

ЗАЩИТА ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

А.А. СТЕПАНОВ, К.Н. ЯРМОНТОВИЧ

В настоящее время во многих сферах человеческой деятельности с целью сбора информации, мониторинга и контроля широко используются беспроводные сенсорные сети. Беспроводная сенсорная сеть представляет собой распределённую, самоорганизующуюся ячеистую структуру, состоящую из большого количества датчиков (сенсоров) и устройств сбора и обработки информации. Максимальное расстояние между датчиками и устройством сбора и обработки информации может составлять от единиц до нескольких сотен метров, а связь между ними осуществляется с использованием радиоканала. Так как основные элементы сети имеют малые габариты и вес, низкое энергопотребление, встроенный радиоинтерфейс, достаточно высокую вычислительную мощность, возможность определения координат с использованием систем глобального позиционирования, то такие сети широко используются, в том числе и в военном деле.

С точки зрения безопасности передаваемой по радиоканалу информации сенсорная сеть может атаковаться методами пассивного прослушивания и активной фальсификации, так как для участия в информационном обмене не требуется

физического подключения. Для защиты передаваемой информации, в случае постановки активных шумовых помех, предусмотрена автоматическая перестройка по частоте на один из 16 свободных от помех каналов. Кроме этого, на сетевом и программном уровнях используется шифрование передаваемых по радиоканалу данных с помощью 128-битных ключей. Для ключей существуют правила, регламентирующие их способы изменения, рассылки и шифрования. Шифрование на программном уровне позволяет установить безопасное соединение между отдельными сенсорами и передавать друг другу информацию, которая не может быть расшифрована другим участником сети, несмотря на то, что все они имеют общий сетевой ключ. Все устройства, входящие в состав беспроводной сенсорной сети, проходят процесс аутентификации.

Перечисленные способы обеспечивают конфиденциальность и подлинность передаваемых по сенсорной сети данных.