УДК 004.725.4
МРНТИ 50.47.29

https://doi.org/10.55452/1998-6688-2025-22-4-40-59

[1,2]*Жукабаева Т.К.,
PhD, профессор, ORCID ID: 0000-0001-6345-5211,
*e-mail: zhukabayeva tk@enu.kz
[1,3]Марденов Е.М.,
магистр, ORCID ID: 0000-0001-9284-9797, e-mail: emardenov@gmail.com
[2]Танирбергенов А.Ж.,
к.т.н., и.о. доцента, ORCID ID: 0009-0000-8401-5434,
e-mail: t.adilbek@mail.ru

[1] Международный научный комплекс «Астана», Казахстан, г. Астана
[2] Евразийский национальный университет им. Л.Н. Гумилева, Казахстан, г. Астана
[3]Astana International University, Казахстан, г. Астана

КОМПЛЕКСНАЯ МЕТОДИКА ВЫЯВЛЕНИЯ И АНАЛИЗА ИНЦИДЕНТОВ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Аннотация

Статья посвящена вопросам киберфизической безопасности беспроводных сенсорных сетей (БСС). Современные БСС уязвимы к широкому классу атак, таких как sinkhole и wormhole-атаки, атаки «человек посередине», атаки подмены данных, универсальные сетевые атаки и др. На практике возможности по защите БСС от данного вида атак затруднены вследствие разнообразия возможных воздействий, узкоспециализированной направленности инфраструктуры и ограниченности ресурсов узлов сети. В настоящей статье предлагается комплексная методика выявления инцидентов безопасности в БСС для эффективного обнаружения атак и реагирования на инциденты, что позволит минимизировать потенциальный ущерб и обеспечить бесперебойную работу таких сетей. К элементам новизны методики относится ее комплексность, способность выявлять разнообразные киберфизические воздействия и обеспечивать высокую точность и полноту обнаружения инцидентов, учитывая распределенную структуру и динамику изменений в составе узлов БСС. Методика апробирована на фрагменте сети, функционирующей по протоколу ZigBee для контроля характеристик состояния атмосферного воздуха промышленного объекта, города. Разработанная методика будет способствовать повышению качества и своевременности обнаружения инцидентов безопасности в беспроводных сенсорных сетях, что позволит улучшить устойчивость сетей к внешним и внутренним злонамеренным воздействиям и предотвращать длительные перебои в работе инфраструктуры в случае успешных атак.

Ключевые слова: беспроводная сенсорная сеть, инцидент безопасности, выявление, моделирование, методика.

Введение

В настоящее время проблематика киберфизической безопасности беспроводных сенсорных сетей (БСС), и выявления и анализа инцидентов безопасности в частности, представляет крайне важный пласт актуальных научно-технических задач, требующих эффективных подходов к их решению. В первую очередь это связано с все более широким распространением данного вида беспроводных сетей. БСС начинают использоваться практически повсеместно, начиная от мониторинга окружающей среды и заканчивая управлением промышленными процессами и медицинскими приложениями в рамках индустриального интернета вещей, что делает БСС привлекательными объектами для проведения атакующих воздействий со стороны злоумышленников.

По сравнению с проводными и беспроводными сетями общего назначения, работающими по протоколам TCP/IP, специализированные беспроводные сенсорные сети, функционирую-

щие по протоколам LoRa, LPWAN, ZigBee и др., подвержены более значительному числу и большему разнообразию угроз киберфизической безопасности, включающим атаки, связанные с нарушением маршрутизации в сети, такими как sinkhole и wormhole-атаки, не характерные для традиционных сетей общего назначения [1]. При этом, как правило, БСС также остаются подверженными таким видам атак, как атаки типа «человек посередине», спуфинг-атаки, атаки отказа в обслуживании, характерные для различных видов сетей.

Ограниченность ресурсов устройств узлов БСС, в том числе энергоресурсов, ресурса оперативной памяти, вычислительных мощностей, затрудняет внедрение сложных криптографических алгоритмов и методов защиты, что увеличивает уязвимость БСС перед атаками [2]. Вместе с тем с увеличением числа экземпляров узлов в сети управление безопасностью, как правило, становится сложнее. Поэтому необходимо разрабатывать эффективные способы обнаружения атак и реагирования на инциденты для того, чтобы минимизировать ущерб от таких атак и обеспечить бесперебойную и киберустойчивую работу беспроводной сети.

Беспроводные сенсорные сети применяются в современных критически важных областях, таких как телемедицинские системы, транспорт, электроэнергетика и физическая безопасность [3]. Нарушение работы таких сетей может привести к серьезным последствиям, в том числе к угрозам нарушений требований экологической, медицинской, транспортной и промышленной безопасности. При этом в условиях стремительного развития современных технологий, таких как машинное обучение, искусственный интеллект, большие данные, интернет вещей, возникает необходимость оптимизировать и адаптировать существующие методы анализа инцидентов и разработки новых подходов, учитывающих особенности современных технологических решений. Помимо этого, различная информация, передаваемая в БСС, зачастую содержит конфиденциальные данные, как, например, журналы событий безопасности БСС. Поэтому важно предотвращать утечки и несанкционированный доступ к таким данным, одновременно обеспечивая их целостность и конфиденциальность.

Отметим, что потребность в комплексности необходимых средств выявления и анализа инцидентов безопасности БСС обуславливается разнообразием факторов, которые необходимо учитывать в процессе обнаружения инцидентов [4]. В частности, при выявлении инцидентов безопасности необходимо рассматривать все основные известные виды угроз, которым подвержена целевая беспроводная сеть. К таким угрозам относятся угрозы нарушения конфиденциальности, включающие раскрытие секретной информации, например перехват данных. Также должны учитываться угрозы целостности, в том числе связанные с изменением или разрушением данных, к примеру, подделка данных, а также угрозы доступности, включающие ограничение доступа к сервисам или ресурсам, например, универсальные сетевые атаки, такие как DoS-атаки [5]. Кроме того, необходимо учитывать различные производные угрозы, объединяющие одновременно нарушение нескольких свойств безопасности.

Отметим также, что процесс выявления инцидентов должен охватывать как активные атаки, которые вмешиваются в работу сети, в том числе внедрение вредоносного программного обеспечения, так и пассивные атаки, включающие наблюдение за сетевой активностью без какого-либо значимого вмешательства в процесс функционирования БСС и отдельных ее узлов [6]. Вместе с тем обнаружение атакующих воздействий должно охватывать различные атаки, отличающиеся масштабом распространения, начиная от локализованных атак, затрагивающих отдельные узлы или сегменты сети, и заканчивая более масштабными воздействиями, охватывающими в том числе всю беспроводную сенсорную сеть или значимую ее часть. По части объектов приложения воздействий выделяются атаки, направленные на конкретные устройства сети, сенсоры, исполнительные механизмы узлов, атаки на каналы связи, нацеленные на нарушение коммуникации между узлами, а также воздействия на инфраструктуру, включающую серверы, системы управления базами данных и другие сущности.

По методам реализации атак выделяются, во-первых, атаки, включающие в первую очередь аппаратные, физические воздействия на оборудование, к примеру, кражу устройства узла,

повреждение сенсора [7]. Во-вторых, учитывается возможность воздействий на программное обеспечение, эксплуатирующих известные виды уязвимостей в программном обеспечении, вирусы, эксплойты [8]. В-третьих, учитываются также различные комбинированные, в том числе многошаговые атаки, объединяющие воздействия аппаратно-физического и программно-информационного характера [9].

Комплексность процессов обнаружения атак в БСС связана также с потребностью в дифференциации атак в зависимости от уровня возможных рисков и предполагаемого ущерба от них [10]. Могут рассматриваться незначительные последствия, такие как отключение единичного узла, временная потеря доступа к определенному сервису. Пример последствий среднего масштаба – временная потеря доступности к сегменту сети, тогда как значительные последствия, например, включают перехват управления и внедрение вредоносного кода в программное обеспечение большого числа узлов сети с потерей работоспособности всей сети.

По источнику воплощаемой угрозы необходимо учитывать как атаки, осуществляемые извне, так и воздействия, проводимые непосредственно со скомпрометированных узлов БСС. При этом в соответствии с этапами жизненного цикла БСС выделяются проявление атакующих воздействий на этапах разработки, развертывания и проектирования БСС, на этапе эксплуатации БСС, а также при обновлении программных модулей и настроек сети и технической поддержки функционирования. Учитываются также степень скрытности атаки и ее проявления, которые зависят в том числе от различных шаблонов и статистических распределений признаков функционирования при нормальных и аномальных операционных сценариях устройств беспроводной сенсорной сети. К значимым факторам, учет которых целесообразен для комплексного обнаружения инцидентов безопасности в БСС относятся также организационная и техническая сложность [11] обнаружения атак и связанная с этим степень автоматизации выявления инцидентов безопасности, определяющая объемы вовлечения человеческого ресурса оператора сети и/или участия эксперта по киберфизической безопасности [12].

Помимо этого, обнаружение инцидентов безопасности должно учитывать специфику сценария функционирования сети, условия и ограничения по ее расширяемости [13], допустимость изменений пространственного местоположения узлов сети, изменений сетевой топологии БСС [14–15], наличие энергоресурсов и особенности их расходования в процессе нормального функционирования [16].

В настоящее время опубликован ряд научно-исследовательских работ, фокусирующихся в первую очередь на вопросах обнаружения аномалий в функционировании беспроводных сенсорных сетей [17–19], на вопросах выявления универсальных сетевых атак на узлы БСС, таких как различные flooding-атаки и атаки сканирования [20–21], атаки нарушения процессов идентификации узлов и маршрутизации в БСС, такие как wormhole-атаки, sinkhole-атаки и Sybil-атаки [22–24], атаки истощения энергоресурсов узлов БСС и другие. При этом детальный анализ литературы в данной предметной области выявил существенную нехватку подходов и конкретных методик по комплексному выявлению инцидентов безопасности в таких сетях, которые могли бы применяться на практике для повышения осведомленности об уровне безопасности БСС в применении к широкому спектру областей приложений.

Основным вкладом настоящей работы является предложенная методика выявления и анализа инцидентов безопасности в беспроводных сенсорных сетях, которая апробирована на фрагменте БСС, функционирующей по протоколу ZigBee для контроля характеристик состояния атмосферного воздуха промышленного объекта, города.

К элементам новизны данной методики можно отнести ее комплексность и ориентированность на выявление широкого класса киберфизических воздействий в условиях достижения высоких значений показателей точности и полноты обнаружения инцидентов с учетом распределенного характера анализируемой БСС и динамического изменения состава ее узлов. Помимо повышения уровня киберфизической безопасности на практике следование данной методике будет также способствовать снижению рисков возникновения инцидентов безопас-

ности и оптимизации стратегии защиты, соответствующей условиям и требованиям безопасности конкретной беспроводной инфраструктуры.

Оставшаяся часть статьи организована следующим образом. Раздел 1 посвящен анализу основных видов инцидентов киберфизической безопасности БСС. В разделе 2 раскрывается сущность методики, в том числе основные предъявляемые к ней требования и стадии методики. В разделе 3 описывается использования методики на примере БСС для контроля характеристик состояния атмосферного воздуха промышленного объекта, города с использованием микроконтроллеров, датчиков и другого электронного оборудования. В заключение подведены основные итоги и сформулированы дальнейшие шаги по данному направлению исследований.

Анализ инцидентов безопасности в беспроводных сенсорных сетях

Проведенный анализ актуальных материалов в предметной области исследования позволил выявить следующие основные виды инцидентов киберфизической безопасности в беспроводных сенсорных сетях, охватывающие широкий спектр потенциальных угроз, направленных в том числе на нарушение конфиденциальности, целостности и доступности данных в таких сетях (таблица 1). Отметим, что конкретный инцидент в БСС может одновременно иметь признаки нескольких приведенных в таблице 1 видов инцидентов. Вместе с тем перечисление указанных видов инцидентов не является полным, а отображает лишь основные, наиболее актуальные виды проявлений.

Таблица 1 – Основные виды инцидентов киберфизической безопасности в БСС

№	Вид инцидента	Описание	Последствия
1	Утечка данных с узла сенсорной сети	Неконтролируемое распространение чувствительной информации о состоянии узла сети	Утечка конфиденциальных данных может приводить к финансовым потерям, репутационным издержкам или другим негативным последствиям
2	Нарушение целостности данных	Несанкционированное изменение данных, передающихся между узлами сети	Снижение достоверности данных в БСС, неправильные и неоптимальные решения, принимаемые в процессе реагирования на события и инциденты безопасности
3	Отказ в обслуживании	Продолжающаяся во времени перегрузка коммуникационных каналов сети, приводящая к недоступности узлов сети и предоставляемых сервисов	Нарушение нормального функционирования БСС, внесение задержек в процесс коммуникации, потеря фрагментов данных, циркулирующих по сети
4	Несанкционированный доступ	Нелегитимное проникновение атакующего в сеть с целью получения доступа к ресурсам узлов и их использования, в том числе для последующих атак	Потеря доступа и контроля над узлами БСС и их ресурсами
5	Несанкционированная модификация данных	Передача модифицированных и скомпрометированных данных от злоумышленника	Принятие ошибочных решений на основе некорректной информации
6	Физическое вмешательство в работу узлов сети	Физическая инциденты, такие как кража, повреждение или модификация, злонамеренные изменения конфигурации оборудования	Полная или частичная приостановка работы БСС, потеря данных, необходимость ремонта или замены оборудования

Продолжение таблицы 1

7	Несанкционированный перехват и анализ трафика	Прослушивание и хранение циркулирующих в сети данных для последующего их анализа	Раскрытие конфиденциальных данных, определение топологии БСС, нахождение открытых уязвимостей в программном обеспечении узлов сети
8	Проявление вредоносного программного обеспечения на узлах сети (вирусы, черви)	Заражение сети вредоносным ПО, направленным на модификацию данных, блокировку работы узлов БСС, хищение информации	Необходимость восстановления сети, включая замену отдельных программно-аппаратных модулей и конфигурационных настроек, финансовые потери, репутационные издержки
9	Подделка данных учетных записей	Компрометация учетных записей пользователей и администраторов сети и сетевых сервисов	Несанкционированный доступ на устройства сети
10	Атаки типа Man-in-the-Middle (человек посередине)	Вмешательство в коммуникационные каналы между узлами БСС с целью перехвата, модификации данных	Подмена передаваемых данных, утечки данных
11	Некорректная конфигурация БСС	Ошибки в настройке беспроводной сети, приводящие в большей уязвимости БСС	Повышение вероятности успешных атак и снижение уровня защищенности БСС

Отметим, что разнообразие видов инцидентов безопасности в беспроводных сенсорных сетях обуславливает необходимость и важность построения комплексной методики для обеспечения безопасности БСС, снижения числа успешно выполненных атакующих воздействий и снижения предполагаемого ущерба от них.

Материалы и методы

Методика выявления и анализа инцидентов безопасности в беспроводных сенсорных сетях

Предлагаемая комплексная методика выявления и анализа инцидентов безопасности в беспроводных сенсорных сетях предназначена для осуществления на этапе функционирования БСС обслуживающим персоналом инфраструктуры сети. Конечной целью методики является повышение уровня защищенности БСС, что выражается в следующих целях:

- максимизация доли успешно выявленных инцидентов безопасности, произошедших за определенный промежуток времени Δt по отношению ко всему объему инцидентов за данный промежуток времени

$$p_{\Delta t}(I,m) \xrightarrow[m\in M]{} \max,$$

где p – обобщенный показатель успешно выявленных инцидентов I с использованием методики m, подвергающийся максимизации;

- минимизации числа выявленных ложно положительных инцидентов безопасности за промежуток времени Δt:

$$f_{\Delta t}(I,m) \xrightarrow[m\in M]{} \min;$$

◆ снижения затрат коммуникационно-вычислительных ресурсов узлов БСС, выделяемых на функционирование распределенного механизма выявления и анализа инцидентов безопасности, а также достижения цели.

В общем случае одновременное достижение поставленных целей представляет собой многокритериальную оптимизационную задачу, решение которой производится с использованием следующих методов. На первом шаге производится сужение пространства возможных решений на основе метода оптимизации по Парето, при котором находится граница Парето для заданной конфигурации беспроводной сенсорной сети – набор неулучшаемых решений, оптимальных по Парето. К альтернативному варианту можно отнести использование DEA-оптимизации, который позволяет получить набор граничных значений, принимаемых за условно оптимальные [25]. На втором шаге применяется метод свертки с определением весовых коэффициентов на основе важности отдельных формулируемых оптимизационных критериев.

Расчет минимизации коммуникационно-вычислительных ресурсов узлов БСС в условиях дискретных моментов времени в рамках промежутка Δt производится следующим образом:

$$\max_{\Delta t \in T} \left\{ \frac{\max_{t \in \Delta t}(|r^{(p)}|) - \max_{t \in \Delta t}(|r|)}{\max_{t \in \Delta t}(|r|)} \right\} \xrightarrow[m \in M]{} \min ,$$

где $r = (r_n, r_c, r_e)$ – вектор показателей ресурсопотребления с компонентом r_n для определения затрачиваемых коммуникационных ресурсов, r_c – затрачиваемых вычислительных ресурсов и r_e – энергоресурсов, затрачиваемых в процессе нормального функционирования сети. Аналогичным образом задается векторный показатель $r^{(p)} = (r_n^{(p)}, r_c^{(p)}, r_e^{(p)})$, специфицирующий каждый вид ресурсов, затрачиваемых в условиях функционирования БСС, включающей работу программных модулей выявления и анализа инцидентов безопасности. Величина T задает множество равных по продолжительности промежутков времени Δt, каждый из которых формирует конечную последовательность дискретных моментов времени t для измерения вычислимых показателей.

Отметим, что значения величин r и $r^{(p)}$ представляют собой нормированные средневзвешенные вектор-значения с использованием коэффициентов важности, задаваемых с учетом специфики конкретного сценария функционирования БСС. Нормировка компонентов величин r и $r^{(p)}$ производится на интервале (0,1), где 1 обозначает максимальное потребление соответствующего ресурса. Интегральное значение ресурсопотребления вычисляется следующим образом

$$|r| = \sqrt{(r_n^{(i+1)})^2 + (r_c^{(i+1)})^2 + (r_e^{(i+1)})^2} ,$$

$$imp : r^{(i)} \to r^{(i+1)} ,$$

$$r_n^{(i+1)} = \frac{k_n \cdot r_n^{(i)}}{k_n + k_c + k_e}$$

$$r_c^{(i+1)} = \frac{k_c \cdot r_c^{(i)}}{k_n + k_c + k_e}$$

$$r_e^{(i+1)} = \frac{k_e \cdot r_e^{(i)}}{k_n + k_c + k_e} , \text{ где}$$

величины k_n, k_c и k_e – коэффициенты важности, в общем случае определяемые рекуррентно, исходя из апостериорно установленных равновесных значений в виде в виде (0,33; 0,33; 0,33),

после чего на основе отображения imp с учетом внешний знаний преобразуются в требуемый вектор для учета критичности используемых ресурсов БСС. При этом алгоритм преобразования коэффициентов производится с учетом знаний об известных уязвимостях программно-аппаратного обеспечения беспроводной сети, извлекаемых из открытых баз данных, таких как CPE для определения характеристик программно-аппаратного обеспечения, CVE – как средства представления уязвимостей и шаблонов атак CAPEC [26].

В частности, из базы данных CAPEC для каждой найденной уязвимости, соответствующей характеристикам CPE, получаются следующие значения:

- Likelihood_Of_Attack – задающее вероятность эксплуатации данной уязвимости; используются три категориальных значения High, Medium и Low, преобразуемые в числовые значения 0,33, 0,66 и 1 соответственно;
- Typical_Severity – определяющее уровень критичности уязвимости, также задаваемое в рамках настоящей методики на основе трех категориальных значений High, Medium и Low, преобразуемые в числовые – 0,33, 0,66 и 1 соответственно.

Отметим, что в рамках текущей реализации методики рекуррентный характер вычисления коэффициентов важности ограничивается одной итерацией применения отображения $imp : r^{(0)} \to r^{(1)}$, в то время как в общем случае большее число итераций позволит более комплексно учесть разноплановость актуальных видов уязвимостей и дифференциацию по характеристикам программно-аппаратного обеспечения в соответствии с конкретными используемыми идентификаторами из базы CPE и их значений.

При этом для расчета коэффициентов важности для коммуникационного ресурса r_n используются шаблоны атак, принадлежащие категориям «CAPEC-216: Communication Channel Manipulation», «CAPEC-192: Protocol Analysis», «CAPEC-117: Interception» и др., для вычислительного ресурса r_c используются категории «CAPEC-20: Encryption Brute Forcing», «CAPEC-49: Password Brute Forcing», «CAPEC-97: Cryptanalysis» и др., тогда как энергоресурса r_e используются, в частности, такие категории, как «CAPEC-604: Wi-Fi Jamming», «CAPEC-124: Shared Resource Manipulation» и «CAPEC-233: Privilege Escalation». Таким образом, коэффициенты важности вычисляются по следующим формулам:

$$k_n = count(v, r_n) \cdot \underset{v \in Vn}{mean}(Likelihood\_Of\_Attack(v)) \cdot \underset{v \in Vn}{mean}(Typical\_Severity(v)) \ ,$$

$$k_c = count(v, r_c) \cdot \underset{v \in Vc}{mean}(Likelihood\_Of\_Attack(v)) \cdot \underset{v \in Vc}{mean}(Typical\_Severity(v)) \ ,$$

$$k_e = count(v, r_e) \cdot \underset{v \in Ve}{mean}(Likelihood\_Of\_Attack(v)) \cdot \underset{v \in Ve}{mean}(Typical\_Severity(v)) \ ,$$

где функция count возвращает общее число уязвимостей, релевантных рассматриваемому сценарию БСС в контексте потребления ресурсов r_n, r_c, r_e соответственно; функция mean возвращает усредненные значения вероятности эксплуатации атаки v и уровень ее критичности. При этом соответствующие множества V_n, V_c и V_e – подмножества уязвимостей, относящихся к расходованию рассматриваемых ресурсов и специфицируемых экспертным путем.

Сформулируем основные группы требований, предъявляемых к методике и определяющих основные критерии проверки ее выполнимости (таблица 2).

Отметим, что выполнение этих требований будет способствовать построению надежной и более гибкой методики выявления и анализа инцидентов безопасности в беспроводных сенсорных сетях, способной адаптироваться к меняющимся с течением времени условиям и угрозам в зависимости от особенностей функционирования конкретной БСС. Рассмотрим основные стадии предлагаемой методики (рисунок 1).

Таблица 2 – Основные виды требований, предъявляемых к методике

№	Группы требований	Требования
1	Универсальность и масштабируемость	- Ориентированность на разные типы БСС, отличающиеся протоколы связи, состав и количество узлов. - Масштабируемость для увеличения числа узлов и датчиков без значительного снижения функциональности, нарушений доступа и задержек, а также повышения интенсивности потоков данных.
2	Качество обнаружения инцидентов	- Высокие точность и полнота выявляемых инцидентов безопасности с возможностью настройки гиперпараметров моделей обнаружения. - Снижение размерности и объемов анализируемых данных за счет удаления случайных выбросов и незначимых событий и их детализации. - Проверка качества работы механизма обнаружения инцидентов на независимых выборках репрезентативных данных достаточных объемов.
3	Оперативность выявления инцидентов безопасности	- Должна обеспечиваться оперативность выявления всех значимых инцидентов безопасности с учетом сценарных ограничений. - Отслеживание инцидентов должно проводиться непрерывно с учетом текущего состояния БСС и ее доступных устройств. - Должны также определяться статистически значимые отклонения от нормального функционирования работы сети, и эти данные необходимо использовать для уточнения и расширения массива анализируемых данных. - Должно соблюдаться ограничение на максимально допустимую задержку между моментом фактического возникновения инцидента и его выявлением.
4	Комплексность методики	- Модульность архитектуры и поддержка возможности интеграции с существующими стандартами и протоколами киберфизической безопасности.
5	Автоматизация методики	- Необходимость автоматизировать наиболее трудоемкие и повторяемые шаги методики по заданному набору правил, в том числе шаги по автоматическому сбору и обработке данных с минимальным участием оператора сети.
6	Защищенность процессов выявления и анализа инцидентов безопасности	- Защищенные хранение и передача исходных и промежуточных данных, а также результатов обнаружения и анализа инцидентов. - Наличие средств резервирования критичных модулей сети и возможности оперативного восстановления работоспособности в случае отказов.
7	Распределенный характер методики	- Необходимость распределения модулей по обнаружению и анализу инцидентов между узлами и устройствами БСС с возможностью применения принципов федеративных вычислений.
8	Эффективное ресурсопотребление	- Необходимость оптимизации затрат на эксплуатацию и обслуживание инфраструктуры БСС и процессов обнаружения и анализа инцидентов безопасности.

Рисунок 1 – Основные стадии методики выявления и анализа инцидентов безопасности в БСС

На стадии 1 методики производится сбор исходных данных о беспроводной сенсорной сети, в том числе:

- статические данные, включающие состав и топологию сети, спецификацию элементов программно-аппаратного обеспечения узлов с использованием идентификаторов CPE, используемый протокол сетевого взаимодействия, применяемые политики безопасности на основе предикативных правил [27], спецификацию инфраструктуры сети;
- динамические данные, включающие данные трафика БСС и журналы событий на узлах, в том числе пользовательские команды ввода/вывода на узлах, показания сенсоров и состояния исполнительных механизмов узлов.

Исходные данные собираются в потоковом режиме, обеспечивая выборки необходимых для анализа данных на протяжении функционирования сети.

Стадия 2 включает предобработку собранных на стадии 1 данных, в том числе:

- унификацию данных – их приведение к единому формату;
- устранение и исправление ошибочных и пропущенных значений;
- фильтрацию данных – удаление лишней, ненужной для последующего анализа информации (в том числе шума, случайных выбросов, незначимых аномалий, дублирующихся данных);
- объединение данных с различных узлов – построение и наполнение единого централизованного хранилища данных с привязкой к узлу-координатору с использованием реляционных и NoSQL-средств хранения. Отметим, что в общем случае такое хранилище может быть децентрализованным – фактически данные могут распределяться в модулях хранения нескольких узлов, но за их управление отвечает узел-координатор;
- снижение размерности данных, которое может осуществляться с использованием метода главных компонент [28] и автоэнкодеров [29];
- нормализацию/стандартизацию данных – приведение к универсальным диапазонам значений, что, в частности, позволяет повысить показатели качества обнаружения атак с использованием ряда обучающих моделей, как, например, KNN.

Стадия 3 представляет собой анализ собранных и предобработанных данных. При этом сбор данных и частично их предобработка могут производиться на уровне конечных узлов БСС с возможностью отбора и накопления фрагментов данных для их периодической от-

правки на сторону узла-координатора сети для централизованной обработки и анализа. Анализ данных включает, в частности, возможность балансировки данных по классам атак для пополнения представителей миноритарных классов. Помимо конкретных методов анализа, включающих метод опорных векторов, сверточные нейронные сети и методы на основе деревьев на данной стадии применяются методы ансамблирования классификаторов, включающие бэггингом и стекинг, бустинг, взвешенное и мажоритарное голосования и др. [30]. При этом такое комбинирование направлено в том числе на снижение влияния эффекта переобучения. Таким образом, для каждого актуального вида атак, который требуется иметь возможность обнаруживать эффективным образом, данная стадия включает выполнение следующих шагов:

- извлечение признаков из предобработанных выборок данных;
- формирование частной гипотезы относительно видов данных, являющихся первостепенными признаками для обнаружения данного вида атак;
- конструирование признакового пространства в соответствии с заданной гипотезой;
- выделение обучающих и валидационных выборок;
- определение требуемых значений показателей качества обнаружения, включающих точность, полноту, f1-меру, а также показателей оперативности и ресурсопотребления;
- выбор моделей и методов обучения для бинарной классификации;
- определение значений гиперпараметров для выбранных обучающих моделей и методов;
- определение разметки данных;
- обучение с применением методов классификации, кластеризации, регрессии;
- комибинирование бинарных классификаторов в рамках мультиклассовой классификации;
- проверка показателей путем тестирования на валидационных выборках. При недостижении требуемых значений показателей возврат на шаг формирования уточнения гипотезы.

Стадия 4 включают визуальную аналитику, выполняемую параллельно методам машинного обучения в целях визуального контроля анализируемых данных, в том числе результатов машинного анализа со стороны оператора целевой системы. Кроме того, визуальный анализ может быть применен для уточнения отдельных шагов стадии 3, в том числе для уточнения и корректировки сформированной гипотезы для проведения машинного обучения и формирования признакового пространства. Стадия 4 включает следующие шаги:

- подготовку источников и выборок данных для визуального анализа;
- подбор визуальных моделей под различные виды атакующих воздействий, а также параметров этих моделей, таких как число отображаемых слоев, осей, параметров группировки, типов используемых графовых структур и пр.;
- проверку и экспертную оценку построенных моделей на тестовых наборах данных, в том числе формирование и уточнение инцидентов безопасности, включающих информацию о типах атак, приведших к выявленному инциденту, устройствах – источниках атак и устройствах, вовлеченных в атаку, временные метки старта, завершения вредоносной активности и другую сопутствующую информацию.

На стадии 5 методики осуществляется поддержка принятия решений по реагированию на выявленные инциденты безопасности, которая включает следующие действия:

- принятие решений по реагированию на обнаруженные инциденты безопасности в БСС. Ключевыми факторами здесь являются категории активов, узлов БСС данных, которые непосредственно связаны с выявленным инцидентом, критичность этих активов и возможные последствия данного инцидента. Основными показателями, на основе которых осуществляется поддержка принятия решения являются величина ущерба от инцидента и риск возможного продолжения действия инцидента в случае продолжающейся во времени атаки;
- выработка мер по реагированию на выявленный инцидент, включающая принятие мер для каждого актива БСС, вовлеченного в инцидент с учетом целевых функций и ограничений

узлов, сценариев функционирования БСС. В частности, к подобным контрмерам относятся повышение отказоустойчивости узлов и предоставляемых сетью информационных сервисов, резервирование узлов, каналов связи и данных, необходимых в процессе работы БСС;

- уточнение и корректировка политик безопасности, определяющих, в частности, правила контроля доступа в сети, фильтрации трафика и проверки служебных команд, пересылаемых по сети;
- расследование, включающее выяснение причин возникновения выявленного инцидента и выяснение сопутствующей информации вектора атаки, включающей время, локации возникновения атак, вовлеченных пользователей и использованные данные и команды. В частности, сбор следов атаки включает сбор и сохранение данных, связанных с инцидентом, системных журналов, трафик и дампы памяти узлов. В случае фрагментарного понимания процесса атаки применяется аналитическое моделирование атаки, позволяющее воспроизвести и оценить ее возможные сценарии с точки зрения их выполнимости, организационно-технической сложности, оперативности и ресурсопотребления;
- непрерывный мониторинг состояния БСС, отдельных узлов и компонентов с целью устранения последствий атаки и предотвращения ее последующих итераций.

Результаты и обсуждение

Предложенная методика апробирована на фрагменте разработанного программно-аппаратного стенда киберфизической системы для контроля характеристик состояния атмосферного воздуха промышленного объекта, города с использованием микроконтроллеров, датчиков и другого электронного оборудования. Реализованный фрагмент БСС включает в свой состав узлы на основе микроконтроллеров Arduino Uno, беспроводные коммуникационные интерфейсы XBee, датчики температуры и влажности.

На данном фрагменте БСС был промоделирован инцидент киберфизической безопасности, представляющий собой следующую комбинированную атаку, осуществляемую с использованием натурного моделирования. Моделируемая атака включает, во-первых, воздействия типа wormhole [31–36], направленные на нарушение процесса корректной маршрутизации пакетов данных в ZigBee-сети и, во-вторых, spoofing-воздействие для подмены значений показаний части сенсоров БСС. На рисунке 2 показан фрагмент интерфейса моделирования сценариев работы БСС с заданием характеристик состояния атмосферного воздуха, снимаемых на узлах сети.

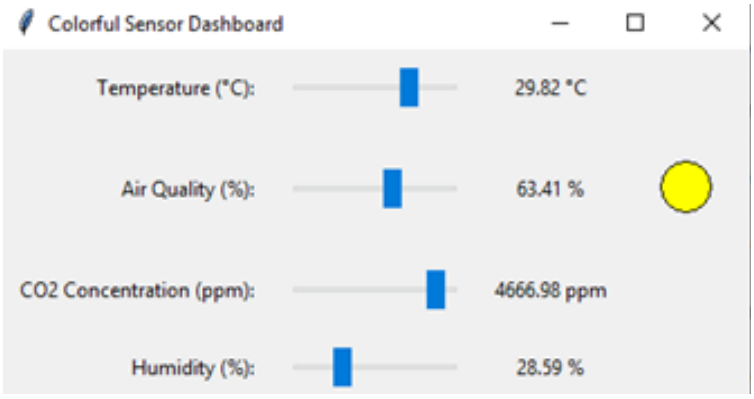

Рисунок 2 – Интерфейс моделирования сценариев работы БСС

В таблицах 3–7 приведены сведения о выполнении 5 стадий предложенной методики в рамках данного демонстрационного сценария.

Таблица 3 – Выполнение стадии сбора исходных данных о БСС

Стадия методики	Действия	Описание
Стадия 1. Сбор исходных данных о БСС	Сбор статических данных БСС	Топология сети в составе 6 узлов с ролью роутера (R_0, R_1, R_2, R_3, R_4, R_5, R_6), отвечающих за обеспечение связности и осуществляющих маршрутизацию в БСС, а также узел с ролью координатора С, относящиеся к уникальному идентификатору сети PAN ID. Топология сети задается в соответствии со схемой, приведенной на рисунке 2, с использованием пар вида (R_i, R_j), где i,j=0..6 и i≠j. Используемое программно-аппаратное обеспечение специфицируется использованием идентификаторов CPE, как, например, с помощью «cpe:/h:raspberrypi:raspberry_pi_3_model_b%2b:-» задается используемый на узле С одноплатный компьютер Raspberry Pi 3B+, где параметр /h обозначает указание конкретного физического устройства, работающего по протоколу ZigBee с использованием модулей XBee series 2. Используемые политики фильтрации задаются с использованием правил вида $N_k \rightarrow N_j$, где k и j задают номера узлов, между которыми коммуникация на прикладном уровне сетевого взаимодействия разрешена. Узлы задаются при помощи уникальных 8-байтовых адресов, представленных в шестнадцатеричной форме.
	Сбор динамических данных БСС	Считываемые в процессе функционирования данные БСС включают: – исходящие и входящие на узел пакеты данных, каждый из которых включает стартовый байт, длину и тип фрейма, 64-битный адрес получателя, уровень приема сигнала RSSI, возможные дополнительные опции фрейма, полезную нагрузку и контрольную сумму, используемую для проверки целостности. – события $\{e_t(n_i)\}_{n_i \in N, t \in \Delta t}$, собираемые в журналах на узлах n_i в пределах промежутка Δt. Пример такого события – АТ-команды *ND*, направляемая узлу-получателю в виде широковещательного запроса для сканирования ZigBee-сети для получения сведений об актуальных узлах-соседях данного узла. – показания цифровых и аналоговых сенсоров $\{(s_i, p_i)\}$, которые могут быть подключены непосредственно к цифровым или аналоговым пинам микроконтроллера, одноплатного компьютера или беспроводного интерфейса XBee. В рамках разработанного стенда на каждом узле $R_0 - R_6$ осуществляется периодическое снятие показаний температуры, концентрации CO_2 и влажности в качестве ключевых характеристик состояния атмосферного воздуха. Вместе с тем специализированных исполнительных механизмов в рамках стенда не предусмотрено.

Таблица 4 – Выполнение стадии предобработки данных

Стадия методики	Действия	Описание

Стадия 2. Предобработка данных	Унификация данных	На данной стадии осуществляется приведение разнородных данных, получаемых из различных источников, к единому формату представления данных. Формируемые события системы мониторинга состояния атмосферного воздуха записываются в JSON-формате. Ниже приведен пример события получения значения датчика температуры с узла R_2:
		{
		“event_id”: “123”,
		“timestamp”: “2025-03-05T10:30:00Z”,
		“node_id”: “R02”,
		“location”: {
		“lat”: 51.166667,
		“lon”: 71.433333
		},
		“sensor_data”: {
		“sensor_type”: “temperature”,
		“value”: 19.3,
		“status”: “in_progress”
		},
		“alerts”: [
		{
		“type”: “info”,
		“message”: “Inside threshold bounds.”
		}
		]
		}

	Устранение и исправление ошибочных и пропущенных значений	– фильтрация событий с неполными данными. – фильтрация событий с данными вне заданных диапазонов на основе ограничений вида $s_i(p_i) \in [s_i^{(min)}, s_i^{(max)}]$ на заданные сенсоры температуры, влажности, углекислого газа и пр. для каждого из узлов.
	Фильтрация данных	– удаление лишней, ненужной для последующего анализа информации, в том числе удаление показаний дублирующих сенсоров или сенсоров, значений которых не требуется сохранять в соответствии с бизнес-логикой и настройками оператора БСС
	Объединение данных с различных узлов	– построение и наполнение единого централизованного хранилища данных, использованием NoSQL базы MongoDB.
	Снижение размерности данных	В целевой БСС снижение размерности направлено в первую очередь для оптимизации объемов размеров хранилища данных в условиях ограничений узлов БСС, осуществляемое на узле-координаторе в рамках Raspberry Pi с использованием библиотеки Keras autoencoder = Model(input_layer, decoded) autoencoder.compile(optimizer=’adam’, loss=’binary_crossentropy’) autoencoder.fit(X_train, X_train, epochs=50, batch_size=256, shuffle=True, validation_split=0.2)
	Нормализация данных	– в целях обработки данных осуществляется min-max-нормализация с использованием библиотеки Sklearn scaler = MinMaxScaler(feature_range=(1, 2)) event = scaler.fit_transform(data)

Таблица 5 – Выполнение стадии анализа данных

Стадия методики	Действия	Описание
Стадия 3. Анализ данных	Извлечение признаков из предобработанных выборок данных	В части собираемых на узлах БСС исходящих и входящих пакетов беспроводного трафика БСС извлекаемые признаки характеризуют конкретные экземпляры пакетов данных, причем каждый пакет включает следующие признаки: номер последовательности пакета, тип пакета, идентификатор PAN ID сети, MAC-адрес источника, MAC-адрес получателя, длину полезной нагрузки, метку времени фактической доставки пакета на узел и некоторые другие поля. В части событий журналов узлов БСС анализируемые образцы данных включают идентификатор команды управления (Command ID), тип команды, основные параметры (название параметра и значение), Cluster ID для указания типа взаимодействия. В части цифровых и аналоговых сенсоров в первую очередь извлекаются тройки (n_i, s_j, p_j, ts), специфицирующие узел n_i, на котором располагается сенсор s_j, показание p_j с меткой времени ts.
	Формирование гипотезы для классификации	Формирование экспертным путем гипотезы о предполагаемой корреляции отдельных видов данных и целевой переменной классификации инцидентов безопасности.
	Конструирование признакового пространства	Следующие производные признаки используются в зависимости от вида инцидентов, которые необходимо выявлять: – статистики по узлам-источникам и получателям пакетов данных; – объемы полезной нагрузки пакетов данных; – статистические величины интервалов времени между пакетами данных; – дискретные значения плотности распределения пакетов данных по их типам; – различные статистические величины интенсивности трафика, в том числе максимальные, минимальные и усредненные значения задержек передачи данных, скорости поступления пакетов и байт в секунду; – доля потерянных и/или неправильно доставленных пакетов данных; – величины энергопотребления узлов БСС; – местоположения узлов БСС (с использованием GPS-координат или иного вида позиционирования в пространстве); – временные статистики доступности и активности узлов БСС и др.
	Выделения обучающих и валидационных выборок	Для обучения классификаторов применяется типовое разбиение на обучающую и тестовую выборки в соотношении 0,8 к 0,2 с учетом суммарного объема выборов и сбалансированности данных по классам.
	Определение требуемых значений показателей качества обнаружения	В качестве референсных значений по умолчанию выбраны значения точности, полноты и f1-меры, а также показателя ROC-AUC в размере 0,95.
	Выбор моделей и методов обучения	В качестве обучающих моделей используются следующие модели, осуществляющие классификацию с учителем на основе деревьев (Random Forest и AdaBoost), сверточная нейронная сеть на основе матриц изображений (CNN) Кроме того, применяется автоэнкодер для снижения размерности данных.
	Разметка данных и обучение с применением методов классификации	Разметка данных на их принадлежность нормальному и аномальному функционированию осуществляется экспертно с применением автоматизирующего скрипта, написанного на Python. Разметка конкретных образцов данных (событий, трафика, показаний сенсоров) проводится в первую очередь исходя из меток времени смоделированных инцидентов безопасности, а также идентификаторов узлов, инициаторов атаки и вовлеченных в нее.
	Комбинирование классификаторов	При недостижении установленных значений показателей качества классификации, а также в целях мультиклассификации однин из путей их повышения – дополнительное использование ансамблирования, включая стекинг и мажоритарное голосование.
	Тестирование классификаторов	Типовое тестирование построенных классификаторов осуществляется на установленной тестовой выборке данных.

Таблица 6 – Выполнение стадии визуальной аналитики

Стадия методики	Действия	Описание
Стадия 4. Визуальная аналитика	Подготовка источников и выборок данных для визуального анализа	Анализ источников данных об узлах БСС и их функционировании, в том числе журналы событий, сетевой трафик и показания сенсоров узлов.
	Подбор визуальных моделей	Используются следующие три основные визуальные модели: – график временного ряда для выявления и анализа аномальной сетевой активности при взаимодействии нескольких узлов БСС; – двумерные и трехмерные диаграммы рассеяния для определения отклонений в ключевых характеристиках событий, пакетов, показаний сенсоров, например для учета поддельных данных характеристик сенсоров температуры, влажности, энергопотребления, свидетельствующих о злонамеренной подделке данных мониторинга БСС. Кроме того, в случае контроля характеристик состояния атмосферного воздуха промышленного объекта или города такая модель визуализации используется также для определения кластеров нормального функционирования системы, что, в свою очередь, повысит осведомленность оператора БСС и повысит качество выявления аномалий; – тепловая карта, которая накладывается на фактическую схему топологии БСС для отображения интенсивности сетевой активности, энергопотребления, маршрутизации пакетов и других характеристик, изменения в которых являются признаками атак на БСС.
	Проверка и экспертная оценка визуальных моделей	Оценивание моделей на основе результатов их применения в случае конкретного фактического или моделируемого инцидента безопасности включает: – формирование машиночитаемых информационных признаков, подаваемых в качестве дополнительной информации на вход интеллектуальным моделям анализа данных в рамках стадии 3 методики; – оценку корректности и качества первичных данных, получаемых от БСС, в том числе данных нормального функционирования сети; – выявление дрейфа в данных с течением времени, что необходимо для своевременной корректировки и переобучения интеллектуальных моделей для выявления инцидентов безопасности; – для возможности повторного использования положительного опыта машинного обучения для выявления инцидентов на сходных кейсах (т.н. transfer learning); – для документирования и повышения человекочитаемости результатов интеллектуального анализа и обнаружения инцидентов в целях повышения эффективности обмена экспертными данными и расследования уже выявленных инцидентов.

Таблица 7 – Выполнение стадии поддержки принятия решений

Стадия методики	Действия	Описание
Стадия 5. Поддержка принятия решений	Принятие решений по реагированию на обнаруженные инциденты безопасности в БСС и выработка мер по реагированию на выявленный инцидент	Для БСС для контроля характеристик состояния атмосферного воздуха промышленного объекта города на данной стадии выполняются следующие действия: – оценка величины ущерба сервисам мониторига состояния атмосферного воздуха, включая последствия от неработоспособности БСС и финансовые затраты на ремонт оборудования инфраструктуры сети; – анализ возможных последствий дальнейшего продолжения и распространения анализируемой атаки; – принятие решения о дальнейших контрмерах, в том числе продолжение функционирования в ограниченном, автономном режиме; – документирование инцидентов в целях обеспечения расследования инцидентов.
	Уточнение и корректировка политик безопасности	Производится уточнение и корректировка политик безопасности для повышения устойчивости сети к будущим атакам, в том числе для: – дифференциации функций и минимизации привилегий узлов; – повышения защищенности БСС на аппаратном уровне; – повышения эффективности процессов аварийного восстановления после инцидентов; – резервирования узлов, мощностей, компонентов защищенного хранения данных.

Результаты классификации на основе методов Random Forest, AdaBoost и сверточной нейронной сети (CNN), выполненных на наборе предобработанных данных, включающих смоделированную комбинированную атаку с использованием wormhole и spoofing-воздействий приведены в таблице 8. В качестве наиболее важного показателя для оценки качества работы классификаторов и их сравнения был выбран показатель f1-меры, представляющий баланс между точностью выявления атаки и полнотой. Показатель приведен с округлением до 2 знаков после запятой.

Таблица 8 – Результаты классификации

Классификатор	F1-мера
Random Forest	0,97
AdaBoost	0,98
CNN	0,67

Таким образом, методы Random Forest и AdaBoost позволяют осуществить классификацию с интегральным показателем качества превышающем референсное значение 0,95, что, в свою очередь, подтверждает выполнимость предлагаемой методики на примере практического сценария работы БСС в рамках построенного стенда киберфизической системы для контроля характеристик состояния атмосферного воздуха промышленного объекта/города. Также отметим, что относительная схожесть результатов классификации для методов Random Forest и AdaBoost обуславливается там, что оба из них представляют ансамблированные методы, построенные на схожих принципах и основанные на деревьях решений. При этом лучшие результаты классификации у метода AdaBoost объясняются взаимосвязанностью отдельных

деревьев решений в процессе итерационного перебора, что более существенно для набора анализируемых данных.

Последующее совершенствование моделей классификации включает также отработку моделей при увеличении числа тестовых сценариев, а также расширение экспериментов для охвата других разновидностей комбинированных многошаговых воздействий на узлы БСС. В том числе предполагается анализ данных функционирования БСС под атакой, в рамках которой нарушитель использует поддельные идентификаторы узлов и манипулирует ими для перехвата данных и нарушений маршрутизации в сети.

Отметим, что в рамках предлагаемой методики расчет коэффициентов важности производится в целях оптимизации затрат аппаратных, коммуникационно-вычислительных ресурсов БСС, выделяемых на функционирование механизма обнаружения атак. Учитываются три вида ресурсов – вычислительные, коммуникационные и энергоресурсы. В зависимости от конкретного прикладного сценария коэффициенты позволяют выбирать те классификаторы из имеющихся, затраты на функционирование которых сбалансированы и в наибольшей степени близки к ресурсным требованиям рассматриваемого сценария. Например, в случае мобильных сетей мониторинга местности, узлы которых монтируются на беспилотные летательные аппараты, характеризующиеся строго ограниченным максимальным временем полета, наиболее важным представляется энергоресурс, тогда как вычислительные и коммуникационные ресурсы оказывают меньшее влияние на достижение целей миссии. И поэтому вычислительными и коммуникационными ресурсами в данном вопросе, вероятно, можно пренебречь.

Отметим, что в общем случае разработанная методика позволяет обеспечить значительное улучшение качества и скорости обнаружения инцидентов безопасности в беспроводных сенсорных сетях, а также оперативно выявлять как внешние, так и внутренние угрозы. Это способствует повышению устойчивости таких сетей к различного вида атакам, таким как DDoS, подмена данных, манипуляции с маршрутизацией и другие типы злонамеренных воздействий. Кроме того, это будет способствовать снижению рисков возникновения длительных перебоев в работе критически важных объектов, производственных комплексов, инфраструктур медицинских учреждений и городских служб мониторинга окружающей среды. В результате внедрения методики персонал сможет быстрее реагировать на инциденты, локализовать их влияние и минимизировать возможный ущерб, что приведет к поддержанию стабильности и надежности всей инфраструктуры. Также накопление данных о выявленных инцидентах даст возможность прогнозировать и предотвращать будущие атаки, что дополнительно повышает уровень киберфизической безопасности БСС.

Заключение

В статье исследуются вопросы киберфизической безопасности беспроводных сенсорных сетей и особенности обнаружения атак в таких сетях с учетом их архитектурных и ресурсных ограничений. Предложена комплексная методика для выявления инцидентов, способствующая более быстрому обнаружению широкого класса атак и минимизации ущерба от них. В качестве направлений дальнейшей работы по данной тематике предполагаются исследования по применению алгоритмов и средств обнаружения состязательных атак (adversarial attacks) на механизмы киберфизической безопасности и мониторинга уровня защищенности БСС.

Информация о финансировании. Работа проводится в рамках AP23489127 «Модели и алгоритмы повышения защищенности киберфизических систем промышленного интернета вещей с использованием граничных вычислений».

ЛИТЕРАТУРА

1 Alansari, Z., Anuar, N.B., Kamsin, A., Belgaum, M.R. A systematic review of routing attacks detection in wireless sensor networks. PeerJ Computer Science, 8, e1135 (2022).

2 Kaushal, K., Kaur, T. A survey on attacks of WSN and their security mechanisms. International Journal of Computer Applications, 118 (18) (2015).

3 Ali, A., Ming, Y., Chakraborty, S., Iram, S. A comprehensive survey on real-time applications of WSN. Future Internet, 9 (4), 77 (2017).

4 Kamaruzzaman, M., Chandra, A. Integration of wireless sensor network in robotics. Machine Learning for Robotics Applications, 71–84 (2021).

5 Elsadig, M.A. Detection of denial-of-service attack in wireless sensor networks: A lightweight machine learning approach. IEEE Access, 11, 83537–83552 (2023).

6 Ismail, S., El Mrabet Z., Reza, H. An ensemble-based machine learning approach for cyber-attacks detection in wireless sensor networks. Applied Sciences, 13 (1), 30 (2022).

7 Sharma, N., Kaushik, I., Agarwal, V.K., Bhushan, B., Khamparia, A. Attacks and security measures in wireless sensor network. Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications, 237–268 (2021).

8 Oztoprak, A., Hassanpour, R., Ozkan, A., Oztoprak, K. Security challenges, mitigation strategies, and future trends in wireless sensor networks: A review. ACM Computing Survey, 57 (4), 1–29 (2024).

9 Monjur, M.M.R., Heacock, J., Calzadillas, J., Mahmud, M.S., Roth, J., Mankodiya, K., Yu, Q. Hardware security in sensor and its networks. Frontiers in Sensors, 3, 850056 (2022).

10 Chen, Y.Y., Xu, B., Long, J. Information security assessment of wireless sensor networks based on bayesian attack graphs. Journal of Intelligent & Fuzzy Systems, 41 (3), 4511–4517 (2021).

11 Subasini, C.A., Karuppiah, S.P., Sheeba, A., Padmakala, S. Developing an attack detection framework for wireless sensor network- based healthcare applications using hybrid convolutional neural network. Transactions on Emerging Telecommunications Technologies, 32 (11), e4336 (2021).

12 Delwar, T.S., Aras, U., Mukhopadhyay, S., Kumar, A., Kshirsagar, U., Lee, Y., et al. The intersection of machine learning and wireless sensor network security for cyber-attack detection: a detailed analysis. Sensors, 24 (19), 6377 (2024).

13 Premkumar, M., Ashokkumar, S.R., Jeevanantham, V., Mohanbabu, G., AnuPallavi, S. Scalable and energy efficient cluster based anomaly detection against denial of service attacks in wireless sensor networks. Wireless Personal Communications, 129 (4), 2669–2691 (2023).

14 Chen, N., Qiu, T., Daneshmand, M., Wu, D.O. Robust networking: Dynamic topology evolution learning for Internet of Things. ACM Transactions on Sensor Networks (TOSN),17 (3), 1–23 (2021).

15 Duan, G., Lv H., Wang H., Feng G., Li X. Practical cyber attack detection with continuous temporal graph in dynamic network system. IEEE Transactions on Information Forensics and Security (2024).

16 Nguyen, V.L., Lin, P.C., Hwang, R.H. Energy depletion attacks in low power wireless networks. IEEE Access, 7, 51915–51932 (2019).

17 Poornima, I.G.A., Paramasivan, B. Anomaly detection in wireless sensor network using machine learning algorithm. Computer Communications, 151, 331–337 (2020).

18 Ayadi, A., Ghorbel, O., Obeid, A.M., Abid, M. Outlier detection approaches wireless sensor networks: A survey. Computer Networks, 129, 319–333 (2017).

19 Rajasegarar, S., Leckie, C., Palaniswami, M. Anomaly detection in wireless sensor networks. IEEE Wireless Communications, 15 (4), 34–40 (2008).

20 Lakshmi, H.N., Anand, S., Sinha, S. Flooding attack in wireless sensor network-analysis and prevention. International Journal of Engineering and Advanced Technology, 8 (5), 1792–1796 (2019).

21 Dubey, A., Meena, D., Gaur, S. A survey in hello flood attack in wireless sensor networks. International Journal of Engineering Research and Technology, 3, 1882–1887 (2014).

22 Hu, Y.C., Perrig, A., Johnson, D.B. Wormhole attacks in wireless networks // IEEE Journal on Selected Areas in Communications, 24 (2), 370–380 (2006).

23 Rehman, A.U., Rehman, S.U., Raheem, H. Sinkhole attacks in wireless sensor networks: A survey. Wireless Personal Communications, 106, 2291–2313 (2019).

24 Xiao, L., Greenstein, L.J., Mandayam, N.B., Trappe, W. Channel-based detection of sybil attacks in wireless networks. IEEE Transactions on Information Forensics and Security, 4 (3), 492–503 (2009).

25 de Oliveira, M.S., Steffen, V., de Francisco, A.C., Trojan, F. Integrated data envelopment analysis, multi-criteria decision making, and cluster analysis methods: Trends and perspectives. Decision Analytics Journal, 8, 100271 (2023).

26 Jiang, Y., Atif, Y., Ding, J. Cyber-physical systems security based on a cross-linked and correlated vulnerability database. International Conference on Critical Information Infrastructures Security (Cham: Springer International Publishing, 2019), pp. 71–82.

27 Marsh, D.W., Baldwin, R.O., Mullins, B.E., Mills, R.F., Grimaila, M.R. A security policy language for wireless sensor networks. Journal of Systems and Software, 82 (1), 101–111 (2009).

28 Livani, M.A., Abadi, M. A PCA-based distributed approach for intrusion detection in wireless sensor networks. 2011 International Symposium on Computer Networks and Distributed Systems (CNDS) (IEEE, 2011), pp. 55–60.

29 Luo, T., Nagarajan, S.G. Distributed anomaly detection using autoencoder neural networks in WSN for IoT. 2018 IEEE International Conference on Communications (ICC) (IEEE, 2018), pp. 1–6.

30 John, A., Isnin, I.F.B., Madni, S.H.H., Faheem, M. Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms. Intelligent Systems with Applications, 22, 200381 (2024).

31 Zahra, F., Jhanjhi, N.Z., Brohi, S.N., Khan, N.A., Masud, M., AlZain, M.A. Rank and wormhole attack detection model for RPL-based internet of things using machine learning. Sensors, 22 (18), 6765 (2022).

32 Alghamdi, R., Bellaiche, M. A cascaded federated deep learning based framework for detecting wormhole attacks in IoT networks. Computers & Security, 125, 103014 (2023).

33 Zhukabayeva, T., et al. A traffic analysis and node categorization-aware machine learning-integrated framework for cybersecurity intrusion detection and prevention of WSNs in smart grids. IEEE Access, 2024.

34 Adamova, A., Zhukabayeva, T., Mardenov, Y. Machine learning in action: An analysis of its application for fault detection in wireless sensor networks. 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST) (IEEE, 2023), pp. 506–511.

35 Mardenov, Y., Adamova, A., Zhukabayeva, T., Othman, M. Enhancing fault detection in wireless sensor networks through support vector machines: A comprehensive study. Journal of Robotics and Control (JRC), 4 (6), 868–877 (2023).

36 Zhukabayeva, T., Adamova, A., Karabayev, N., Mardenov, Y., Satybaldina, D. Comprehensive vulnerability analysis and penetration testing approaches in smart city ecosystems. 2024 8th International Symposium on Innovative Approaches in Smart Technologies (ISAS) (IEEE, 2024), pp. 1–6.

[1,2]*Жукабаева Т.К.,
PhD, профессор, ORCID ID: 0000-0001-6345-5211,
*e-mail: zhukabayeva tk@enu.kz
[1,3]Марденов Е.М.,
магистр, ORCID ID: 0000-0001-9284-9797,
e-mail: emardenov@gmail.com
[2]Танирбергенов А.Ж.,
т.ғ.к., доцент м.а., ORCID ID: 0009-0000-8401-5434,
e-mail: t.adilbek@mail.ru

[1]«Астана» халықаралық ғылыми кешені, Астана қ., Қазақстан
[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан
[3]Astana International University, Астана қ., Қазақстан

СЫМСЫЗ СЕНСОРЛЫҚ ЖЕЛІЛЕРДЕГІ ҚАУІПСІЗДІК ИНЦИДЕНТТЕРІН АНЫҚТАУ ЖӘНЕ ТАЛДАУҒА АРНАЛҒАН КЕШЕНДІ ӘДІСТЕМЕ

Андатпа

Мақалада сымсыз сенсорлық желілердің (ССЖ) киберфизикалық қауіпсіздігі мәселелері қарастырылады. Қазіргі заманғы ССЖ sinkhole және wormhole шабуылдары, «ортадағы адам» типіндегі шабуылдар, деректерді алмастыру, әмбебап желілік шабуылдар және т.б. сияқты кең ауқымды қауіптерге осал. Тәжі-

рибеде мұндай шабуылдардан қорғануға ықпал ететін факторлардың әртүрлілігі, инфрақұрылымның тар бағытталған ерекшелігі және желі түйіндерінің шектеулі ресурстары кедергі келтіреді. Бұл мақалада ССЖ-дегі қауіпсіздік инциденттерін анықтауға арналған кешенді әдістеме ұсынылады. Ол шабуылдарды тиімді анықтауға және инциденттерге уақытылы әрекет етуге мүмкіндік береді, бұл өз кезегінде ықтимал зиянды азайтып, желінің үздіксіз жұмысын қамтамасыз етеді. Ұсынылған әдістеменің жаңалығы оның кешенділігінде, әртүрлі киберфизикалық қауіп-қатерлерді анықтау қабілетінде және ССЖ түйіндерінің таралған құрылымы мен құрамындағы өзгерістер динамикасын ескере отырып, инциденттерді жоғары дәлдікпен және толықтықпен айқындауында жатыр. Әдістеме ZigBee протоколы негізінде жұмыс істейтін және өндірістік нысанның немесе қаланың атмосфералық ауасының сипаттамаларын бақылауға арналған ССЖ фрагментінде сынақтан өткізілді. Дамытылған әдістеме сымсыз сенсорлық желілердегі қауіпсіздік инциденттерін анықтау сапасы мен жеделдігін арттырып, желілердің ішкі және сыртқы зиянды әсерлерге төзімділігін жоғарылатады және шабуыл сәтті болған жағдайда инфрақұрылым жұмысының ұзақ уақытқа тоқтап қалуын болдырмайды.

Тірек сөздер: сымсыз сенсорлық желі, қауіпсіздік инциденті, анықтау, модельдеу, әдістеме.

[1,2]*Zhukabayeva T.K.,
PhD, Professor, ORCID ID: 0000-0001-6345-5211,
*e-mail: zhukabayeva tk@enu.kz
[1,3]Mardenov E.M.,
MSc, ORCID ID: 0000-0001-9284-9797,
e-mail: emardenov@gmail.com
[2]Tanirbergenov A.,
PhD, acting Associate Professor, ORCID ID: 0009-0000-8401-5434
e-mail: t.adilbek@mail.ru

[1]International Scientific Complex «Astana», Astana, Kazakhstan
[2]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
[3]Astana International University, Astana, Kazakhstan

COMPLEX TECHNIQUE FOR DETECTION AND ANALYSIS OF SECURITY INCIDENTS IN WIRELESS SENSOR NETWORKS

Abstract

The article comprises issues of cyber-physical security of wireless sensor networks (WSN). Modern WSNs are vulnerable to a wide class of attacks, such as sinkhole and wormhole attacks, man-in-the-middle attacks, data substitution attacks, universal network attacks, etc. In practice, the ability to protect WSNs from this type of attacks is hampered by the variety of possible impacts, highly specialized focus of the infrastructure and limited resources of network nodes. This article proposes a comprehensive technique for identifying security incidents in WSNs for effective attack detection and incident response, which will minimize potential damage and ensure uninterrupted network operation. The novelty of the technique includes its complexity, the ability to identify various cyber-physical threats and ensure high accuracy and completeness of incident detection, taking into account the distributed structure and dynamics of changes in the composition of WSN nodes. The technique has been tested on a WSN fragment operating on the ZigBee protocol to monitor the characteristics of the atmospheric air of an industrial facility or a city. The developed technique will help improve the quality and timeliness of detecting security incidents in wireless sensor networks, which will enhance the resilience of networks to external and internal malicious influences and prevent long-term interruptions in the operation of the infrastructure in the event of successful attacks.

Keywords: wireless sensor network, security incident, detection, modeling, technique.

Дата поступления статьи в редакцию: 04.05.2025