Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский государственный нефтяной технический университет»

при поддержке:
Российской академии естественных наук
Академии наук Республики Башкортостан
Общественной организации
«Профессионалы дистанционного обучения»
Ассоциации образовательных программ
«Электронное образование Республики Башкортостан»
Российского союза научных и инженерных
общественных объединений

Информационные технологии
Проблемы и решения

Посвящается 75-летию Уфимского государственного
нефтяного технического университета

У ф а
УНПЦ «Издательство УГНТУ»
2 0 2 3

ОГЛАВЛЕНИЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В НАУКЕ, ОБРАЗОВАНИИ И ПРОИЗВОДСТВЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ, УПРАВЛЕНИИ И БИЗНЕСЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ГЛАЗАМИ ШКОЛЬНИКА

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

пользователь, данные виды атак, которые были приведены в статье, являются каплей в море, и имеют более частый характер применения. На практике могут встретиться и другие виды атак или комбинированные с приведенными выше видами и у всех них стоит главная задача — обмануть пользователя и заставить его добровольно выдать свои данные. Поэтому необходимо постоянная работа в области социальной инженерии не только с детьми, но и взрослыми, так как нарушение информационной безопасности может привести к потерям данных, как личного характера, так и коммерческой тайны.

Литература

1. Актуальные киберугрозы: IV квартал 2022 года — URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q4/ (дата обращения: 19.03.2023).

2. Как заработать на БЛОГЕРАХ? Фонд Блогеров обман – ЧЁРНЫЙ СПИСОК #74 — URL: https://www.youtube.com/watch?v=BBgHgD1fanI (дата обращения: 25.03.2023).

3. Как избежать атаки с использованием социальной инженерии — URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks (дата обращения: 19.03.2023).

4. Краткое введение в социальную инженерию — URL: https://habr.com/ru/post/83415/ (дата обращения: 19.03.2023).

УДК 004.056

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ К ОТКАЗАМ И СБОЯМ

RESEARCH THE VULNERABILITIES OF WIRELESS SENSOR NETWORKS TO FAILURES AND FAULTS

Мехтиев Ш.А., Рзаева Н.А.,
Институт информационных технологий, г. Баку, Азербайджан

Sh.A. Mehdiyev, N.A. Rzayeva,
Institute of Information Technology, Baku, Azerbaijan

e-mail: shakir.mehtieff@gmail.com

Аннотация. Беспроводные сенсорные сети (БСС) привлекли большое внимание из-за их большого потенциала для использования в различных приложениях. По сравнению с классическими сетями БСС могут работать практически в любой среде, особенно там, где проводная связь невозможна. Как правило, БСС состоят из сенсорных устройств с батарейным питанием, оснащенных вычислительными, запоминающими и коммуникационными компонентами. БСС широко используются в различных по назначению системах, таких как мониторинг окружающей среды, промышленная автоматизация, здравоохранение, умные города и другие инфраструктурные проекты, которые необходимы для поддержания национальной безопасности, экономической жизнеспособности, здоровья и безопасности населения.Поэтому понимание и снижение уязвимостей БСС к сбоям и отказам имеет решающее значение для обеспечения их надежной работы. В статье исследуются различные типы отказов и сбоев, которые могут возникнуть в БСС, включая сбои и отказы сенсорных узлов, беспроводной связи, питания, программного обеспечения и другие. Анализируются причины, влияние и последствия этих сбоев и отказов на работу БСС.

Abstract. Wireless sensor networks (WSNs) have attracted significant attention due to their immense potential for various applications. Compared to traditional wired networks, WSNs can operate in virtually any environment, particularly where wired communication is not feasible. Typically, WSNs consist of battery-powered sensor devices equipped with computing, storage, and communication components. WSNs are widely used in systems for various purposes such as environmental monitoring, industrial automation, healthcare, smart cities, and other infrastructure projects that are necessary to maintain national security, economic viability, public health, and safety. Therefore, understanding and mitigating the vulnerabilities of WSNs to failures and faults is crucial for ensuring their reliable operation. The article explores the various types of failures and faults that can occur in a WSN, including failures and faults of sensor nodes, wireless communications, power, software, etc. The causes, impacts, and consequences of these failures and faults in WSN operation are analyzed.

Ключевые слова: беспроводные сенсорные сети, сенсорные узлы, безопасность, уязвимость, сбои, отказы.

Keywords: wireless sensor networks, sensor nodes, security, vulnerability, failures, faults.

Введение

Беспроводная сенсорная сеть (БСС) является на сегодня устоявшимся термином для описания архитектуры сети, состоящей из множества самоорганизующихся беспроводных сенсорных узлов, которые могут собирать, передавать и обрабатывать данные из окружающей среды [1]. Причинно-следственные связи между технологиями производства мини, микро и наносенсоров, интернет-протоколом нового поколения IPv6, снявшего ограничения на количество подключаемых датчиков и устройств, и внедрение энергоэффективных протоколов беспроводной связи способствовали использованию БСС в различных приложениях мониторинга и управления, которые ранее считались дорогими, сложными или даже невозможными в осуществлении. Критическая инфраструктура, общественная и национальная безопасность, чрезвычайные ситуации; экологический мониторинг, здравоохранение, транспорт и логистика – это неполный перечень различных применений БСС.

Однако такое разнообразие использования создает серьезные ограничения для решения специфических задач безопасности и надежности в БСС, которые могут сталкиваться с множеством проблем, связанных со сбоями и отказами [2].

Известно, что под отказом понимаются непредвиденные и нежелательные прекращения работы технической системы или ее компонент. Отказы могут возникнуть по различным причинам, таким как неправильная конструкция, износ, воздействие внешних факторов, ошибки в проектировании, человеческий фактор, а также технические несоответствия, программные проблемы и другие. Отказы могут иметь различные последствия, от незначительных сбоев в работе системы до серьезных проблем, включая остановку производственных процессов, потерю данных, финансовые потери, потерю репутации и даже угрозу безопасности.

Сбой – это неполадка или нарушение в работе технической системы или ее компонент, который приводит к некорректному функционированию или неправильному выполнению задачи системой. Сбои могут быть вызваны различными причинами, такими как ошибки в программном обеспечении, аппаратные проблемы, неправильная конфигурация или взаимодействие между компонентами системы, ошибки ввода данных и другие факторы.

Существует ряд стандартов и методологий, таких как ITIL (InformationTechnologyInfrastructureLibrary), ISO 20000 (международный стандарт для управления ИТ-сервисами), ISO 9001 (международный стандарт системы менеджмента качества) и другие, которые предоставляют руководство и рекомендации по управлению отказами и сбоями в технических системах. Эти стандарты описывают процессы, методы и

практики, которые могут быть использованы организациями для предотвращения, обнаружения, устранения и управления отказами и сбоями с целью обеспечения более надежной работы технических систем и минимизации возможных негативных последствий.

Методы, описанные в [3], могут быть использованы при проектировании и эксплуатации надежных БСС, включая:

- профилактические меры для предотвращения сбоев и отказов;
- обеспечение непрерывного предоставления услуг при возникновении сбоев и отказов;
- меры по устранению сбоев и отказов, а также снижению их числа и серьезности;
- прогнозирование возможных сбоев и отказов, оценка частоты их возникновения и потенциальных последствий.

Уязвимости сенсорных узлов и БСС

Важно отметить, что под уязвимостью понимается нежелательное состояние системы, которое может быть использовано злоумышленниками для атак и нарушения безопасности. Определим, что устойчивое, надежное и эффективное функционирование БСС тесно связано с рядом уязвимостей, которые определяют политику управления сбоями и отказами. Ошибки в такой политике могут привести к снижению надежности и производительности БСС. Неконтролируемые сбои и отказы могут вызвать потерю данных, прерывания в работе системы и нарушение доставки критически важных сервисов. Далее рассмотрены некоторые свойства и характеристики БСС, которые могут стать причиной возникновения уязвимостейи создать проблемы для устойчивого функционирования.

Так, например, свойство мобильности, присущее сенсорным узлам, установленным на автомобилях или роботах, может потребовать более сложного управления ресурсами, высокой надежности сетевых соединений и мобильного оборудования, а также сложных механизмов обеспечения безопасности данных и защиты от внешних угроз.

Беспроводные каналы по своей природе подвержены помехам, затуханию сигнала и другим факторам окружающей среды, которые могут привести к потере пакетов, задержке и уменьшению покрытия сети. Обеспечение надежной и устойчивой беспроводной связи имеет решающее значение для поддержания общей производительности и отказоустойчивости БСС.

Ограниченные вычислительные ресурсы, память и энергоэффективность сенсорных узлов не позволяют реализовать высокопроизводительные алгоритмы обработки данных и сложную аналитику, сложные механизмы защиты и шифрования данных. Из-за недостаточной кибербезопасности и неприменения соответствующих мер

по защите данных как непосредственно в сенсорных узлах, так и в инфраструктуре беспроводной сети (базовые станции, шлюзы), существуют вероятности киберугроз, таких, как перехват, подмена или дискредитация данных, а также атаки на протоколы связи или на сетевую инфраструктуру.

Недостаток стандартов безопасности и единых принципов защиты данных для БСС может приводить к неправильной или неполной реализации мер безопасности, а также затруднять оценку уровня безопасности системы в целом.

Различные устройства могут иметь различные уровни безопасности, а их динамическая природа, такая как перемещение или добавление/удаление из сети, может создавать сложности в установлении и поддержании защиты данных.

Возможность проникновения в БСС через физически незащищенные точки доступа, неправильно сконфигурированные сетевые устройства или слабые пароли может создавать риски несанкционированного доступа к данным или нарушения конфиденциальности.

Сенсорные сети могут быть уязвимы к атакам на физические параметры среды, в которой они работают. Например, атакующий может изменить условия окружающей среды, такие как освещение, температура или влажность, чтобы исказить измеряемые сенсорами данные или вызвать ошибки в их работе.

Атаки на управление энергопотреблением: БСС могут быть подвержены атакам, направленным на их энергопотребление и энергоснабжение. Например, атакующий может осуществлять атаку "потребление энергии" (EnergyDepletion), принуждая сенсорные узлы работать в режиме высокого энергопотребления, что снижает их жизненный цикл и надежность работы[4].

Использование технологий социальной инженерии может быть направлено на обман пользователей или администраторов сети, чтобы получить доступ к сенсорным узлам или системам управления. Например, злоумышленник может отправлять фишинговые электронные письма или проводить атаки методом "внутренней угрозы" (InsiderThreat), получая доступ к системам от имени сотрудника организации или пользователя сети и возможность осуществлять незаконные действия, такие как, несанкционированный доступ к данным, кража информации или нарушение политик безопасности [5].

Таким образом уязвимости могут проявляться на разных уровнях, включая аппаратное обеспечение, программное обеспечение и протоколы связи, и требуют комплексного подхода к их решению.

Методы противодействия отказам и сбоям в БСС

БСС являются активной областью исследований свыше 20-ти лет. Во многих работах дается всесторонний анализ БСС с акцентом на вопросы безопасности и методы противодействия отказам и сбоям; рассматриваются аппаратные и протокольные архитектуры; предлагается системный подход к изучению различных алгоритмов и техник для обнаружения и устранения ошибок в БСС, включая техники резервирования, репликации и дублирования данных [6, 7].

В [8] предлагается обзор различных методов противодействия отказам и сбоям в БСС, включая методы обнаружения, коррекции и восстановления ошибок. Здесь также рассматриваются проблемы и вызовы, связанные с надежностью и безопасностью, и предлагаются подходы для повышения устойчивости БСС.

В [9] рассматриваются методы противодействия отказам и сбоям маршрутизации в БСС. Исследованы различные алгоритмы и протоколы, предназначенные для обеспечения надежной и устойчивой маршрутизации в условиях переменных сетевых условий и отказов сенсорных узлов.

В [10] рассматриваются методы противодействия отказам и сбоям в синхронных системах передачи сообщений, такие как техники репликации, кодирования и дублирования данных, а также протоколы обнаружения и восстановления ошибок.

На основе проведенного краткого обзора по обеспечению отказоустойчивости БСС на различных уровнях архитектуры сети можно выделить основные методы противодействия отказам и сбоям.

Уровень аппаратного обеспечения.

Этот уровень включает в себя физическое оборудование сети, такое как сенсорные узлы, антенны и источники питания, а также другие компоненты. Для обеспечения отказоустойчивости на уровне аппаратного обеспечения могут быть применены методы, такие как установка дополнительных резервных источников питания, использование множества антенн на разных местах, а также улучшение устойчивости к внешним воздействиям, например, к влаге, пыли, температурным экстремумам.

Уровень программного обеспечения.

Этот уровень включает в себя программное обеспечение, работающее на сенсорных узлах и отвечающее за управление сетью, передачу данных, маршрутизацию и другие функции. Для обеспечения отказоустойчивости на уровне программного обеспечения могут быть использованы методы, такие как дублирование данных на нескольких узлах, автоматический выбор альтернативных маршрутов при обнаружении сбоев, а также использование распределенных алгоритмов принятия решений.

Уровень сетевой архитектуры.

Этот уровень включает в себя организацию и структуру сети, включая топологию, протоколы маршрутизации, методы сбора данных и другие аспекты. Для обеспечения отказоустойчивости на уровне сетевой архитектуры могут быть использованы методы, такие как использование резервных узлов и каналов связи, а также реализация механизмов обнаружения и восстановления отказов.

Уровень прикладных приложений.

Этот уровень включает в себя прикладные приложения, которые используют данные, собранные сенсорными узлами сети. Для обеспечения отказоустойчивости на уровне прикладных приложений могут быть применены методы, такие как репликация данных на разных узлах, использование механизмов кэширования для локальной обработки данных на узлах, использование кодирования и шифрования данных для защиты от потери или несанкционированного доступа.

Дополнительно для противодействия уязвимостям в БСС можно использовать также следующий инструментарий.

Мониторинг и управление ресурсами в БСС.

Систематический мониторинг ресурсов, таких как процессорное время, память и сетевая пропускная способность, может помочь выявить несанкционированное использование ресурсов, что может стать источником уязвимостей, таких как перегрузка сети, истощение ресурсов или злоупотребление доступом.

Методы защиты от внешних угроз.

Эти методы включают в себя использование механизмов аутентификации и авторизации, шифрования данных, механизмов обнаружения вторжений и других мер безопасности. Обеспечение конфиденциальности, целостности и доступности данных, передаваемых и хранящихся в БСС, имеет решающее значение для предотвращения несанкционированного доступа, подделки и утечки данных. Следует отметить, что обучение сотрудников методам защиты данных, обновление их знаний в области безопасности и регулярное уведомление о потенциальных угрозах также могут помочь предотвратить ошибки и неправильные действия, которые могут стать источниками уязвимостей в БСС.

Заключение

Инновационные кибернетические экосистемы, такие как БСС, обладают огромным потенциалом для применения в различных отраслях, включая промышленность, здравоохранение, транспорт, сельское хозяйство и др. Они могут применяться в широком спектре сфер деятельности,

предлагая решения и возможности для оптимизации бизнес-процессов, улучшения безопасности и эффективности работы в различных секторах экономики. Чтобы успешно развернуть и эксплуатировать устойчивые к отказам и сбоям БСС, необходимо решить ряд вызовов, связанных с их надежностью, энергоэффективностью, управлением и безопасностью. Внедрение современных механизмов аутентификации и авторизации, использование шифрования данных, мониторинг и обнаружение инцидентов, регулярное тестирование на безопасность, создание стандартов и использование новых технологий, таких как блокчейн, в сочетании с обучением персонала и созданием культуры безопасности могут значительно повысить уровень защиты БСС и обеспечить их безопасную и надежную работу. Дальнейшие исследования и разработки в этой области имеют важное значение для обеспечения устойчивости и безопасности БСС, а также их успешного применения в различных сферах экономики и общества.

Эта работа поддержана Научным Фондом Государственной Нефтяной Компании Азербайджанской Республики (SOCAR) (Контракт № 3LR-AMEA).

Литература

1. Алгулиев Р. М. и др. Сенсорные сети: состояние, решения и перспективы // Телекоммуникации. – 2007. – №. 4. – С. 27-33.

2. Mehdiyev S. On Monitoring the Technical Condition and Technological Safety of Functional Elements of the Cyber-Physical Infrastructure //Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems. – IOS Press, 2022. – С. 18-26.

3. Avizienis A., Laprie J. C., Randell B. Fundamental concepts of dependability // Department of Computing Science Technical Report Series. – 2001.

4. Nguyen V. L., Lin P. C., Hwang R. H. Energy depletion attacks in low power wireless networks // IEEE Access. – 2019. – Т. 7. – С. 51915-51932.

5. Theoharidou M. et al. The insider threat to information systems and the effectiveness of ISO17799 // Computers & Security. – 2005. – Т. 24. – №. 6. – С. 472-484.

6. Bari A. et al. Design of fault tolerant wireless sensor networks satisfying survivability and lifetime requirements // Computer Communications. – 2012. – Т. 35. – №. 3. – С. 320-333.

7. Selmic R. R., Phoha V. V., Serwadda A. Wireless Sensor Networks: Security, Coverage, and Localization. – Springer, 2018.

8. Banerjee I., Rahaman H., Samanta T. Fault-Tolerant Routing in Wireless Sensor Networks. – 2017.

9. Mahmood M. A., Seah W. K. G., Welch I. Reliability in wireless sensor networks: A survey and challenges ahead // Computer networks. – 2015. – Т. 79. – С. 166-187.

10. Raynal M. Fault-tolerant agreement in synchronous message-passing systems // Synthesis Lectures on Distributed Computing Theory. – 2010. – Т. 1. – №. 1. – С. 1-189.

УДК 004

ЭТАПЫ РАЗРАБОТКИ ПРОГРАММНОГО ПРОДУКТА ДЛЯ СБОРА ОСНОВНЫХ СВЕДЕНИЙ ОБ АППАРАТНОМ ОБЕСПЕЧЕНИИ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

STAGES OF SOFTWARE PRODUCT DEVELOPMENT FOR COLLECTING BASIC INFORMATION ABOUT THE HARDWARE OF A PERSONAL COMPUTER

Вершинин К.Е.,
Институт нефтепереработки и нефтехимии
ФГБОУ ВО УГНТУ в г. Салавате, г. Салават, Россия.

K.E. Vershinin,
Institute of Oil Refining and Petrochemistry
FSFEI HE USPTU in Salavat, Salavat, Russia.

e-mail: vlone.kirill@yandex.ru

Аннотация. Статья рассматривает разработку программного продукта, предназначенного для сбора информации об аппаратном обеспечении персональных компьютеров. В статье отмечается, что существующие проблемы с получением полной и централизованной информации о компьютерном аппарате могут затруднять обслуживание и обновление персонального компьютера (ПК). В связи с этим, был разработан программный продукт (ПП), обладающий простым интерфейсом и возможностью собирать информацию о процессоре, оперативной памяти, жестких дисках и базовых характеристиках системы. Основными преимуществами программы являются ее удобство использования и возможность экспорта полученной информации в различные форматы, такие как текстовый файл или excel-файл, для последующего анализа и обработки данных. Кроме того, автор отмечает,