Второй этап выполнения проекта № 19-07-00953 (2020 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.

Работа по проекту на втором этапе его выполнения включает разработку методики верификации моделей представления беспроводной сенсорной сети, разработку методики и алгоритмов распределенных сбора, обработки и анализа больших массивов данных от сенсоров БСС, разработку методики и алгоритмов выявления аномальных данных от сенсоров БСС.

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.

В качестве способов дальнейшего использования полученных результатов планируется, что полученные на текущем этапе результаты будут использованы на завершающем этапе Проекта для формирования программно-аппаратных прототипов решений по анализу защищенности и их оценки. В частности, в рамках дальнейшей работы планируется построение архитектуры и программно-аппаратных прототипов средств анализа защищенности программно-аппаратных компонентов БСС с использованием одноплатных компьютеров Raspberry Pi, Arduino-совместимых микроконтроллеров, беспроводных интерфейсов Digi XBee и других электронных компонентов. Программно-аппаратные прототипы, реализующие предложенные в рамках настоящего отчета методики и алгоритмы, будут апробированы на примере одной или нескольких областей приложения БСС Интеллектуального Города с применением принципов распределенных вычислений и самоорганизации, как на уровне сетевого протокола, так и на уровне коммуникационно-вычислительных прикладных сервисов.

Кроме того в рамках дальнейшего использования полученных результатов планируется получение экспериментальных оценок разработанных научно-технических решений с использованием функциональных и нефункциональных показателей программно-аппаратных прототипов средств анализа защищенности программно-аппаратных компонентов БСС и их вычислением путем тестирования на различных входных данных и сценариях функционирования моделируемой сети. Также на завершающем этапе Проекта планируются проведение анализа применимости разработанных программно-аппаратных решений и теоретическая оценка полученных в Проекте результатов.