуатирующих в том числе свойства децентрализации и самоорганизации, являются особенно актуальными.

Обзор релевантных работ

Рассмотрим основные виды атак, присущих БСС. Суть sinkhole-атаки, нацеленной как на прослушивание данных сети, так и на их модификацию, заключается в том, что злонамеренный узел форсирует передачу другими узлами данных через него и тем самым «убеждает» их, что передача данных через него представляет кратчайший маршрут [1, 2] – узлы начинают передавать данные только через данный атакующий (зараженный) узел.

Атака нарушает механизм маршрутизации и может быть выполнена путем добавления нового узла в БСС или же при помощи воздействия на уже существующий.

Wormhole-атака перехватывает сообщение от одного узла другому и доставляет его быстрее, то есть за меньшее количество ретрансляций. В результате оригинальный, легитимный экземпляр сообщения будет отброшен узлом получателем [1, 3, 4]. Эта атака реализуется с помощью двух злонамеренных узлов, которые могут передавать друг другу сообщения по каналу связи, отличному от канала, используемого в рамках атакованной БСС. Отметим, что данная атака также направлена на нарушение процесса маршрутизации, и ее целью является модификация и подслушивание данных в сети.

Целью blackhole-атаки (так называемой атаки «черной дыры») является прерывание коммутации в сети, когда атакующий узел забирает (фактически теряет) полученные пакеты, и другие узлы начинают искать альтернативные маршруты в сети [1, 5]. При этом узлам приходится отправлять потерянные пакеты повторно, в том числе другими маршрутами. Атака нарушает маршрутизации в сети, а также из-за необходимости повторной передачи происходит лишнее расходование коммуникационных и вычислительных ресурсов сети.

Sybil-атака заключается в формировании на узлах сети сведений о существовании нескольких различных узлов, которые по факту являются одним узлом злоумышленника, что также нарушает правила маршрутизации в сети [1].

Под атаками внедрения вредоносного кода понимается разновидность атак, которые эксплуатируют ошибки в программном обеспечении и внедряют вредоносный код в управляющую программу узла, например, путем инъекции кода в пакет данных [6, 7]. Целью является нарушение алгоритмов работы узла.

Атаки нарушения агрегации данных и вмешательства в работу узла представляют внедрение вредоносного кода для нарушения работы узлов. Нарушение агрегации данных представляет атаку на узел, реализующий обработку и агрегацию данных, полученных от других узлов. Примером атак вмешательства является изменение алгоритма работы управляющей программы узла или корректировка физической среды его окружения узла, что может приводить к искажению показаний его сенсоров.

Hello-flood-атаки и атаки Denial-of-Sleep представляют разновидности DoS-атак [1, 8, 9]. Hello-flood-атака заключаются в частой рассылке «приветственных» широковещательных сообщений, информирующих соседние узлы о предлагаемых параметрах коммуникации. Узлы, получая такие сообщения, вынуждены на них реагировать. Узел-получатель может корректировать собственный список узлов сети, доступных для коммуникации с ним, и корректировать свои таблицы маршрутизации. Атака приводит к излишнему расходу энергоресурсов и вычислительных ресурсов узлов, поэтому она может довольно эффективно поражать БСС. Цель Denial-of-Sleep атаки – не дать узлу сети перейти в энергосберегающий режим, что приводит к повышению его энергопотребления. Атака выполняется отправкой приветственного запроса и способна приводить к потере доступности узла.

Атаки десинхронизации, атаки типа clock-skeing и data-replay можно отнести к атакам на протокол взаимодействия между узлами [1, 10]. Атака десинхронизации включает отправку пакетов с дубликатом номера текущей сессии. Поскольку в соответствии с правилами корректного функционирования сети одновременно двух одинаковых номеров сессии быть не должно, то атака приводит к закрытию сессии с отправленным порядковым номером. Поэтому узлам приходится создавать новые сессии (а это, в свою очередь, включает предварительный обмен сообщениями), что дополнительно расходует ресурсы узлов и в результате может привести к нарушениям в функционировании сети.

Атака типа clock-skeing является атакой на датчики БСС, которые требуют синхронизации текущего времени для работы. Она рассинхронизирует датчики, распространяя ложные значения текущего момента времени. Атака типа data-replay заключается в несанкционированном повторении пакетов данных – злоумышленником проводится повторная отправка по сети корректных, ранее записанных пакетов данных, что может приводить к искажению информации о состоянии среды, в которой работает БСС.

Атака типа jamming заключается в зашумлении канала связи, по которому узлы БСС осуществляют коммуникацию [11, 12]. Атаку можно отнести к физическому способу воздействия, поэтому она может приводить к полному нарушению работы сети или отключению от сети одного, двух или более узлов, что может не сразу быть обнаружено механизмом выявления атак из-за наличия в сети свойства самоорганизации.

В рассмотренных выше работах авторы рассматривают наиболее простые («базовые») реализации данных атак – варианты атак без учета свойств децентрализации сети. Однако самоорганизация и в большей степени децентрализация могут позволить злоумышленнику реализовать атаку менее заметно для средств защиты, чем при ее базовой реализации. Например, такой, более скрытной вариацией атаки может быть эксплуатация децентрализации и ролевого распределения для нелегитимного получения конкретной роли, которая предполагает получение информации от других узлов сети. Или это может быть использование механизма перераспределения ролей для реализации атак отказа в обслуживании, а именно flood-атаки, при которой узлы «впустую» тратят доступные энергоресурсы узлов. Все это позволяет сделать вывод о том, что задача анализа влияния свойств самоорганизации и децентрализации при реализации описанных выше атак, а также разработка алгоритмов их обнаружения являются на сегодняшний день актуальными.

В работе предложены модель атак самоорганизующейся децентрализованной БСС и методика обнаружения атак. Особенностью модели атак является учет свойств децентрализации и самоорганизации атак, рассматриваемых в недостаточной степени в рамках, опубликованных к настоящему времени работ в предметной области обнаружения атак в БСС. Особенность методики – использование специфичных, характеризующих рассматриваемые виды атак наборов данных, необходимых для обнаружения атак, а также способы их получения. К отличиям методики можно отнести также построенные наборы признаков, которые целесообразно использовать для обнаружения атак с применением методов машинного обучения.

Модель атак на самоорганизующуюся децентрализованную БСС

Обобщенно модель атак можно представить в виде множества кортежей:

$$\{(Type_{impact}, Type_{attack}, Target_{attack}, Involv_{selforg}, Involv_{decentral})\},$$

где $Type_{impact}$ определяет подкласс объекта, на который осуществляются воздействия. Например, $Type_{impact}$ может включать данные, программное обеспечение (ПО) узла, используемый протокол сетевого и транспортного уровней, физический канал связи. $Type_{attack}$ определяет тип атаки – используемый способ воздействия на объект атаки. $Target_{attack}$ задает конкретную цель атаки. $Involv_{selforg}$ – бинарная характеристика, определяющая наличие влияния свойства самоорганизации на реализацию атаки. $Involv_{decentral}$ – бинарная характеристика, определяющая наличие влияния свойства децентрализации на реализацию атаки.

Таким образом, каждый конкретный экземпляр кортежа определяет набор из пяти характеристик рассматриваемой атаки. Для wormhole-атаки кортеж будет иметь следующий вид: (передаваемые в БСС данные, тип wormhole, нарушение конфиденциальности и целостности данных, True, True).

Рассмотренные атаки на самоорганизующиеся децентрализованные БСС можно разделить на несколько подклассов, характеризующих объект, на которые они оказывают воздействие: а именно атаки на данные, передаваемые по сети; на программное обеспечение узлов; на устройства (узлы БСС); на протокол взаимодействия и канал связи. Обобщенно для каждого класса атак возможные разновидности атак приведены в табл. 1.

Таблица 1

Анализ атак на БСС с учетом влияния свойств самоорганизации и децентрализации

Типы атак	Цель	Влияние самоорганизации БСС	Влияние децентрализации БСС
1. Воздействия на пользовательские и служебные данные в БСС			
Sinkhole, Sybil, wormhole, blackhole	Нарушение целостности и конфиденциальности передаваемых данных (в том числе данных маршрутизации)	Расширенные возможности атакующего по нелегитимному внедрению узла в сеть, а также по подмене адресов узлов	Эксплуатация атакующим функций назначения и перераспределения ролей узлов
2. Воздействия на ПО БСС			
Внедрение вредоносного кода, искажение процессов агрегации данных	Модификация алгоритмов работы ПО узлов БСС	Расширенные возможности атакующего по нелегитимному внедрению узла в сеть и перестроению логической структуры сети	Заражение узла модифицированной командой по смене роли узла. Форсированное получение ролей коллектора или обработчика данных
3. Воздействия на узел БСС			
Hello-flood-атака, Denial-of-Sleep, атака вмешательства в работу узла (Node Tampering) и др.	Нарушение доступности узлов, что приводит к нарушению функционирования, в том числе истощение энергоресурсов узлов БСС	Возможность внедрения в сеть значительного числа новых узлов с заданными сетевыми настройками со сложностью их априорного отнесения к аномальным	Возможности эксплуатации слабых мест механизма децентрализации, в том числе назначение ролей несуществующим узлам
4. Воздействия на коммуникационный протокол БСС			
Атака десинхронизации и атаки типа clock-skeing и data-replay	Нарушение работы протокола взаимодействия узлов	Возможность «санкционированного» добавления в БСС узла-злоумышленника	Эксплуатация слабых мест протокола, в том числе модификация полей протокола «на лету»
5. Воздействия на каналы связи БСС			
Атака зашумления (jamming)	Зашумление каналов связи, по которым осуществляется беспроводная коммуникация в сети	Ввиду самоорганизации БСС, с точки зрения последствий эффект от атаки может быть расценен как легитимное изменение БСС	Возможности воздействия на узлы и инициирования процесса распределения ролей с вовлечением в него всех узлов БСС

Приведенные в табл. 1 атаки выполнимы как в БСС общего вида, так и в самоорганизующихся децентрализованных БСС. Однако при наличии в БСС свойств самоорганизации и децентрализации атакующий получает расширенные возможности по выполнению таких атак, используя действия, которые в таких сетях априори рассматриваются как легитимные. Например, в БСС общего вида появление в сети нового узла может являться явным признаком злонамеренной модификации структуры сети, тогда как в самоорганизующейся сети данный факт сам по себе не может однозначно свидетельствовать о какой-либо атаке. Поэтому для обнаружения атак на самоорганизующиеся децентрализованные БСС требуется расширенный набор признаков и более сложные способы их обнаружения.

Для каждой из рассмотренных в работе атак анализировалось, в какой степени свойства самоорганизации и децентрализации, а также ролевое функционирование сети могут влиять на выполнимость атак. Выявлено, что в некоторых случаях, например, при атаке типа sinkhole, реализация атаки упрощается, тогда как для других видов атак, например, атаки типа data-replay – наоборот, усложняется. Результаты проведенного анализа представлены в табл. 1, в которой описываются возможные типы атак на данный класс сетей с определением отличительных признаков каждой атаки. В табл. 1 также включены результаты анализа влияния свойств самоорганизации и децентрализации на выполнимость рассматриваемых атак. Необходимость разработки модели связана с потребностью в определении актуальных видов атак, которым подвержены узлы БСС, а также основных характеристик таких атак, которые, в свою очередь, должны использоваться в качестве основы для формирования признакового пространства для разрабатываемых алгоритмов обнаружения.

Отметим, что, строго говоря, описанная в табл. 1 модель атак не является исчерпывающей и может быть дополнена некоторыми другими видами атакующих воздействий, но вместе с тем она охватывает все основные, наиболее важные, описанные в литературе типовые виды атакующих воздействий на рассматриваемую разновидность БСС.

Методика обнаружения атак

Предложенная методика направлена на обеспечение эффективного обнаружения атак при использовании децентрализованных и самоорганизующихся архитектур БСС. В табл. 2 приведены основные виды данных, которые требуется собирать для обнаружения атак, описанных в модели атак.

Таблица 2

Исходные данные для обнаружения атакующих воздействий

Вид данных	Источник данных	Единица измерения	Примеры атак
Маршруты сообщений БСС	Таблицы маршрутизации каждого узла	шт.	Sinkhole, Sybil, wormhole, blackhole
Запросы на перераспределение ролей узлов	Служебный лог контроллера сети	Событие и его атрибуты	Sinkhole, Sybil, wormhole, blackhole
Показания сенсоров узлов	Все сенсорные узлы сети	Факт считывания	Внедрение вредоносного кода
Контрольные суммы управляющего ПО	Все узлы сети	Целочисленное значение	Внедрение вредоносного кода, искажение агрегации данных

Вид данных	Источник данных	Единица измерения	Примеры атак
Размер полезной нагрузки пакетов данных	Пакеты сообщений, передающиеся по сети	байты	Внедрение вредоносного кода
Потребление ресурсов узлов, (нагрузка процессора, потребление памяти, остаток энергоресурсов)	Все узлы сети	проценты	Denial-of-Sleep, hello-flood
Геолокация узлов	Все узлы сети	Координаты GPS/ГЛОНАСС	Jamming, sinkhole
События добавления новых узлов в сеть и покидания узлами сети	Служебный лог контроллера сети	Событие и его атрибуты	Jamming, sinkhole, Sybil, wormhole, blackhole
Качество беспроводного сигнала	Все узлы сети	дБм	Jamming

Рассматриваемая БСС имеет ролевое функционирование, и все действия, связанные с обнаружением атак, производятся узлом с ролью детектора. Отметим, что указанные исходные данные могут уточняться и актуализироваться под конкретный прикладной сценарий.

Методика базируется на обнаружении атак и использовании методов машинного обучения. Методика включает комбинирование данных, полученных от различных узлов сети для повышения качества обнаружения атак. Предложенная методика схематично представлена на рис. 1.

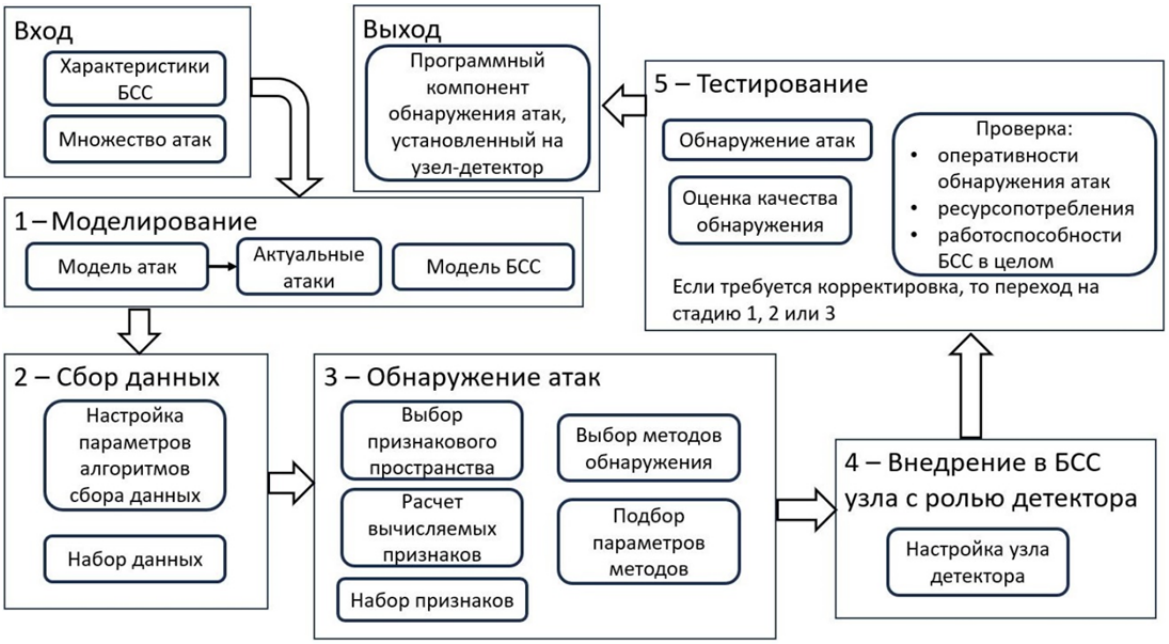

Рис. 1. **Схема методики обнаружения атак**

Методика включает пять основных этапов. Входными данными методики являются перечень атак, которые необходимо обнаружить, а также характеристики конкретной БСС, в том числе характеристики сети, включающие свойства самоорганизации и децентрализации, список ролей узлов, типы используемых сенсоров, назначение БСС и др.

Методика также учитывает ряд требований и ограничений, в том числе ограничений на потребляемые алгоритмами обнаружения объемы аппаратных ресурсов, а также требование на сохранение работоспособности сети в процессе обнаружения атак.

Этапом 1 является моделирование БСС и построение модели атак. На данном этапе производится формальное описание БСС и ее свойств, а также выделение актуальных видов атак с оценкой влияния свойств самоорганизации и децентрализации на ход каждого вида атаки.

На этапе 2 производится сбор данных, необходимых для обнаружения атак. Проводится настройка параметров сбора данных, определяются место и длительность их хранения и алгоритмы предобработки. Результатом этапа является набор размеченных данных, предназначенный для формирования алгоритмов обнаружения на основе методов машинного обучения с учителем.

На этапе 3 производится конструирование признаков из полученного набора данных, выбор обучающих методов и подбор подходящих гипер-параметров для них.

Этап 4 включает развертывание построенных алгоритмов обнаружения атак в БСС на узел с ролью детектора атак.

Этап 5 включает проведение экспериментов по обнаружению атак с оценкой качества обнаружения (с использованием показателей точности, полноты, F1-меры) и оценкой выполнимости заданных требований и ограничений. Выход методики – готовый программный компонент, настроенный на особенности реализации процессов сбор данных в сети и обнаружения на их основе атак, актуальных для рассматриваемой БСС. В табл. 3 описаны основные виды признаков, используемых для обнаружения атак.

Таблица 3

Признаки для обнаружения атак

Классы атак	Признаки
1. Воздействия на пользовательские и служебные данные в БСС	– количество задействованных маршрутов за единицу времени; – количество уникальных маршрутов, проходящих через определенный узел за единицу времени; – запросы на смену ролей узлов сети и атрибуты данного запроса (в том числе адрес узла БСС – инициатора смены ролей, характеристики данного узла, такие как объем свободной памяти его локального хранилища и остаток энергоресурсов); – атрибуты события добавления узла в сеть (в том числе геолокация, ресурсные характеристики)
2. Воздействия на ПО БСС	– средняя частота считываний узлами показаний сенсоров за единицу времени; – контрольные суммы управляющего ПО; – размер полезной нагрузки пакетов данных; – запросы на смену ролей узлов сети и их атрибуты (идентификатор узла – инициатора запроса, его характеристики)
3. Воздействия на узел БСС	– средняя частота смены ролей узлов сети; – потребление ресурсов узлов за единицу времени; – геолокация узлов; – количество событий добавления узлов в сеть за единицу времени; – частота считываний узлами показаний сенсоров за единицу времени
4. Воздействия на коммуникационный протокол БСС	– запросы на смену ролей узлов сети и его атрибуты (статус запроса и количество таких запросов); – количество событий добавления узлов в сеть за единицу времени
5. Воздействия на каналы вязи БСС	– качество беспроводного сигнала; – геолокация узлов перед отключением; – количество событий ухода узлов из сети за единицу времени

Приведенные в табл. 3 признаки атак могут непосредственно извлекаться из собираемых данных в сети, а также могут конструироваться путем статистической обработки собираемых в сети данных. Такими производными признаками могут быть, во-первых, количество задействованных маршрутов за единицу времени, что может быть вычислено на основе данных о маршрутах передачи сообщений в БСС, и, во-вторых, средняя частота смены ролей узлов сети – путем анализа запросов на перераспределение ролей узлов за единицу времени. Методика отличается универсальностью – применение методики позволяет настроить и внедрить защитные меры по эффективному обнаружению актуальных видов атак на самоорганизующуюся децентрализованную БСС в различных областях приложений.

Эксперименты и дискуссия

В качестве апробации предложенной методики обнаружения атак на разработанном программно-аппаратном стенде самоорганизующейся децентрализованной БСС с ролевым функционированием [13] проведено моделирование атаки отказа в обслуживании (атака типа flood), схематично представленной на рис. 2. Суть моделируемой атаки состоит в подключении к сети злонамеренного узла и несанкционированного инициировании механизма перераспределения ролей в сети. Предполагается, что злоумышленник выполняет следующие шаги: подключение скомпрометированного узла к БСС; инициирование запроса на реконфигурацию ролей узлов; некорректное завершение запроса на реконфигурацию ролей; возврат сети в исходное состояние; повтор всех предыдущих шагов множество раз.

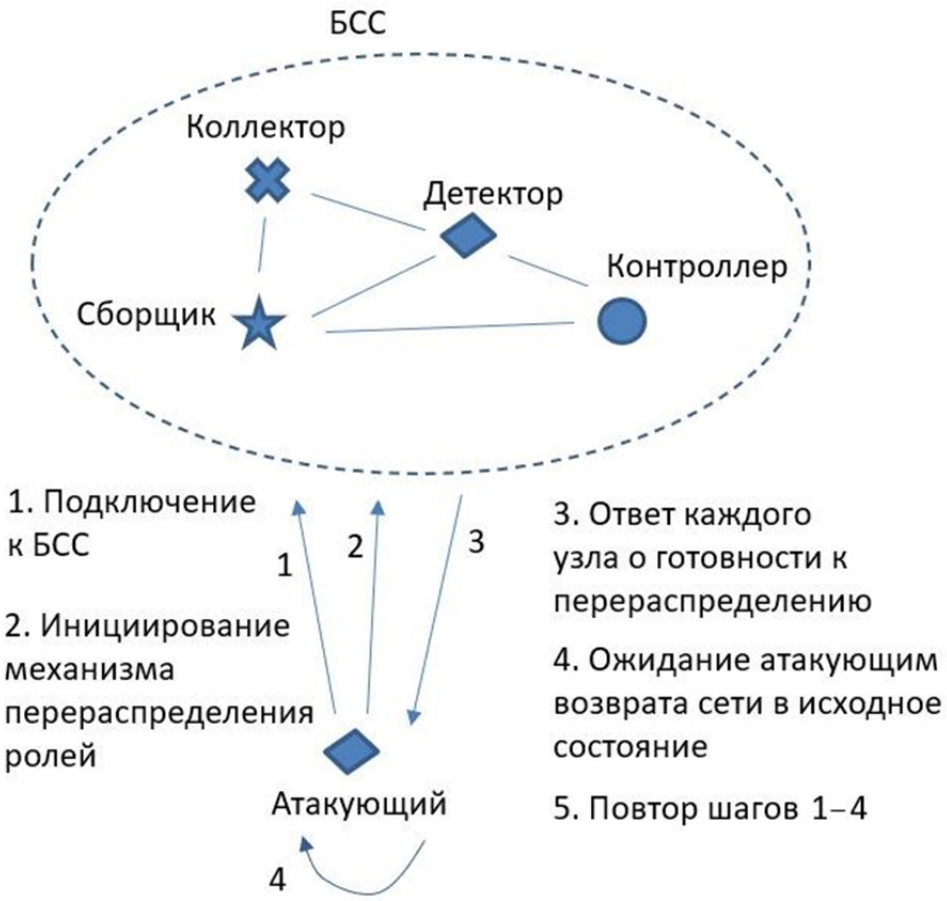

Рис. 2. **Иллюстрация атакующих воздействий при моделировании атаки типа flood**

В рамках моделирования атаки узлы БСС вынуждены тратить дополнительные ресурсы на выполнение служебных команд – ответов на запросы штатного перераспределения ролей в сети. Однако под атакой каждое очередное перераспределение завершается некорректно, и БСС возвращается в исходное состояние. В итоге работоспособность сети нарушается, и значительно сокращается время ее автономной работы. Полученный набор данных содержит передаваемые по сети показания сенсоров и записи служебного лога контроллера сети, который включает в себя запросы о перераспределении или реконфигурации сети. Эксперименты на имеющемся программно-аппаратном стенде БСС подтвердили, что собираемых данных достаточно для корректного обнаружения моделируемой атаки.

При разработке прототипа компонента обнаружения flood-атаки использовались следующие модели машинного обучения (рис. 2): AdaBoost-классификатор, случайный лес, байесовский классификатор, логистическая регрессия, линейный классификатор SVM, деревья решений и Ridge-классификатор. Для оценки качества использовался показатель F1-меры как универсальный показатель, объединяющий точность обнаружения атак и полноту. Проведенные эксперименты показали высокие значения показателя – среднее значение F1-меры составляет 0,98, что подтверждает корректность предлагаемой методики для использования в самоорганизующихся децентрализованных БСС.

Заключение

В работе описаны модели и методика обнаружения атак в децентрализованных БСС. Методика учитывает особенности ролевого функционирования узлов сети и включает алгоритмы сбора данных и обнаружения атак. Методика позволяет формировать средства обнаружения атак, актуальных для конкретной сети, настраивать и развертывать в существующие инфраструктуры БСС в различных приложениях. В дальнейшей работе планируется апробация методики на других видах атак, в том числе с их натурным моделированием в различных вариациях.

Список источников

1. Grover J., Sharma S. Security issues in wireless sensor network – a review // 5th International Conference on Reliability. Infocom Technologies and Optimization (ICRITO), 2016. P. 397–404.

2. Rehman Au., Rehman S.U., Raheem H. Sinkhole attacks in wireless sensor networks: a survey // Wireless Personal Communications. 2019. № 106. P. 2291–2313. DOI: 10.1007/s11277-018-6040-7.

3. Ahutu O.R., El-Ocla H. Centralized routing protocol for detecting wormhole attacks in wireless sensor networks // IEEE Access. 2020. Vol. 8. P. 63270–63282. DOI: 10.1109/ACCESS.2020.2983438.

4. Ghugar U., Pradhan J. Survey of wormhole attack in wireless sensor networks // Computer Science and Information Technologies. 2021. Vol. 2. № 1. P. 33–42. DOI: 10.11591/csit.v2i1.p33-42.

5. Шахов В.В., Юргенсон А.Н., Соколова О.Д. Моделирование воздействия атаки Black Hole на беспроводные сенсорные сети // Программные продукты и системы. 2017. Т. 30. № 1. С. 34–39. DOI: 10.15827/0236-235X.030.1.034-039.

6. Alahari H.P., Yelavarthi S.B. Performance analysis of denial of service dos and distributed dos attack of application and network layer of IoT // Third International conference on inventive systems and control (ICISC). 2019. P. 72–81. DOI: 10.1109/ICISC44355.2019.9036403.

7. Nwokoye C.H., Madhusudanan V. Epidemic models of malicious-code propagation and control in wireless sensor networks: an indepth review // Wireless personal communications. 2022. № 125. P. 1827–1856. DOI: 10.1007/s11277-022-09636-8.

8. 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. DOI: 10.3390/electronics12010123.

9. Denial-of-Service Attacks on Wireless Sensor Network and Defense Techniques / M.N.U. Islam [et al.] // Wireless personal communications. 2021. Vol. 116. P. 1993–2021. DOI: 10.1007/s11277-020-07776-3.

10. Amirreza Zaman, Behrouz Safarinejadian, Wolfgang Birk. Security analysis and fault detection against stealthy replay attacks // International Journal of Control. 2022. Vol. 95:6. P. 1562–1575. DOI: 10.1080/00207179.2020.1862917.

11. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks / M. Adil [et al.] // Sensors. 2020. Vol. 20(8):2311. DOI: 10.3390/s20082311.

12. SVM-Based cloning and jamming attack detection in iot sensor networks / M. Jeyaselvi [et al.] // Advances in information communication technology and computing. Lecture notes in networks and systems. 2022. Vol. 392. DOI: 10.1007/978-981-19-0619-0_41.

13. Мелешко А.В., Десницкий В.А. Детектирование атак в самоорганизующихся децентрализованных беспроводных сенсорных сетях // Математическое и информационное моделирование: материалы Всерос. конф. молодых ученых. 2022. Т. 20. С. 276–281.

References

1. Grover J., Sharma S. Security issues in wireless sensor network – a review // 5th International Conference on Reliability. Infocom Technologies and Optimization (ICRITO), 2016. P. 397–404.

2. Rehman Au., Rehman S.U., Raheem H. Sinkhole attacks in wireless sensor networks: a survey // Wireless Personal Communications. 2019. № 106. P. 2291–2313. DOI: 10.1007/s11277-018-6040-7.

3. Ahutu O.R., El-Ocla H. Centralized routing protocol for detecting wormhole attacks in wireless sensor networks // IEEE Access. 2020. Vol. 8. P. 63270–63282. DOI: 10.1109/ACCESS.2020.2983438.

4. Ghugar U., Pradhan J. Survey of wormhole attack in wireless sensor networks // Computer Science and Information Technologies. 2021. Vol. 2. № 1. P. 33–42. DOI: 10.11591/csit.v2i1.p33-42.

5. Shahov V.V., Yurgenson A.N., Sokolova O.D. Modelirovanie vozdejstviya ataki Black Hole na besprovodnye sensornye seti // Programmnye produkty i sistemy. 2017. T. 30. № 1. S. 34–39. DOI: 10.15827/0236-235X.030.1.034-039.

6. Alahari H.P., Yelavarthi S.B. Performance analysis of denial of service dos and distributed dos attack of application and network layer of IoT // Third International conference on inventive systems and control (ICISC). 2019. P. 72–81. DOI: 10.1109/ICISC44355.2019.9036403.

7. Nwokoye C.H., Madhusudanan V. Epidemic models of malicious-code propagation and control in wireless sensor networks: an indepth review // Wireless personal communications. 2022. № 125. P. 1827–1856. DOI: 10.1007/s11277-022-09636-8.

8. 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. DOI: 10.3390/electronics12010123.

9. Denial-of-Service Attacks on Wireless Sensor Network and Defense Techniques / M.N.U. Islam [et al.] // Wireless personal communications. 2021. Vol. 116. P. 1993–2021. DOI: 10.1007/s11277-020-07776-3.

10. Amirreza Zaman, Behrouz Safarinejadian, Wolfgang Birk. Security analysis and fault detection against stealthy replay attacks // International Journal of Control. 2022. Vol. 95:6. P. 1562–1575. DOI: 10.1080/00207179.2020.1862917.

11. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks / M. Adil [et al.] // Sensors. 2020. Vol. 20(8):2311. DOI: 10.3390/s20082311.

12. SVM-Based cloning and jamming attack detection in iot sensor networks / M. Jeyaselvi [et al.] // Advances in information communication technology and computing. Lecture notes in networks and systems. 2022. Vol. 392. DOI: 10.1007/978-981-19-0619-0_41.

13. Meleshko A.V., Desnickij V.A. Detektirovanie atak v samoorganizuyushchihsya decentralizovannyh besprovodnyh sensornyh setyah // Matematicheskoe i informacionnoe modelirovanie: materialy Vseros. konf. molodyh uchenyh. 2022. T. 20. S. 276–281.

Информация о статье:
Статья поступила в редакцию: 14.09.2023; одобрена после рецензирования: 15.09.2023;
принята к публикации: 20.09.2023

The information about article:
The article was submitted to the editorial office: 14.09.2023; approved after review: 15.09.2023;
accepted for publication: 20.09.2023

Информация об авторах:
Мелешко Алексей Викторович, младший научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук (199178, Санкт-Петербург, 14-я линия Васильевского острова, д. 39), e-mail: meleshko.a@iias.spb.su, https://orcid.org/0000-0002-1209-4230, SPIN-код: 9600-6970
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, SPIN-код: 9600-6970

Information about authors:
Meleshko Alexey V., junior researcher at the Saint-Petersburg Federal research center of the Russian academy of sciences (199178, Saint-Petersburg, 14th line of Vasilievsky island, 39), e-mail: meleshko.a@iias.spb.su, https://orcid.org/0000-0002-1209-4230, SPIN: 9600-6970
Desnitsky Vasily A., senior researcher at the Saint-Petersburg Federal research center of the Russian academy of sciences (199178, Saint-Petersburg, 14th 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: 9600-6970