УДК 004.716

ИМИТАЦИЯ АТАК В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ: ПОСТРОЕНИЕ ЭКСПЕРИМЕНТА И АНАЛИЗ РЕЗУЛЬТАТОВ

Е.М. Марденов[1, 2], Б. Ху Вен-Цен[1], А.А. Абдилдаева[1]
[1]*Международный научный комплекс «Астана», Астана, Казахстан*
[2]*Международный университет Астана, Астана, Казахстан*

Аннотация. В данной работе рассматривается моделирование атак на беспроводные сенсорные сети (БСС) с целью анализа их влияния на безопасность и работоспособность сети. В рамках исследования разработан стенд, имитирующий киберфизическую систему мониторинга атмосферного воздуха, построенный на основе ZigBee-сети с узлами на базе Arduino и Raspberry Pi. Основное внимание уделено моделированию атаки типа Wormhole, при которой злоумышленник создает нелегитимный канал связи между удаленными узлами, что приводит к нарушению маршрутизации и перехвату данных. Проведен анализ функционирования сети в условиях атаки и нормальной работы, а также разработаны подходы к выявлению подобного типа угроз. Представленные результаты могут быть полезны для дальнейшей разработки методов защиты БСС от атак на маршрутизацию.

Ключевые слова: беспроводные сенсорные сети, ZigBee, безопасность, атака Wormhole, киберфизические системы, маршрутизация, имитация атак, анализ уязвимостей, мониторинг воздуха, ZigBee-устройства.

SIMULATION OF ATTACKS IN WIRELESS SENSOR NETWORKS: EXPERIMENT DESIGN AND RESULT ANALYSIS

E.M. Mardenov[1, 2], B. Hu Wen-Tsen[1], A.A. Abdildayeva[1]
[1]*International Scientific Complex "Astana", Astana, Kazakhstan*
[2]*Astana International University, Astana, Kazakhstan*

Abstract. This study examines the simulation of attacks on wireless sensor networks (WSNs) to analyze their impact on network security and functionality. As part of the research, a testbed was developed to simulate a cyber-physical system for atmospheric air monitoring, built on a ZigBee network with nodes based on Arduino and Raspberry Pi. The primary focus is on modeling a Wormhole attack, in which an attacker creates an illegitimate communication channel between remote nodes, leading to routing disruption and data interception. The network's performance was analyzed under both attack conditions and normal operation, and approaches were developed for detecting such threats. The presented results may be useful for the further development of methods to protect WSNs from routing attacks.
Keywords: wireless sensor networks, ZigBee, security, Wormhole attack, cyber-physical systems, routing, attack simulation, vulnerability analysis, air monitoring, ZigBee devices.

Введение

Беспроводные сенсорные сети (БСС) представляют собой одну из ключевых технологий в современных киберфизических системах, обеспечивающих мониторинг окружающей среды, промышленных объектов, городской инфраструктуры и критически важных систем. Благодаря самоорганизующейся архитектуре, компактным размерам и низкому энергопотреблению, узлы таких сетей широко применяются в системах экологического мониторинга, умных городах, медицине и промышленной автоматизации. Однако, наряду с преимуществами, беспроводные сети подвержены различным видам атак, среди которых особую угрозу представляют атаки на маршрутизацию, такие как Wormhole (червоточина) [1].

Атака Wormhole представляет собой один из наиболее опасных типов атак на сетевой уровень БСС. Ее суть заключается в том, что злоумышленник создает скрытый высокоскоростной канал связи между двумя узлами сети, которые физически могут находиться далеко друг от друга. Это позволяет перехватывать, модифицировать и перенаправлять сетевой трафик, вводя в заблуждение легитимные узлы относительно реальной топологии сети. В результате атакующие узлы могут не только осуществлять перехват и анализ данных, но и нарушать нормальное функционирование сети, влияя на маршруты передачи сообщений [2]. Данный тип атаки особенно опасен для сетей, использующих протокол ZigBee, поскольку маршрутизация в таких сетях основана на минимальном количестве переходов (hops), а Wormhole-атака создает искусственно укороченные маршруты [3].

В данной работе представлена разработка экспериментального стенда для моделирования атак на беспроводные сенсорные сети, а также проведение анализа их воздействия на сеть. В качестве тестовой среды используется сеть из семи узлов, работающих по протоколу ZigBee с использованием модулей Digi XBee. Четыре узла построены на базе микроконтроллеров Arduino Uno, два узла – на одноплатных компьютерах Raspberry Pi, а один узел выполняет роль координатора сети и подключен к персональному компьютеру. Для моделирования атаки Wormhole используется канал связи GSM/GPRS между двумя атакующими узлами, что позволяет эмулировать нелегитимный высокоскоростной путь передачи данных.

Рис. 1. Вид на экспериментальный стенд
Fig. 1. View of the experimental stand

Атака Wormhole является одной из самых сложных для обнаружения, поскольку она не требует компрометации криптографических механизмов, а вместо этого использует уязвимости самой структуры сети. В связи с этим важно разрабатывать и тестировать новые методы выявления таких атак, включая мониторинг задержек передачи пакетов, анализ топологии сети и применение алгоритмов машинного обучения для обнаружения аномалий в маршрутизации [4].

Основной целью данной работы является исследование воздействия атаки Wormhole на беспроводные сенсорные сети и разработка подходов к ее обнаружению.

Научная новизна работы заключается в создании экспериментального стенда для анализа атак на беспроводные сенсорные сети и исследовании специфики их влияния на маршрутизацию в ZigBee-сетях. В отличие от существующих работ, в которых основное внимание уделяется теоретическому анализу угроз, в данной работе предложена практическая реализация атаки с использованием реального оборудования.

Основная часть

Беспроводные сенсорные сети (БСС) представляют собой распределенные системы, состоящие из множества узлов, взаимодействующих друг с другом для мониторинга окружающей среды, передачи данных и выполнения вычислительных задач. Каждый узел БСС, как правило, включает в себя сенсоры, микроконтроллер, модуль связи и источник питания. Эти сети широко применяются в таких областях, как промышленный контроль, экологический мониторинг, системы «умного города» и медицинские приложения [5].

Основными характеристиками БСС являются:

– самоорганизация – узлы сети автоматически формируют топологию, определяя маршруты передачи данных;

– ограниченные ресурсы – узлы обладают малым объемом памяти, низким энергопотреблением и ограниченной вычислительной мощностью;

– динамическая топология – конфигурация сети может изменяться из-за перемещения узлов или внешних воздействий;

– многохоповая маршрутизация – данные передаются от узла к узлу, поскольку не все узлы имеют прямую связь с конечным получателем.

Важной особенностью БСС является использование беспроводных технологий связи, таких как Wi-Fi, Bluetooth, ZigBee и LoRaWAN. В данной работе рассматривается технология ZigBee как одна из наиболее популярных для построения БСС.

Протокол ZigBee представляет собой стандарт для низкоэнергетичных беспроводных сетей, разработанный на основе IEEE 802.15.4. Он предназначен для создания энергоэффективных сетей с поддержкой самоорганизации и масштабируемости [6]. В ZigBee-сетях используются три типа устройств:

Координатор (Coordinator, C) – центральный узел сети, управляющий маршрутизацией и обеспечивающий взаимодействие с другими системами.

Роутеры (Routers, R) – промежуточные узлы, передающие трафик и поддерживающие сеть.

Рис. 2. Промежуточные узлы
Fig. 2. Intermediate nodes

Конечные устройства (End Devices, E) – узлы, собирающие данные, но не выполняющие функции ретрансляции.

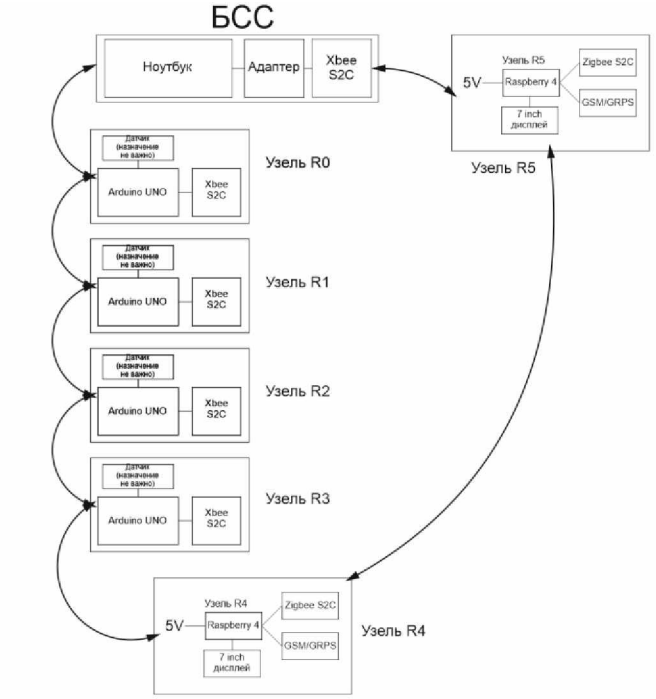

Рис. 3. Общая схема работы стенда
Fig. 3. General scheme of the stand operation

Для маршрутизации данных в ZigBee применяется протокол AODV (Ad hoc On-Demand Distance Vector Routing), который строит маршруты по запросу. Основные этапы маршрутизации в ZigBee:

Формирование сети – координатор инициирует создание сети и назначает уникальный PAN ID.

Обнаружение маршрута – узел, желающий отправить данные, отправляет широковещательный запрос (route request).

Выбор маршрута – узлы пересылают запрос, а конечный узел отправляет ответ (route reply) по наикратчайшему маршруту.

Передача данных – данные передаются по установленному маршруту, а при изменении топологии происходит обновление маршрутов.

Ключевой особенностью ZigBee является минимизация числа hops (прыжков) при выборе маршрута, что делает сеть уязвимой к атакам на маршрутизацию, таким как Wormhole.

В ходе эксперимента для настройки и мониторинга параметров ZigBee-сети использовалась программа XCTU, предоставляемая компанией Digi. Данный инструмент позволил конфигурировать модули Digi XBee, задавать сетевые параметры, изменять роли узлов (координатор, роутер, оконечное устройство). С помощью XCTU была проведена диагностика соединений между узлами, анализ задержек передачи данных и выявление изменений в маршрутизации, что сыграло ключевую роль в моделировании атаки Wormhole и оценке ее воздействия на работу сети.

Рис. 4. Вид работы программы XCTU
Fig. 4. View of the XCTU program operation

Беспроводные сенсорные сети подвержены множеству атак, направленных на нарушение их функционирования. Среди них можно выделить атаки на физический, канальный и сетевой уровни модели. На сетевом уровне, к которому относится маршрутизация, наиболее опасными являются Blackhole, Sinkhole, Replay Attack, Hello Flood, Wormhole [7].

Таблица 1. Наиболее опасные атаки на сетевом уровне
Table 1. The most dangerous attacks at the network level

Название атаки	Описание атаки	Последствия
Blackhole	Злоумышленник узел перехватывает пакеты и не передает их дальше, что нарушает связь в сети.	Потеря данных, отказ в обслуживании (DoS), разрыв связи. [8]
Sinkhole	Компрометированный узел перенаправляет трафик на себя, создавая ложный центр сети.	Снижение производительности сети, увеличение задержек, централизованный контроль злоумышленника. [9]
Replay Attack	Злоумышленник записывает пакеты данных и повторно отправляет их в сеть, вызывая дублирование информации.	Дублирование пакетов, искажение информации, перегрузка сети. [10]
Hello Flood	Атакующий рассылает ложные сообщения о близости ко всем узлам, перегружая сеть.	Перегрузка сети, сбои в маршрутизации, увеличение задержек [11]
Wormhole	Создание нелегитимного быстрого канала между двумя узлами, что изменяет маршрутизацию и позволяет перехватывать трафик.	Перехват, модификация и блокировка трафика, нарушение маршрутизации [12]

Атака Wormhole считается одной из наиболее сложных для обнаружения, поскольку не требует компрометации криптографических ключей или внесения изменений в программное обеспечение узлов [12]. Она заключается в следующем:

Создание скрытого канала – два атакующих узла устанавливают быстрый канал связи, например, через GSM/GPRS или Wi-Fi. Перехват пакетов – один из узлов атакующей пары перехватывает пакеты, передаваемые по ZigBee. Пересылка пакетов – пакеты мгновенно пересылаются через нелегитимный канал и передаются в сеть вторым атакующим узлом. Формирование ложных маршрутов – из-за сокращенного количества hops другие узлы считают маршрут через атакующие узлы наиболее оптимальным и начинают передавать данные через них.

Разработан сценарий атаки, в котором два атакующих узла создают скрытый канал передачи данных, искажающий топологию сети. Атака позволила злоумышленнику перенаправлять значительную часть сетевого трафика через компрометированные узлы. Были зафиксированы случаи изменения маршрутизации: узлы, выбирая оптимальный путь передачи данных, использовали нелегитимный канал, созданный атакующими узлами. В результате атаки были продемонстрированы возможности перехвата, модификации и блокировки сетевого трафика, что подтвердило уязвимость ZigBee-сетей перед данным видом угроз.

Зафиксировано сокращение числа переходов (hops) при передаче пакетов, что свидетельствовало о ложном сокращении маршрута. Наблюдались искажения данных, вызванные перехватом и изменением передаваемых пакетов. В некоторых случаях атака приводила к полной потере связи между узлами, что демонстрирует возможность организации отказа в обслуживании (DoS-атаки). Были исследованы методы выявления атаки, в том числе анализ задержек передачи пакетов и анализ топологии сети с учетом подозрительных изменений в маршрутизации.

Заключение

В ходе исследования была разработана экспериментальная платформа для моделирования атак на беспроводные сенсорные сети (БСС) на основе технологии ZigBee. Созданная сеть из семи узлов включала координатор, роутеры и атакующие узлы, работающие на микроконтроллерах Arduino Uno и одноплатных компьютерах Raspberry Pi. Для связи между узлами использовались модули Digi XBee, а атакующие узлы были дополнительно оснащены GSM/GPRS модулями (SIM800/SIM900), что позволило создать нелегитимный высокоскоростной канал связи. Данный стенд позволил имитировать атаку Wormhole и изучить ее влияние на работу сети.

Эксперименты показали, что атака Wormhole существенно изменяет маршрутизацию трафика в сети. В результате узлы начинали выбирать нелегитимный маршрут через атакующие узлы, сокращая количество hops и перенося основную нагрузку на узлы злоумышленника. Это позволяло атакующему не только перехватывать и анализировать передаваемые данные, но также блокировать или модифицировать трафик, изменяя показания датчиков. В отдельных случаях атака приводила к потере связи между узлами и отказу в передаче данных, что может иметь критические последствия для систем мониторинга.

Полученные результаты подтверждают высокую уязвимость БСС к атакам на маршрутизацию. Протокол ZigBee, ориентированный на минимизацию количества переходов при передаче данных, не учитывает возможность существования нелегитимных каналов связи. Это делает атаку Wormhole особенно сложной для обнаружения. В рамках исследования были рассмотрены потенциальные методы защиты, включая мониторинг задержек передачи пакетов, анализ сетевой топологии и применение алгоритмов машинного обучения для обнаружения аномалий в маршрутизации.

Перспективы дальнейших исследований включают разработку и тестирование алгоритмов обнаружения атак, а также изучение других видов атак на маршрутизацию, таких как Sinkhole, Blackhole и Hello Flood. Внедрение механизмов защиты на уровне протоколов маршрутизации, включая многофакторную проверку маршрутов и использование доверенных узлов, может значительно повысить устойчивость БСС к атакам. Таким образом, проведенное исследование вносит вклад в развитие методов обеспечения безопасности киберфизических систем и беспроводных сенсорных сетей.

Список использованных источников / References

1. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.-W. Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. Sensors 2022, 22, 2087.

2. Krishnakumar, Parvathy. (2021). Wormhole Attacks in Wireless Sensor Net-works (Wsn) & Internet of Things (IoT): A Review. International Journal of Re-cent Technology and Engineering. 10. 199-203.

3. Jegan, G. & Punniakodi, Samundiswary. (2016). Wormhole Attack Detection in Zigbee Wireless Sensor Networks using Intrusion Detection System. Indian Journal of Science and Technology.

4. Dutta, Nishigandha & Singh, Moirangthem. (2019). Wormhole Attack in Wireless Sensor Networks: A Critical Review.

5. T. Zhukabayeva, A. Pervez, Y. Mardenov, M. Othman, N. Karabayev and Z. Ahmad, "A Traffic Analysis and Node Categorization- Aware Machine Learning-Integrated Framework for Cybersecurity Intrusion Detection and Prevention of WSNs in Smart Grids," in IEEE Access, vol. 12, pp. 91715-91733, 2024, doi: 10.1109/ACCESS.2024.3422077.

6. Fafoutis, Xenofon & Tsimbalo, Evgeny & Zhao, Wenrui & Chen, Haowen & Mellios, Evangelos & Harwin, William & Piechocki, R.J. & Craddock, I.J.. (2016). BLE or IEEE 802.15.4: Which Home IoT Communication Solution is more Energy-Efficient?. EAI Endorsed Transactions on Internet of Things.

7. A. Adamova, T. Zhukabayeva and Y. Mardenov, "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), Astana, Kazakhstan, 2023, pp. 506-511.

8. Hasan, A.; Khan, M.A.; Shabir, B.; Munir, A.; Malik, A.W.; Anwar, Z.; Ahmad, J. Forensic Analysis of Blackhole Attack in Wireless Sensor Networks/Internet of Things. Appl. Sci. 2022, 12, 11442.

9. Ali, Mubashir & Nadeem, Muhammad & Siddique, Ayesha & Ahmad, Shahbaz & Ijaz, Amir. (2020). Addressing Sinkhole Attacks In Wireless Sensor Networks -A Review. International Journal of Scientific & Technology Research. 9. 406-411.

10. Pichamuthu, Rajaram. (2024). An Enhanced Deep Learning Approach for Preventing Replay Attacks in Wireless Sensor Network. 63. 8010-8023.

11. Singh, Virendra & Sweta, Jain & Jyoti, Singhai. (2010). Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. International Journal of Computer Science Issues. 7.

12. Zhukabayeva T.K., Mardenov E.M. (2021). Detecting wormhole attacks in wireless sensor networks. Issue No. 4(107): Herald of Science of S. Seifullin Kazakh Agro Technical University.

Сведения об авторах

Марденов Е.М., научный сотрудник, Международный научный комплекс «Астана», yerik.mardenov@aiu.edu.kz.
Абдилдаева А.А., PhD, старший научный сотрудник, Международный научный комплекс «Астана».
Ху Вен-Цен Б., д-р техн. наук, проф., ведущий научный сотрудник, Международный научный комплекс «Астана».

Information about the authors

Mardenov E.M., Researcher, International Scientific Complex "Astana", yerik.mardenov@aiu.edu.kz.
Abdildaeva A.A., PhD, Senior Researcher, International Scientific Complex "Astana".
Hu Wen-Tsen B., D.Sc. (Eng.), prof., leading research fellow, International Scientific Complex "Astana".