УДК 004.72

МЕТОДЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ СЕНСОРНЫХ СЕТЕЙ

Бруневич А.А. ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Научный руководитель – преподаватель Кривоносова Н.В.

ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Введение:

Беспроводные сенсорные сети (wireless sensor networks, WSN) все чаще используются для организации различных видов мониторинга:

- параметров окружающей среды;
- состояния конструкций, зданий и сооружений;
- в системах безопасности (пожарной, сейсмической, экологической и др.);
- для отслеживания целей в процессе ведения боевых действий и т. п.

В таких системах разнородные данные собираются мультисенсорами, входящими в состав узлов, расположенных в подлежащих мониторингу точках определенной географической области, и передаются по беспроводной сети в центральный узел (sink) для обработки и принятия решений. Обычно сеть имеет иерархическую (древовидную) структуру, в которой на каждом уровне данные могут передаваться от узлов источников к одному или нескольким узлам приемникам.

Основная часть:

Основные проблемы обеспечения информационной безопасности беспроводных сенсорных сетей связаны со следующими факторами (но не ограничиваются ими): интеграция Интернета вещей с туманными / облачными средами (IoT – Fog/Cloud), передача данных в беспроводной среде, взаимодействие с промышленным Интернетом вещей и киберфизическими системами (IIoT / CPSs), работа с ошибками пользователей (ботнеты), управление внутренними физическими проблемами (извлечение данных на уровне датчиков) и т.д. Все чаще внедряются проекты, в которых объекты Интернета вещей развертываются в крупном масштабе, когда в сети присутствует либо большое количество устройств, либо они должны быть очень сильно рассредоточены на местности (например, стая дронов, выполняющих некоторую поисковую миссию или мониторинговое задание). Также, давно известно, что беспроводная связь сама по себе не гарантирует безопасности, но увеличивает трудность подслушивания при использовании определенных упреждающих мер. Быстрое развитие IoT, промышленного Интернета вещей (IIoT) и киберфизических систем (Cyber-Physical Systems, CPS) привело к появлению огромного спроса на умные объекты (датчики, оборудование и устройства, в основном называемые «вещами»), которые способны воспринимать информацию из окружающей среды, обрабатывать и передавать ее в отдаленные места (обычно называемые приемниками данных) для дальнейшего анализа и осуществления выводов.

Также большую опасность представляют ботнеты – сети компьютеров, которые инфицированы вредоносным программным обеспечением, находящихся под управлением злоумышленников, осуществляющих удаленный контроль над узлами этой сети. Устройства Интернета вещей уязвимы для сенсорных угроз из-за отсутствия надлежащих мер безопасности, доступных для контроля использования датчиков приложениями. Злоумышленники могут извлекать информацию из устройства, передавать вредоносное программное обеспечение на устройство или запускать вредоносную активность, чтобы скомпрометировать устройство, просто используя датчики (например, гироскоп, микрофон и т.д.) на устройстве Интернета вещей.

Для улучшения и обеспечения возможности обработки операций, связанных с безопасностью, на сенсорном уровне Интернета вещей перспективным представляется использование аппаратных физически неклонируемых функций (Physical Unclonable

Functions, PUFs), представляющих собой систему, воплощенную в физической структуре, которую просто оценить, но трудно охарактеризовать, смоделировать или воспроизвести.

Вывод:

Из-за унаследованных критериев проектирования, а также из-за технологических проблем кибербезопасность Интернета вещей является нетривиальной задачей. Обеспечение безопасности в IoT является сложной задачей не только из-за ограниченных ресурсов конечных устройств наряду с потерями каналов связи, но и из-за новых коммуникационных и сетевых технологий, которые недавно были внедрены.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ:

1. Wireless Sensor Networks Market by Offering (Hardware, Software, Services), Sensor Type, Connectivity Type, End-user Industry (Building Automation, Wearable Devices, Healthcare, Automotive & Transportation, Industrial), and Region - Global Forecast to 2023 // MarketsandMarkets : [сайт]. – 2019 – URL: https://www.marketsandmarkets.com/Market-Reports/wireless-sensor-networks-market-445.html (дата обращения: 22.05.2018).
2. Муравьев С.В., Тараканов Е.В. Передача данных в беспроводных сенсорных сетях с приоритетами на основе агрегирования предпочтений // Известия Томского политехнического университета. – 2012 – Т. 320– № 5. – С. 111–116.
3. Довгаль В. А., Довгаль Д. В. Анализ проблем обеспечения информационной безопасности беспроводных сенсорных сетей и методов обеспечения безопасности интернета вещей // Вестник АГУ. – 2021 – № 1(276). – С. 75–83.