А. В. Мелешко, В. А. Десницкий
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, г. Санкт-Петербург
УДК 004.056.5

ДЕТЕКТИРОВАНИЕ АТАК В САМООРГАНИЗУЮЩИХСЯ ДЕЦЕНТРАЛИЗОВАННЫХ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Аннотация. *В работе представлен процесс разработки модуля детектирования атак в самоорганизующихся децентрализованных беспроводных сенсорных сетях (БСС). Для реализации модуля детектирования проводятся разработка натурной модели БСС и протокола ее функционирования, создание модели нарушителя, моделирование атакующих воздействий на разработанной натурной модели. Предварительные эксперименты показали достаточно высокую точность детектирования, более 90%.*

Ключевые слова: *беспроводная сенсорная сеть, модель атакующего, моделирование беспроводной сенсорной сети, детектирование атак, моделирование атак, машинное обучение.*

Введение. Сегодня применение беспроводных сенсорных сетей (БСС) получает все больший охват. Они применяются в различных областях деятельности человека, например, БСС могут работать в области мониторинга климатических характеристик окружающего пространства, системах управления водоснабжением и других областях. Самоорганизующаяся БСС это сеть, узлами которой являются сенсорные устройства, соединенные беспроводным каналом связи, с нефиксированной заранее структурой, меняющимся составом узлов и соединений между ними. Ресурсные ограничения таких сетей, различные режимы функционирования, а также вариативность действий злоумышленников влияют на вопросы их безопасности.

Проблема исследования. Ввиду низкой защищенности децентрализованных самоорганизующихся БСС существует необходимость проведения исследований в области их безопасности и разработки моделей и алгоритмов для обнаружения атакующих воздействий, учитывающих специфику таких сетей — свойства самоорганизации и децентрализации, ограниченные ресурсы.

Настоящая работа направлена на изучение и разработку механизмов детектирования атак в самоорганизующихся беспроводных сенсорных сетях и защиты от них. Вклад работы заключается: а) в разработке модели атакующего, которая учитывает свойства самоорганизации и децентрализации БСС, а также динамического назначения/перераспределения узлов сети; б) разработке натурных и полунатурных моделей атак (с помощью прототипа БСС) на рассматриваемую БСС, позволяющих получить размеченные исходные данные для обнаружения атак; в) разработке алгоритмов детектирования атак на самоорганизующуюся децентрализованную БСС, которые позволят проводить детектирования с приемлемой точностью в условиях ограничения на ресурсопотребление узлов сети.

Материалы и методы. Был проведен анализ работ в области безопасности самоорганизующихся децентрализованных БСС. В работе [1] авторы рассматривают модель нарушителя для БСС, которая структурирует и упорядочивает типичные предположения о нарушителях в БСС. В [2] представлена модель доверия для БСС. А именно рассматриваются вопросы доверия базовой станции к данным, которые ей передают другие узлы сети. Авторы исследовали атаку злонамеренного узла, который передает ложные данные. Для моделирования атаки, а также для построения модели авторы использовали программный «симулятор» TRMsim-WSN. Также был проведен анализ энергопотребления узлов сети. В статье [3] представлена децентрализованная система обнаружения вторжений (IDS). Данная система отличается тем, что функции детектирования распределены на несколько узлов БСС. Авторы статьи [4] реализовали БСС для мониторинга качества воды и механизмы детектирования аномалий в данной сети. Они используют различные сенсоры загрязнения воды. Отличительной особенностью является высокое качество детектирования в условиях возможных неточностей и отсутствия значений части признаков (то есть в условиях неполноты данных) [4]. Анализ показал, что рассмотренные работы можно разделить на три направления — децентрализованные механизмы управления и защиты БСС, модели атак и атакующих и механизмы обнаружения атак. Однако, вопросы безопасности именно децентрализованных самоорганизующихся БСС в существующей литературе

затронуты в недостаточной степени, поэтому исследование можно считать целесообразным.

В целом задачу настоящей работы можно представить следующим образом: необходимо разработать алгоритмы детектирования атак в децентрализованных БСС, чтобы максимально повысить показатель качества их обнаружения в условиях заданных ограничений, а именно ограничений на аппаратные ресурсы сети и условий сохранения ее работоспособности.

Проведено натурное моделирование БСС, а именно создание программно-аппаратного прототипа сети и протокола ее функционирования. В основе разрабатываемого протокола функционирования децентрализованной БСС закладывается протокол сетевого уровня, реализующий функции самоорганизации сети, а именно протокол ZigBee. Сам протокол функционирования является протоколом прикладного уровня, включает систему из 5 ролей узлов: сборщик данных, коллектор, обработчик, детектор атак и контроллер сети. Сборщик данных ответственен за сбор, предобработку данных от сенсоров. Коллектор ответственен за хранение собранных и обработанных данных от других узлов сети. Обработчик проводит преобразование и агрегацию данных за определенный период времени. Детектор атак осуществляет интеллектуальную обработку данных в том числе анализ защищенности сети — разрабатываемый модуль детектирования атак расположен на узлах с данной ролью. Контроллер осуществляет принятие решений о реорганизации и распределении ролей в сети. Реализуемая протоколом децентрализация БСС сводится к динамическому распределению ролей, и взаимодействию узлов между собой в соответствии с определяемой ролью.

На данный момент прототип содержит четыре узла — два сборщика, один коллектор, а также контроллер сети. С аппаратной точки зрения каждый узел состоит из: одноплатного компьютера Raspberry Pi 3-й и 2-й версии, модуля связи Digi XBee и сенсоров. Узел-контроллер отличается от остальных и представляет собой ноутбук с подключенным модулем XBee. Программная часть всех узлов состоит из приложения на языке Python, которая реализует функционирование различных ролей узлов.

После реализации программно-аппаратного прототипа БСС была составлена модель атакующего для таких сетей. Модель может быть представлена в виде трех составляющих — множества целей атакующего, множества средств, которые атакующий способен использовать при реализации атаки и его действий. На основе анализа предметной области были выделены 4 разновидности атак, которые направлены на эксплуатацию свойств децентрализации и самоорганизации сети, и применительно к ним была составлена модель атакующего. На примере атаки внедрения ложного узла сети рассмотрим модель атакующего: атакующий преследует такие цели как подслушивание данных, их модификацию, а также возможное несанкционированное получение своим узлом какой-то роли, например, коллектора данных. При реализации он использует средства удаленного доступа к каждому узлу сети и информацию о конфигурации сети. Тогда для реализации атаки ему нужно провести взлом узла сети, получить идентификатор сети, настроить и подключить свой узел к ней и далее можно осуществлять преследуемые цели.

Рассмотренная ранее атака была промоделирована на программно-аппаратном прототипе. Моделирование проводилось с целью получения исходных данных для разработки модуля детектирования, а также для проверки выполнимости атак на прототипе.

Результаты. Была разработана первая версия модуля детектирования атак. Для разработки модуля были протестированы различные методы машинного обучения с учителем, а именно Ada BoostClassifier, Random Forest, Bayesian classifier, LogisticRegression, Linear SVM, Decision tree, RidgeClassifier. В процессе тестирования был проведен подбор наилучших параметров для каждого из методов, а также рассчитана корреляция признаков с целевой переменной.

Были проведены предварительные эксперименты на ограниченном наборе нерепрезентативных исходных данных. В качестве источника исходных данных был использован программно-аппаратный прототип системы управления водоснабжением со специфич-

ным ему набором атак [5]. Эксперименты показали высокие показатели качества детектирования — f-мера 0.99 и точность 99%, что подтверждает корректность разработанного модуля. В дальнейшем разработанный модуль детектирования атак будет протестирован и адаптирован на исходных данных, которые будут получены в результате моделирования атак на БСС.

Заключение. В работе представлен процесс разработки модуля детектирования атак в самоорганизующихся беспроводных сенсорных сетях. Отличительной особенностью модуля является учет специфики таких БСС, а именно механизмов самоорганизации и децентрализации, а также учет аппаратных. Кроме того, к особенностям настоящей работы можно отнести прототипирование рассматриваемой БСС, натурное моделирование атак на разработанном прототипе, а также разработку модели атакующего.

В качестве дельнейшей работы планируются продолжение моделирования различных атак на разработанном прототипе для получения достаточного количества исходных данных для проведения обучения моделей детектирования и проведения экспериментов, адаптация разработанного модуля детектирования атак на новых исходных данных, а также формальная верификация разработанных решений. Кроме того, планируется продумать ряд рекомендаций к повышению защищенности самоорганизующихся децентрализованных БСС.

СПИСОК ЛИТЕРАТУРЫ

1. Benenson Z. Attacker Models for Wireless Sensor Networks / Z. Benenson, E. O. Blab, F. C. Freiling. — Text : electronic // Information Technology. — 2010. — Vol. 52, № 6. — P. 320-324. — URL: https://doi.org/10.1524/itit. 2010.0609.
2. Kodali R. K. Trust model for WSN / R. K. Kodali, S. Soratkal. — Text : direct // 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). — 2015. — P. 903-906. — DOI: 10.1109/ICATCCT.2015.7457012.
3. Silva A. R. Decentralized intrusion detection in wireless sensor networks / A. R. Silva, H.T. Martins, P. S. Rocha [et al]. — Text : direct // Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet '05). — 2005. — P. 16-23.

4. Raciti M. Anomaly Detection in Water Management Systems / M. Raciti, J. Cucurull, S. Nadjm-Tehrani. — Text : direct // Critical Infrastructure Protection. Lecture Notes in Computer Science. — 2012. — Vol. 7130. — P. 98-119. — DOI: 10.1007/978-3-642-28920-0_6.
5. Meleshko A. V. Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems / A. V. Meleshko, V. A. Desnitsky, I. V. Kotenko. — Text : direct // IOP Conference Series: Materials Science and Engineering. International Conference on Modern Trends in Manufacturing Technologies and Equipment, 2019. — 2020. — P. 033034.

Д. Г. Бурилов, К. В. Подобрий, Т. И. Паюсова
Тюменский государственный университет, г. Тюмень

УДК 004.056

РАЗРАБОТКА МЕТОДИЧЕСКИХ МАТЕРИАЛОВ ПО ВИРУСНОМУ АНАЛИЗУ

Аннотация. *В ходе работы были рассмотрены основные техники и методы вирусного анализа, а также представлено описание разработанных методических материалов по вирусному анализу.*

Ключевые слова: *вирусный анализ, статический анализ, динамический анализ, компьютерный вирус, индикаторы компрометации, обфускация, вредоносное программное обеспечение.*

Введение. В настоящее время практически все сферы деятельности человека связаны с применением компьютеров, а информация является одним из самых дорогих ресурсов. Так как компьютерные системы и программное обеспечение постоянно развиваются, возрастает объем и повышается уязвимость хранящихся в них данных.

Сейчас можно утверждать, что компьютерные вирусы остаются одной из наиболее распространенных причин искажения и уничтожения важной информации, как следствие, возникают финансовые и временные потери. Согласно интерактивной карте угроз от Лаборатории Касперского, во всем мире ежедневно происходит до