УДК 681.3

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

© 2022 Я. Е. Львович, Ю. П. Преображенский, Е. Ружицкий

Воронежский государственный технический университет (Воронеж, Россия)
Воронежский институт высоких технологий (Воронеж, Россия)
Панъевропейский университет (Братислава, Словакия)

В статье обсуждаются некоторые вопросы, связанные с характеристиками информационной безопасности в беспроводных сенсорных сетях. Показаны ограничения беспроводных сенсорных сетей, дана их характеристика. Процессы защиты информации в беспроводных сенсорных сетях, имеют свои характерные особенности в связи с выбираемыми протоколами и оборудованием. Указаны классы сетевых атак.

Ключевые слова: беспроводная сеть, управление, автоматизация, информационная безопасность.

Поскольку беспроводные сенсорные сети очень ограничены по своим возможностям к обработке данных, имеют небольшую память, малую способность к пропуску данных, ограничения по потреблению энергии и небольшие размеры устройств, это ведет к ряду ограничений на способы, позволяющие обеспечить сетевую безопасность, а ряд из них использовать вообще не представляется возможным [1].

Такими ограничениями являются:

1. Ограничения по ресурсной базе;
   - Ограничения по способности к вычислениям;
   - Ограничения по потреблению энергии.
2. Малая надежность связи
   - Небольшая надежность передачи данных;
   - Наличие конфликтов;
   - Наличие задержек.
3. Форс – мажорные ситуации.

Далее, мы проведем рассмотрение каждого ограничения.

Львович Яков Евсеевич – Воронежский государственный технический университет, профессор, e-mail: office@vivt.ru.
Преображенский Юрий Петрович – Воронежский институт высоких технологий, профессор, e-mail: petrovich@vivt.ru.
Ружицкий Евгений – Панъевропейский университет, канд. техн. наук, доцент, e-mail: rush_evg_br53@yandex.ru.

Ограниченность по способности к вычислениям. Сенсоры сами по себе очень небольшие по размеру, в них содержится процессор, небольшая по объему оперативная память и свободная память, и очень урезанная ОС с минимумом алгоритмов. В связи с этим, алгоритмы, которые обеспечивают защиту, не могут выставлять к сенсорам требований по сложным расчетам, поскольку сенсоры обязаны исполнять свою главную задачу – собирать и передавать информацию.

Ограничения по потреблению энергии. Потребление энергоресурсов в сенсорных датчиках приходится на 3 их главных составляющих – непосредственно датчиком, трансивером, а также микропроцессором. Выполнение сложных алгоритмов приводит к дополнительной загрузке процессора, вместе с модулем связи, когда нужно интенсивно обмениваться информацией. Микропроцессором исполняется до тысячи действий за секунду, однако потребление им энергии при передаче информации, будет намного больше, нежели тогда, когда она обрабатывается центральным процессором. Обычно сенсоры используются на длительное время работы с емким элементом питания, и способы, обеспечивающие безопасность, приводящие к сокращению этого времени, не являются практичными и не применяются.

Небольшая надежность передачи данных. Беспроводные сенсорные сети представляют собой огромное число сенсоров,

которые связаны между собой, передающих информацию, как правило, пакетами. И поскольку информация передается беспроводным способом, возможно повреждение этих пакетов, если передающем канале возникли помехи или ошибки, а также если узлы очень загружены, то просто не смогут быть ими приняты. Если в сети, не будут работать протоколы, позволяющие найти и ликвидировать такие ошибки, то возможна потеря важной информации об окружающей среде, или же отвечающей за какие – либо процессы защиты сети.

Наличие конфликтов. Если сеть содержит большое число сенсоров, располагающихся на определенной ее части, то возможно возникновение конфликтов при передаче данных. Пакет может быть передан не полностью или не передан вообще, и это сделает связь менее стабильной и надежной [2].

Наличие задержек. Очень часто, поскольку беспроводные сети имеют свои характерные особенности при осуществлении развертки, нельзя создать сетевую архитектуру, где можно осуществить глобальную адресацию между двумя узлами. Такие сети, обычно передают данные несколькими узлами на один центральный управляющий узел. Поэтому, разрабатывая топологическую схему, необходимо учитывать, как узлы должны располагаться и каким образом должны быть связаны. Разное удаление узлов от центрального узла, их поломка, разная загрузка, всегда приведут к тому, что пакеты будут пересылаться другими путями, что приведет к временным задержкам. И функционирование определенных средств защиты данных при этом, не будет иметь должного эффекта и надежности.

Форс – мажорные ситуации. Беспроводные сенсорные сети и внешняя среда имеют прямое взаимодействие, в связи с этим, сети могут использоваться в масштабных средах, которые могут быть и враждебными, где невозможен контроль, за меняющейся обстановкой. Здесь может возникнуть физический выход из строя сенсоров, при определенной, непредвиденной смене обстановки в среде. Конечно же при этом, абоненту непросто принять надежную информацию от тех сенсоров, которые располагаются далеко физическим образом.

Процессы защиты информации в беспроводных сенсорных сетях, имеют свои характерные особенности в связи с установленными ограничениями:

1) У криптографических протоколов очень большие затраты по ресурсам, и поэтому их нельзя применять для оборудования с небольшой мощностью, если нет отдельного источника энергопитания.

2) Дополнительные протоколы, работающие в надстройках сети, тоже потребляют большое количество ресурсов и оказывают влияние на качество передачи данных [3].

3) Защита информации прямо зависит от того, какой квалификацией обладает администратор. Кроме того, иногда, если сеть содержит большое число оборудования, то при помощи встроенных средств почти нельзя защитить его на должном уровне.

4) Оборудование может выйти из строя в определенных средах.

Также стоит учесть, что беспроводные сети имеют свои особенности при передаче данных – при наличии определенного оборудования, преступники способны перехватить передаваемую информацию, а также осуществить подключение к БСС и атаковать ее. В качестве примера можно привести такое программное обеспечение как Wireshark, позволяющее очень быстро и просто парсинговать сеть. Когда в сеть добавляется новое оборудование, то на уровне сети передается ключ, перехватив его, можно подключиться к БСС, также перехватив трафик и осуществить разнообразные атаки.

Нужно сказать, что подтверждающие фреймы (acknowledgement frame), которые применяются для того, чтобы подтвердить принятие информации, не имеют шифрования с кодом целостности (MIC – message integrity code), и, в связи с этим их можно применить для организации атаки «отказа в обслуживании».

Стоит рассмотреть еще одну уязвимость беспроводных сенсорных сетей, работающих на протоколе ZigBee. Если узел не проверяет целостность пакета, то можно заменить показатель счетчика, который их учитывает, после чего «нормальный» пакет не будет приниматься, поскольку будет иметь другое значение [4].

Кроме того, есть масса способов, при помощи которых преступник способен подключиться к беспроводной сети. Им производится формирование своего сетевого ко-

ординатора, после чего реальный поменяет сетевой адрес на другой. В связи с тем, что сетевые узлы будут также завязаны на старый адрес, сеть станет доступной для преступника. На практике это обозначает отсутствие своевременной реакции датчиков, на смену значений и они перестанут работать. Это очень опасно, когда, к примеру, датчики не реагируют на дым или возникновение пожара.

В целом сетевые атаки разделяют по 3-м классам:

1. По тому, насколько активен злоумышленник – либо он активен, либо пассивен.

2. По тому, откуда совершается атака на систему – с внешней стороны или внутри ее.

3. По уровню модели сети (они показаны на рис.). Далее, мы поясним, что представляют из себя, данные атаки.

Рисунок. Стеки протоколов беспроводной сенсорной сети

При пассивных атаках, как правило, происходит нарушение конфиденциальности информации.

Злоумышленник осуществляет прослушивание взломанного трафика, с поиском необходимых ему данных, которые понадобятся, когда он будет проводить атаки другого типа.

К такому типу атак можно отнести проведение анализа трафика, его расшифровку, прослушивание, а также взлом учетных записей. При пассивных атаках злоумышленник получает возможность к предугадыванию дальнейших сетевых действий. Результатом этого становится кража данных, принадлежащих абоненту беспроводной сенсорной сети.

Активные атаки подразумевают, соответственно, активные действия злоумышленника при его попытках взломать сеть.

При внешних атаках возможна пассивная «прослушка» потоков информации, и внедрение в сети неверных данных, для того чтобы пользоваться ресурсами системы и подготовить атаку, при которой произойдет отказ в обслуживании.

Злоумышленники, действующие внутри сети, наносят ей ущерб в скрытном порядке, не проводя авторизацию в ней, поскольку выступают в качестве правомерных узлов. В связи с этим, довольно трудно выявить цель их атак и характер, был ли это системный сбой или действия злоумышленника. Когда происходят подобные атаки, как правило, осуществляется потеря важных данных, или их медленная доставка до БС. Это значительно уменьшает показатели производительности сети, к примеру, значение скорости их передачи, потому при подобных атаках наблюдаются сбросы передачи.

Выводы. Проанализированы возможности обеспечения защиты информации в современных беспроводных сенсорных сетях. Приведен анализ стеков протоколов.

СПИСОК ИСТОЧНИКОВ

1. Щукин А. А. Проведение численных экспериментов для оценки характеристик обнаружения на математической модели радиолокационной станции / А. А. Щукин, А. Е. Павлов // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 1 (36).

2. Мишуков С. В. Особенности имитационного моделирования измерительных схем емкостных датчиков / С. В. Мишуков // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 1 (36).

3. Львович И. Я. Исследование модели спутникового канала связи / И. Я. Львович, А. П. Преображенский, О. Н. Чопоров // Си-

стемы управления и информационные технологии. – 2018. – № 3 (73). – С. 17-21.

4. Preobrazhenskiy A. P. Radar characteristic prediction for objects having radio-absorbing coatings over a wavelength range / A. P. Preobrazhenskiy // Telecommunications and Radio Engineering. – 2004. – Т. 62. – № 6. – С. 569-576.

THE PROBLEMS OF INFORMATION PROVISION SECURITY IN WIRELESS SENSOR NETWORKS

© 2022 Ya. E. Lvovich, Yu. P Preobrazhensky, E. Ruzhitsky

Voronezh State Technical University (Voronezh, Russia)
Voronezh Institute of High Technologies (Voronezh, Russia)
Pan-European University (Bratislava, Slovakia)

The paper discusses some issues related to the characteristics of information security in wireless sensor networks. Limitations of wireless sensor networks are shown, their characteristics are given. Information security processes in wireless sensor networks have their own characteristics in connection with the protocols and equipment chosen. Classes of network attacks are indicated.

Keywords: wireless network, control, automation, information security.