УДК 004.7

АНАЛИТИЧЕСКИЙ ОБЗОР УЯЗВИМОСТЕЙ СЕНСОРНЫХ СЕТЕЙ

Дворецков К.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»

Проблема безопасности сенсорных сетей в условиях внедрения технологии интернета-вещей очень актуальна, поэтому обзор уязвимостей сенсорных сетей - это один из первых этапов проектирования любой сенсорной сети. Обзор безопасности сетей важен для системного администратора для своей дальнейшей профессиональной деятельности. Данная статья будет посвящена обзору уязвимостей сенсорных сетей и механизмов обеспечения их безопасности.

Сенсорные сети - это сети, состоящие из множества небольших узлов, оснащенных маломощным приемо-передатчиком, микропроцессором и сенсором, могут связать воедино глобальные компьютерные сети и физический мир. Принцип сенсорных сетей имеет заинтересованность у исследовательских институтов и ученых.

Наибольшее распространение сенсорные сети получили в области мониторинга живых существ и окружающей среды. Из-за своей способности к самоорганизации, автономности и высокой отказоустойчивости такие сети активно применяются в системах безопасности и военных приложениях.

В реальном времени рано говорить, что сенсорная сеть привержена к отказоустойчивости. Атакой в сенсорной сети, приводящей к отказу обслуживания является любое событие, которое уменьшает или ликвидирует возможность сети выполнять ожидаемую от нее функцию.

Большинство уязвимостей в беспроводных сетях схожи с уязвимостями и атаками на проводные сети, но беспроводные сети труднее защитить, так как используется открытая среда в качестве канала передачи данных.

Анализ трафика и прослушивание канала связи неавторизованными лицами определяется пассивной атакой. Такие атаки направлены на получение передающихся по каналам связи данным.

Существует также активные атаки, они характерны внесением изменений в структуру данных во время коммутации, осуществляются лицами, которые не были авторизованы в системе.

Для защиты сенсорной сети необходимо реализовать систему мониторинга, которая может включать в себя модуль нейронных сетей для организации принятия решений в режиме онлайн, защищенный канал связи и конечно же правильные настройки сетевого оборудования.

Основные уязвимости сенсорных сетей:

- неисправность узла - неисправный узел может нарушить целостность сенсорной сети, например, если это будет главный узел – это повлечет за собой большие потери информации и работоспособности сенсорной сети;
- уязвимость сетевого уровня - удаление информации об одном из узлов может привести к увеличению задержки передачи данных, закольцовыванию маршрутов;
- компрометирование узлов - скомпрометированные узлы могут удалять пакеты, отправлять неточную или некорректную информацию.

- физический фактор - физическое воздействие на сеть из вне может привести к внедрению ложного узла, который будет передавать не только некорректные данные, но и вредоносный код, способный вывести сенсорную сеть из строя.
- отсутствие защиты уникальных идентификаторов узла сенсорной сети - злоумышленник захватывает один узел из сенсорной сети, меняет конфигурацию сети, внедряя подложные узлы.

Для организации сенсорной сети с учетом возможных уязвимостей необходимо использовать базовые механизмы защиты, приведенные ниже:

Низкие уровни защиты:

- аутентификация и секретность - шифрование на канальном уровне;
- защита маршрутизации - использование безопасных и защищенный протоколов маршрутизации;
- защита от захвата узла - использование видеонаблюдения, установка усиленного корпуса узла, алгоритмизация функций узла.

Высокие уровни защиты:

- определение вторжений - использование систем обнаружения вторжений (IDS);
- защита управления группой узлов - использование протокола защиты связей между узлами;
- защита передачи данных - использование защищенных протоколов маршрутизации.

Защита сенсорной сети – одно из важнейших направлений в теории защиты информации, так как на сегодняшний день сенсорные сети широко применяются на объектах критической инфраструктуры. Но, как описано в статье, если при проектировании сети учесть возможные уязвимости и реализовать защиту на низком и высоком уровнях, то можно повысить безопасность сети от потерь и искажения передаваемых данных, обезопасив объект критической информационной инфраструктуры.