Первый-третий этапы выполнения проекта № 19-07-00953 (2019-2021 г.)
"Модели, методики и алгоритмы анализа защищенности программно-аппаратных компонентов беспроводных сенсорных сетей"

Работа по Проекту направлена на решение вопросов информационной безопасности современных беспроводных сенсорных сетей, функционирующих в потенциально враждебном, не доверенном окружении. Цель Проекта – совершенствование подходов, моделей, методик и алгоритмов анализа защищенности программно-аппаратных компонентов беспроводных сенсорных сетей (БСС). Проект ориентирован на моделирование, анализ и прототипирование средств анализа защищенности беспроводных сенсорных сетей в условиях наличия разнородных и взаимодействующих между собой устройств, использующих беспроводные протоколы передачи данных с учетом повышенных требований к защищенности таких сетей.

Проведен анализ и сделан обзор научно-исследовательских работ в предметной области анализа защищенности программно-аппаратных компонентов в беспроводных сенсорных сетях, включающий более 100 источников научно-технической информации, в том числе научно-технических статей, опубликованных на русском и английском языках по тематике исследований в рецензируемых изданиях трудов конференций, научных журналах по тематике исследований.

Проведено научное обоснование задачи анализа защищенности программно-аппаратных компонентов в беспроводных сенсорных сетях, включающее обоснование актуальности проводимых исследований, формальную постановку задачи исследования и обоснование целесообразности решения задач Проекта.

Разработаны модели представления беспроводных сенсорных сетей, специфицирующие структуру, функциональные и поведенческие особенности сетей и устройств, входящих в их состав. В частности, модели построены на основе JSON-формата, удобного для формирования, модификации и использования данных, как человеком, так и при помощи автоматизированных программных средств обработки данных. Также построены, применяемые, в том числе при экспертном анализе беспроводных сенсорных сетей, модели на основе UML-диаграмм, позволяющих специфицировать, как статическую, так и изменяющуюся во времени структуру сети, сценарии работы сети, протоколы взаимодействия и различные операционные процедуры.

Разработана комбинированная модель нарушителя в беспроводных сенсорных сетях. Модель относится к классу аналитических моделей и включает объединенную классификацию и анализ возможных атакующих воздействий, которые нарушитель способен произвести и их особенности. Комбинированный характер модели нарушителя выражается в применении ряда существующих классификаций, используемых при исследовании беспроводных сенсорных сетей, встроенных устройств, систем Интернета вещей и адаптированных под условия БСС. Выделены основные, заложенные в модель нарушителя, отличительные признаки нарушителей безопасности беспроводных сенсорных сетей.

Разработана методика верификации моделей представления беспроводной сенсорной сети на предмет выполнимости условий осуществления атакующих воздействий нарушителем. Методика базируется на анализе спецификаций сети, модели нарушителя и правил соответствия функционала узлов сети, их ограничений, допущений о нарушителе и возможных видах угроз информационной безопасности. На основе JSON и UML моделей представления БСС, определяющих статическую и динамическую структуру сети, сценарии ее работы, протоколы взаимодействия и различные операционные процедуры, а также учитывая функциональные возможностей сети и ее нефункциональные ограничения, методика позволяет сформировать перечень возможных актуальных атак, которым подвержена целевая БСС.

Разработаны методика и алгоритмы распределенных сбора, обработки и анализа больших массивов данных от программных и аппаратных сенсоров беспроводной сенсорной сети в режиме

близком к режиму реального времени. Построенные методика и алгоритмы обеспечивают объединение множеств разнородных устройств БСС в единую логическую коммуникационную инфраструктуру с выполнением процессов самоорганизации, самонастройки и самоконфигурации такой сети для решения задач безопасного обмена прикладными данными между устройствами сети. Организация сбора, обработки и анализа данных производится с использованием вычислительного кластера на примере интегрируемых в беспроводную сеть одноплатных компьютеров Raspberry Pi. Разворачиваемые прикладные сервисы кластерных вычислений реализуют трехуровневую многопроцессную архитектуру вычислений микроконтроллеров, входящих в состав БСС, и осуществляют функции параллельной обработки данных с возможностью распределения и перераспределения функций предобработки, фильтрации, нормализации и группового анализа собираемых данных на доступных вычислительных мощностях узлов сети.

Разработаны методика и алгоритмы выявления аномальных данных от сенсоров беспроводных сенсорных сетей на основе применения методов машинного обучения и аппарата нейронных сетей. Построенные методика и алгоритмы позволяют выявлять закономерности в данных, формируемых сенсорами БСС и являющихся признаками наличия атакующих воздействий или же неправильного и нетипичного поведения пользователей сети. В частности, такое детектирование позволяет определять атакующие воздействия, связанные со злонамеренной модификацией показаний одного или нескольких сенсоров, а также атаки физической подмены сенсора и воздействия, направленные на его физическое окружение. Методика и алгоритмы выявления аномалий основаны на учете не только некорректных состояний сети, но также и некорректных переходов между ее предполагаемо корректными состояниями. Исходными данными алгоритмов являются наборы признаков атак, выражаемых посредством данных о текущих показаниях сенсоров сети, снабженных метками времени, а также метаданных, включающих местоположения узлов БСС и особенности режимов их работы. В качестве аппарата для выполнения детектирования используются, в частности, алгоритмы машинного обучения с учителем, в т.ч. методы KNN, SVM, DT, NB, и искусственные нейронные сети с использованием библиотек Scikit-learn и Keras.

Разработаны архитектура и программно-аппаратные прототипы средств анализа защищенности компонентов беспроводных сенсорных сетей. Предложенная архитектура описывает основные структурно-функциональные элементы и поведенческие особенности прототипов средств анализа защищенности и специфицируется с использованием диаграмм классов, активностей и последовательности универсального языка моделирования UML. Разработанные программно-аппаратные прототипы зарегистрированы в ФИПС в качестве программ для ЭВМ. На базе построенных прототипов получены экспериментальные оценки разработанных научно-технических решений с использованием целевых показателей средств анализа защищенности.

Проведен анализ применимости разработанных программно-аппаратных решений и сделана теоретическая оценка полученных результатов. Теоретическая оценка предложенных методик выражается в выяснении их корректности путем проверки обоснованности применения подходов и методов, лежащих в основе каждой из методик. В качестве технологий перспективных для дальнейшего развития данного направления представляются технология Больших Данных в ее приложении к БСС и технология облегченных обучающих моделей, в том числе библиотек и программных средств построения облегченных нейронных сетей. Также перспективными будут технологии туманных вычислений в их применении к БСС, в том числе децентрализованным и самоорганизующимся. Туманные вычисления позволят осуществлять большую часть вычислений сети непосредственно в местах сбора данных - на сенсорных узлах. Это позволит обеспечить, во-первых, снижение объемов передаваемых данных, во-вторых, повышение оперативности принятия решений по управлению сетью и мониторингу непосредственно на узлах и, в-третьих, надежность

и бесперебойность прикладных сервисов сети. Также это позволит применить принципы распределенного (федеративного) обучения, как по причине возможной конфиденциальности части данных, собираемых на конечных устройствах, так и в целях повысить децентрализацию и гибкость комплексного механизма обнаружения атак и аномалий.