ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Декабрь 2019 Том 7 № 1 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
December 2019 Vol. 7 Iss. 1 ISSN 2307-1303 http://www.itt.sut.ru

АНАЛИЗ ЗАЩИЩЕННОСТИ ПРОГРАММНО-АППАРАТНЫХ КОМПОНЕНТОВ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

В. А. Десницкий[1,2*], А. В. Мелешко[1]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Санкт-Петербург, 199178, Российская Федерация
[2]Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

[*]Адрес для переписки: desnitsky@comsec.spb.ru

Аннотация
Статья представляет обзор подходов к анализу защищенности программно-аппаратных компонентов в беспроводных сенсорных сетях. **Предмет исследования.** Предметом исследования являются существующие подходы к анализу защищенности. **Метод.** В работе применяются методы системного анализа. **Основные результаты.** Проведен детальный анализ существующих угроз и атак на беспроводные сенсорные сети, а так же анализ уязвимостей и протоколов передачи данных между узлами подобных систем. Выявлены основные направления работ по обеспечению безопасности беспроводных сенсорных сетей. **Практическая значимость.** Полученные в данной работе результаты могут применяться для совершенствования средств защиты беспроводных сенсорных сетей от различных киберфизических атак.

Ключевые слова
Анализ защищенности, беспроводные сенсорные сети, программно-аппаратные компоненты сетей.

Информация о статье
УДК 004.733
Язык статьи – русский.
Поступила в редакцию 23.07.19, принята к печати 02.09.19.

Ссылка для цитирования: Десницкий В. А., Мелешко А. В. Анализ защищенности программно-аппаратных компонентов в беспроводных сенсорных сетях // Информационные технологии и телекоммуникации. 2019. Том 7. № 1. С. 75–83. DOI 10.31854/2307-1303-2019-7-1-75-83

SECURITY ANALYSIS OF SOFTWARE AND HARDWARE COMPONENTS IN WIRELESS SENSOR NETWORKS

V. Desnitsky[1,2*], A. Meleshko[1]

[1]St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, 199178, Russian Federation
[2]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, St. Petersburg, 193232, Russian Federation

[*]Corresponding author: desnitsky@comsec.spb.ru

Abstract—The paper comprises a review of approaches to security analysis of software and hardware components in wireless sensor networks. **Research subject.** The subject of the research is existing approaches to security analysis. **Method.** The methods of system analysis are applied in the work. **Core results.** A detailed analysis of existing threats and attacks on wireless sensor networks as well as an analysis of vulnerabilities and data transfer protocols between nodes of such systems has been performed. The main directions to ensure security of the wireless sensor networks are identified. **Practical significance.** The results obtained in this paper can be used to improve the means of protecting the wireless sensor networks from various cyber-physical attacks.

Keywords—Security analysis, wireless sensor networks, hardware and software components of networks.

Article info
Article in Russian.
Received 23.07.19, accepted 02.09.19.

For citation: Meleshko A., Desnitsky V.: Security analysis of software and hardware components in wireless sensor networks // Telecom IT. 2019. Vol. 7. Iss. 1. pp. 75–83 (in Russian). DOI 10.31854/2307-1303-2019-7-1-75-83

Введение

В общем случае беспроводная сенсорная сеть (БСС) представляет собой распределённую, самоорганизующуюся сеть, состоящую из множества датчиков и исполнительных элементов, объединённых между собой посредством радиоканалов связи. Область покрытия подобной сети может составлять от нескольких метров до нескольких километров за счёт способности ретрансляции сообщений от одного узла к другому [1].

Типовая БСС состоит из следующих элементов: узел-датчик; шлюз (точка доступа), обеспечивающий связь между узлами; сетевой менеджер, отвечающий за конфигурацию сети, планирование обмена данными между устройствами, управление таблицами маршрутизации и мониторинга и отчетности здоро-

вья сети; менеджер безопасности, ответственный за функции безопасности, генерацию, хранение и управление ключами [2].

Проблема подверженности БСС атакующим воздействиям приобретает все более существенное значение, как из-за возрастающего проникновения БСС в различные сферы жизни, так и в результате повышения структурно-функциональной сложности таких сетей и предоставляемых ими сервисов, что в свою очередь повышает риски нелегитимного использования БСС нарушителем информационной безопасности.

Статья организована следующим образом: раздел 1 содержит обзор существующих подходов к анализу защищенности БСС; в разделе 2 приведены основные выводы, которые можно сделать по результатам обзора.

1. Подходы к анализу защищенности

В [3] приведен обзор основных характеристик и требований к безопасности БСС, алгоритмов шифрования, которые возможно применять для обеспечения конфиденциальности данных в БСС, а также протоколы безопасной передачи данных в БСС. К ключевым характеристикам авторы отнесли масштабируемость, ограниченность ресурсов (энергопитания), избыточность передаваемых данных и специфические требования безопасности, возникающие в основном из-за ресурсных ограничений. В тоже время требования к безопасности содержат не только основные требования к конфиденциальности, доступности и целостности, но еще и требования «свежести» и аутентичности данных. Под требованием аутентичности понимается то, что узлы сети должны отделять «свои» пакеты данных от «чужих», а требование «свежести» вводится для того, чтобы злоумышленник не мог ретранслировать копию старых данных.

В [3] раскрываются также возможные уровни, на которых злоумышленник может провести атаки, в том числе атаки на физическом уровне, сетевом, транспортном и пр. Кроме того в статье проанализированы следующие применяемые в БСС алгоритмы шифрования: DES, 3DES, DES-X, Blowfish, Twofish, TEA, XTEA, XXTEA, AES, Skipjack, HIGHT, а также следующие протоколы безопасности: TinySec, IEEE 802.15.4, SPINS, MiniSEC, LSec, LLSP, LISA, LISP.

Статья [2] посвящена анализу безопасности в БСС, в ней рассматривается архитектура БСС, а также приведена классификация атак на подобные сети по уровням модели OSI. Помимо этого в [2] описаны возможные контрмеры, позволяющие противодействовать атакам. В частности, описаны такие атаки как отказ в обслуживании (физический, канальный, сетевой уровни), Sybil-атаки (физический, канальный, сетевой уровни), Wormhole-атаки (сетевой уровень), outsider-атаки и некоторые другие виды. Приведенные механизмы противодействия классифицированы по уровням, физический, канальный и сетевой, причем для каждого уровня перечислены угрозы и конкретные меры противодействия.

В [4] описывается подход к оценке безопасности БСС применительно к системам Умного дома. Методика основана на генерации графов атак и направлена на обнаружение и противодействие и помогает предугадать существующие уязвимости в интеллектуальных домашних сетях. С использованием языка логического программирования Пролог на основании данных о топологии сети, конфигурации домашних устройств и заданных правилах возникает возможность

имитировать действия, применяемые злоумышленником для достижения своих целей по компрометации домашней сети. Входом в разработки данного метода являются – отчеты уязвимости, конфигурация устройств и топология сети. Отчеты об уязвимости описывают информацию об уязвимостях в конкретном экземпляре домашней сети.

Статья [5] описывает обзор принципов кибербезопасности систем мониторинга интеллектуальных сетей на основе БСС, а также основные принципы безопасности широковещательной аутентификации. Также авторами предлагается безопасный и устойчивый к DoS-атакам протокол широковещательной аутентификации. Преимуществом протокола является то, что устройства не тратят свое буферного пространства при обработке несанкционированных пакетов, что не приводит к повышению электропитания, в том числе в условиях наличия атак истощения энергоресурсов. Протокол был протестирован на реальных устройствах с разной производительностью и было показано, что время работы протокола приемлемо для подобного рода систем.

В статье [6] рассмотрены БСС, различные типы атак, в том числе активные и пассивные, и их последствия, а так же произведена выработка контрмер. К пассивным относятся атаки, направленные на нарушение конфиденциальности (мониторинг, прослушивание, анализ трафика), тогда как к активным относят атаки типа Sinkhole, Sybil-атаки и др. В данной работе приводятся также некоторые механизмы противодействия данному виду атак.

Статья [7] посвящена рассмотрению таких атак на БСС как атаки отказа в обслуживании, Sybil-атаки, Wormhole-атаки, HelloFlood-атаки и атаки, нацеленные на перехват и анализ трафика. Указаны механизмы противодействия атакам типа HelloFlood и Outsider атак, при этом от Outsider-атак авторы предлагают защищаться путем шифрования канального уровня, тогда как для защиты от HelloFlood-атаки узлы должны подтвердить двунаправленность ссылки, прежде чем предпринимать действия, основанные на сообщении, полученном по этой ссылке.

В [8] описываются различные механизмы обнаружения вторжений применительно к БСС. В частности, описан механизм обнаружения на основе сигнатур, а именно на основе, так называемого, децентрализованного правила. Такие системы хорошо подходят для известных вторжений, однако они не могут обнаружить новые атаки и атаки, не имеющие заранее определенных сценариев.

В [9] описаны некоторые атаки на БСС, а также известные протоколы маршрутизации в БСС, такие как DirectedDiffusion, TinyOSbeaconing, Geographicrouting, Rumorrouting. Вместе с тем описан протокол, который направлен на борьбу с атакой типа wormhole.

В [10] подробно рассматриваются классификации БСС, их типы, топологии и модели атак. Также авторами затрагиваются вопросы управления ключами, в том числе распределение ключей шифрования между узлами. Авторы выделяют следующие цели, которые необходимо достичь для построения протокола управления ключами БСС. Анализируются вопросы оценки протоколов управления ключами по следующим особенностям: добавление – насколько сложным является добавление динамического узла; отзыв – насколько сложным является отзыв динамического узла; размер сети – максимально возможный размер сети;

эластичность – сколько узлов будет поставлено под угрозу для того, чтобы повлиять на трафик не скомпрометированных узлов.

В [11] раскрываются типовые сферы применения БСС, в том числе в военной сфере, медицинской, экологической, в промышленности, сельском хозяйстве. Проанализированы основные атаки на БСС и требования к безопасности с учетом конкретных ее применений.

В [12] представлен обзор DoS-атак на беспроводные сети датчиков, а также представлены экспериментальные результаты моделирования интерференционных атак – то есть атак, основанных на генерации помех, которые проанализированы на физическом, канальном, сетевом, транспортном и прикладном уровнях.

При этом в рамках практической части работы, описывается один из способов продуцирования DoS-атак. Моделируется сценарий атаки этого типа путем добавления узла злоумышленника к БСС. Атакующий анализирует большое количество трафика и данных с целью отключения других узлов в сети. БСС, на основе которой проводится моделирование, состоит из 5 легитимных узлов, один из которых представляет приемник. В отсутствии атакующего, приемник получает данные от 4 легитимных узлов. В случае возникновения атакующего приемник перестает получать все пакеты, отправленные с легитимных узлов (атакующий генерирует помехи, мешающие передаче). Авторы произвели оценку того, сколько пакетов приемник будет получать в случае, если атакующий перемещается на различное расстояние от приемника. Отметим, что легитимные узлы в сети являются статическими, и они расположены на определенном расстоянии друг от друга для того, чтобы избежать помех. Атакующий узел является мобильным узлом, который означает, что он может находиться в движении. Полученные экспериментальные результаты подтвердили применимость данного вида атак и показали, что количество пакетов существенно снижается, когда атакующий узел физически приближается к приемнику.

В [13] ставится вопрос энергоэффективности БСС в контексте задач информационной безопасности. В частности, описываются архитектуры и протоколы функционирования БСС на базе сетей IEEE 802.15.4, обеспечивающие повышенную энергоэффективность, в том числе протоколы SPINS, TinySec, LLSP, LEAP/LEAP+, NOVSF-based, LSec, HASF. В качестве наиболее энергоэффективных обозначены следующие протоколы: SERP (Secure Energy Efficient Routing Protocol), EENC (Energy Efficiency Routing with Node Compromised Resistance) и REceiveWAtchReDirect (REWARD) routing protocol. Для каждого из приведенных протоколов представлены сервисы безопасности и показаны их свойства.

В [14] рассматриваются вопросы маршрутизации протоколов, масштабируемости, связи и безопасности. Рассматривается интеграция виртуализации, облачных вычислений, и Software Defined Networking (SDN) в БСС. Авторы подчеркивают, что для разработки защищенной среды, необходимо рассмотреть возможности аппаратных ресурсов БСС (память, процессор и питание). Шифрование обеспечивает конфиденциальность, но потребляет больше энергии. Экспериментальные результаты показывают, что алгоритм шифрования с использованием 64-битных ключей для обеспечения конфиденциальности данных может быть вскрыт за 3,5 месяца с использованием супер-вычислительной техники, которая может обрабатывать 10^{12} паролей в секунду. Для 128 битных ключей

это значение $5.4*10^{18}$ в год. В результате встает вопрос, нужен ли такой большой ключ с ограниченными ресурсами сенсорных узлов.

2. Дискуссия

По результатам рассмотрения современных работ в области безопасности БСС можно выделить несколько следующих наиболее актуальных направлений:

- исследование конкретных видов атак и контрмер с учетом разновидностей архитектур и топологий БСС, в том числе практическое моделирование атак на БСС;
- оценка эффективности систем безопасности БСС в конкретных областях приложения (таких как систему Умного дома, робототехнические комплексы, имплантируемые медицинские устройства и др.);
- исследование защищенных широковещательных протоколов связи в БСС;
- тестирование на проникновение и обнаружение вторжений в БСС;
- организация защиты активов БСС с учетом ограничений на их энергоресурсы и наличия атак по истощению заряда узлов сети.

По сути рассмотренные в настоящей статье работы представляют собой обзоры возможных атак на БСС, протоколов передачи данных между узлами, мер противодействия. Обзоры составлены с разной степенью детализации. При этом они могут быть использованы не только для анализа уровня защищенности функционирующих сетей, но также и для уточнения требований и параметров безопасности еще на этапе проектирования БСС [15].

Вместе с тем, присутствуют также работы, имеющие более специфичный приклад и практическую значимость: в [4] описывается подход к оценке защищенности БСС Умного дома, где на основании данных о топологии сети, конфигурации домашних устройств, правилах автономных атак имеется возможность имитировать действия, которые злоумышленник способен достичь в домашней сети [16].

Анализ рассмотренных работ показал актуальность, как сигнатурных, так и основанных на анализе поведенческих особенностей подходов к выявлению атак в БСС, а также необходимость комбинированных моделей к детектированию злонамеренных воздействий.

Помимо анализа разновидностей атакующих воздействий на БСС, таких как HelloFlood и Outsider-атаки, затрагиваются вопросы применимости репутационных и доверительных механизмов. Причем в [17] авторы полагают, что доверительные механизмы помогут решить некоторые проблемы за пределами традиционной криптографической защиты. Например, оценку качества узлов БСС и качество предоставляемых сетью сервисов, а также предоставление соответствующего контроля доступа и своевременности поступления данных [18].

Анализ интерференционных атак выявил не только их нацеленность на нарушения свойств доступности узлов БСС, но также направленность на прямую потерю работоспособности узла, в том числе путем эксплуатации атак истощения энергоресурсов.

Заключение

В статье представлен обзор работ, затрагивающих вопросы моделирования, анализа, оценки эффективности процессов защиты в беспроводных сенсорных сетях. В качестве дальнейших направлений исследований предполагается решение задач верификации моделей нарушителя для оценки защищенности сетей. Работа выполнена при частичной финансовой поддержке гранта Российского Фонда Фундаментальных Исследований (РФФИ) № 19-07-00953 и гранта Президента Российской Федерации № МК-5848.2018.9.

Литература

1. Dargie W. and Poellabauer C. Fundamentals of wireless sensor networks: theory and practice // John Wiley and Sons. 2010. 311 p.

2. Kumar H. K. and Kar A. Wireless sensor network security analysis // International journal of computer science & information Technology (IJCSIT). 2009. Т. 1. № 1. pp. 1–10.

3. Dener M. Security Analysis in Wireless Sensor Networks // International Journal of Distributed Sensor Networks. 2014. Т. 10. № 10. pp. 1–9.

4. Zhang M. et al. A New Approach to Security Analysis of Wireless Sensor Networks for Smart Home Systems // International Conference on Intelligent Networking and Collaborative Systems (INCoS). 2016. pp. 318–323.

5. He D., Chan S., Guizani M. Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring // IEEE Wireless Communications. 2017. Т. 24. № 6. pp. 98–103.

6. Prusty A. R. The Network and Security Analysis for Wireless Sensor Network : A Survey // (IJCSIT) International Journal of Computer Science and Information Technologies. 2012. Т. 3. pp. 4028–4037.

7. Ruhul Amin H. M. Wireless sensor network security analysis [Электронный ресурс]. URL: https://www.academia.edu/28228231/ wireless_sensor_network_ security _analysis

8. Kalnoor G., Agarkhed J. Intrusion threats and security solutions in wireless sensor networks // International Robotics & Automation Journal. 2018. Т. 1. pp. 54–58.

9. Sadeghi M. et al. Security Analysis of Routing Protocols in Wireless Sensor Networks // IJCSI International Journal of Computer Science Issues. 2012. Т. 9. № 3. pp. 465–472.

10. El-mawla N. A, Badawy M., Arafat H. Security and key management challenges over WSN (a survey) // International Journal of Computer Science & Engineering Survey (IJCSES). 2019. Т. 10. № 1. pp. 15–34.

11. Pratap V., Kirar S. A Survey of Attacks and Security Requirements in Wireless Sensor Networks // Engineering and Technology International Journal of Electronics and Communication Engineering. 2014. Т. 8. No. 12. pp. 2198–2203.

12. Gavric Z., Simic D. Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks // Ingeniería e Investigacion. 2018. Т. 38. № 1. pp. 130–138.

13. Daniluk K., Niewiadomska-Szynkiewicz E. A Survey of Energy Efficient Security Architectures and Protocols for Wireless Sensor Networks // journal of telecommunications and information technology. 2012. Т. 3. pp. 64–72.

14. Bangash Y. A. et al. Security Issues and Challenges in Wireless SensorNetworks: A Survey // IAENG International Journal of Computer Science. 2017. Т. 44. № 2. С. 94–108.

15. Десницкий В. А., Котенко И. В. Проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной безопасности. Компьютерные системы. 2013. № 1. С. 44–54.

16. Чечулин А. А., Десницкий В. А., Котенко И. В. Анализ информационных потоков для построения защищенных систем со встроенными устройствами // Системы высокой доступности. 2012. Т. 8. № 2. С. 116–122.

17. Rathod V., Mehta M. Security in Wireless Sensor Network: A survey // Ganpat University Journal of Engineering & Technology. 2011. Т. 1. № 1. pp. 35–44.

18. Киреев А. О., Светлов А. В. Беспроводные сенсорные сети в сфере технологий охраны объектов // Труды международного симпозиума: Надежность и качество. Инф.-изд. центр ПензГу. 2008. Т. 2. С. 179–181.

References

1. Dargie, W. and Poellabauer, C. Fundamentals of wireless sensor networks: theory and practice // John Wiley and Sons. 2010. 311 p.

2. Kumar, H. K. and Kar, A. Wireless sensor network security analysis // International journal of computer science & information Technology (IJCSIT). 2009. Vol. 1. No. 1. pp. 1–10.

3. Dener, M. Security Analysis in Wireless Sensor Networks // International Journal of Distributed Sensor Networks. 2014. Vol. 10. No. 10. pp. 1–9.

4. Zhang, M. et al. A New Approach to Security Analysis of Wireless Sensor Networks for Smart Home Systems // International Conference on Intelligent Networking and Collaborative Systems (INCoS). 2016. pp. 318–323.

5. He, D., Chan, S., Guizani, M. Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring // IEEE Wireless Communications. 2017. Vol. 24. No. 6. pp. 98–103.

6. Prusty, A. R. The Network and Security Analysis for Wireless Sensor Network : A Survey // (IJCSIT) International Journal of Computer Science and Information Technologies. 2012. Vol. 3. pp. 4028–4037.

7. Ruhul Amin, H. M. Wireless sensor network security analysis [Electronic resource]. URL: https://www.academia.edu/28228231/wireless_sensor_ network_ security_analysis.

8. Kalnoor, G., Agarkhed, J. Intrusion threats and security solutions in wireless sensor networks // International Robotics & Automation Journal. 2018. Vol. 1. pp. 54–58.

9. Sadeghi, M. et al. Security Analysis of Routing Protocols in Wireless Sensor Networks // IJCSI International Journal of Computer Science Issues. 2012. Vol. 9. No. 3. pp. 465–472.

10. El-mawla, N. A, Badawy, M., Arafat, H. Security and key management challenges over WSN (a survey) // International Journal of Computer Science & Engineering Survey (IJCSES). 2019. Vol. 10. No. 1. pp. 15–34.

11. Pratap, V., Kirar, S. A Survey of Attacks and Security Requirements in Wireless Sensor Networks // Engineering and Technology International Journal of Electronics and Communication Engineering. 2014. Vol. 8. No. 12. pp. 2198–2203.

12. Gavric, Z., Simic, D. Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks // Ingeniería e Investigacion. 2018. Vol. 38. No. 1. pp. 130–138.

13. Daniluk, K., Niewiadomska-Szynkiewicz, E. A Survey of Energy Efficient Security Architectures and Protocols for Wireless Sensor Networks // journal of telecommunications and information technology. 2012. Vol. 3. pp. 64–72.

14. Bangash, Y. A. et al. Security Issues and Challenges in Wireless SensorNetworks: A Survey // IAENG International Journal of Computer Science. 2017. Vol. 44. No. 2. pp. 94–108.

15. Desnitsky, V. A., Kotenko, I. V. Designing secure embedded devices based on configuration // Information Security Issues. Computer systems. 2013. No. 1. pp. 44–54.

16. Chechulin, A. A., Desnitsky, V. A., Kotenko, I. V. Analysis of information flows for building secure systems with embedded devices // High availability systems. 2012. T. 8. No. 2. pp. 116–122.

17. Rathod, V., Mehta, M. Security in Wireless Sensor Network: A survey // Ganpat University Journal of Engineering & Technology. 2011. Vol. 1. No. 1. pp. 35–44.

18. Kireev, A. O., Svetlov, A. V. Wireless sensor networks in the field of object security technologies // Proceedings of the international symposium: Reliability and quality. Inf.-ed. PenzGu Center. 2008. T. 2. pp. 179–181.

Десницкий Василий Алексеевич – кандидат технических наук, старший научный сотрудник, СПИИРАН, Санкт-Петербург, 199178; доцент, СПбГУТ, 193232, Российская Федерация, desnitsky@comsec.spb.ru

Мелешко Алексей Викторович – младший научный сотрудник, СПИИРАН, Санкт-Петербург, 199178, Российская Федерация, lexa.0710@gmail.com

Desnitsky Vasily – Candidate of Engineering Sciences, Senior Research Officer, SPIIRAS, St. Petersburg, 199178; Associate Professor, SUT, St. Petersburg, 193232, Russian Federation, desnitsky@comsec.spb.ru

Meleshko Alexey – Research Assistant, SPIIRAS, St. Petersburg, 199178 Russian Federation, lexa.0710@gmail.com