УДК 621.396.6

ЗАЩИТА ДАННЫХ В РАДИОКАНАЛЕ ПРИ ДИСТАНЦИОННОМ УПРАВЛЕНИИ СТАЦИОНАРНЫМИ И ДВИЖУЩИМИСЯ ОБЪЕКТАМИ

Шелованов Е.Л., студент; Суков С.Ф., доцент, к.т.н.
(Донецкий национальный технический университет, г. Донецк, Украина)

Системы дистанционного управления нашли широкое применение в современных радиоэлектронных устройствах – охранные системы для автомобилей, системы ограничения доступа в помещения, идентификационные системы, управление технологическими процессами и т.д. В качестве среды передачи данных (команд) чаше всего используют – радиоканал, проводной канал или ИК лучи.

С появлением этих систем появилась необходимость защиты таких каналов от несанкционированного доступа. При этом к проводному каналу получить доступ труднее всего. Для этого необходимо физически подключиться к кабелю. ИК лучи широко не распространены из-за малого радиуса действия. Поэтому наиболее актуальна защита радиоканала при дистанционном управлении автоматизированными объектами.

Чаще всего при управлении объектами используется несколько команд, например, включить объект или выключить, поставить под охрану или снять с охраны. Эти команды в виде кода и должны передаваться с помощью дистанционного управления. Но использовать для таких целей радиомодемы очень дорого, а существующие решения имеют ряд недостатков, поэтому ставиться задача – разработать алгоритм защиты данных при их передаче через радиоканал.

Относительно простые и недорогие системы дистанционного управления используют однонаправленный канал связи, что приводит к снижению безопасности системы в целом. В таких устройствах, обычно, кодовая комбинация не изменяется или их число ограничено. Системы с обратным каналом связи имеют высокую степень защиты, но из-за своей сложности и высокой стоимости не нашли широкого коммерческого применения.

Самыми первыми появились системы, в которых для каждой команды использовалась своя кодовая комбинация. «Взлом» таких систем с однонаправленным каналом связи и ограниченным числом кодовых комбинаций возможен за короткий промежуток времени, простым перебором всех возможных вариантов. По такому принципу работают устройства называемые - сканер кода. Например, в устройствах содержащих восемь конфигурационных перемычек (256 комбинаций) отвечающих за выбор кода защиты, код может быть подобран за 32 секунды (пробуя 8 комбинаций в секунду). Даже в системах использующих 16-битный код (более 65000 комбинаций) время на полный перебор всех вариантов составит около 2 часов. Среднее время подбора кода составляет половину от максимально возможного времени. Методом защиты от такого сканирования

может быть увеличение разрядности кода. Так 66-битный код содержит 7,3*10^19 возможных комбинаций и на его полный перебор уйдет время, равное 2.3*10^11 годам.

Но даже системы с длинным кодом не обеспечивают безопасности. Для взлома таких систем начали создаваться кодграбберы. С помощью этих устройств можно без проблем перехватить и записать коды управления объектом, а затем использовать их для доступа. Устройства перехвата кода имеют выигрыш по времени по сравнению со сканерами кода.

Новым уровнем защиты в создании кодировок можно назвать технологию динамического кодирования KeeLoq, которая позволяет изменять код команды после каждого нажатия на кнопку. KeeLoq изначально — это система алгоритмов, разработанная и запатентованная Южно-Африканской компанией Nanoteq в середине 80-х. В 1995 году фирма Microchip приобрела отделение KeeLoq у Nanoteq вместе с лицензионными правами. В настоящее время алгоритм KeeLoq принят во всем мире и положен в основу тестовых критериев для систем безопасности в Великобритании, адаптирован рядом европейских производителей.

В основу алгоритма положен псевдослучайный «прыгающий» код, так что никто, кроме «своего» приемника, не может предсказать, какой код должен быть передан в следующий раз. «Прыгающий» код генерируется кодером по лицензированному алгоритму на основе 64 битного кода «ключа», 28 битного серийного номера и 16 битного счетчика синхронизации. Код «ключа» программируется пользователем в EEPROM кодера. Серийный номер уникален и задается в процессе производства. Приемники и передатчики KeeLoq работают в последовательном коде с посылкой длиной 66 или 69 бит, состоящей из кодированной «прыгающей» части в 32 бита, 28 бит серийного номера, 4 бит пользователя (состояние кнопок), 1 бита индикации разряда батареи и для ряда устройств — контрольной суммы CRC [1].

Но даже такой защищенный алгоритм есть возможность взломать. Для взлома систем управления с кодировкой KeeLoq была создана электронная отмычка, которая перехватывает код управляющего устройства и искажает его в эфире так, чтобы он не был принят охранной системой. Объект не реагирует на сигнал, и пользователь подает команду заново. Отмычка опять перехватывает код, а на объект передается предыдущий сигнал. Объект принимает сигнал, а в отмычке остается следующий правильный код управления. Подмена кода занимает доли секунды, и ее никто не заметит. От этого устройства надежно защищают лишь те системы управления, которые имеют разные кнопки для каждой команды, но в технологии KeeLoq номер каждой нажатой кнопки передается не только в закрытой части кода, но и в открытой.

Совсем недавно появилась новая технология D2 (двойной динамический код). Она заключается в том, что у команд различная структура, и система, по сути, управляется не одним динамическим кодом, а двумя (если система управляется двумя командами). Получается, что перехваченный сигнал, например, на включение системы, бесполезен, если надо ее отключить. С одной стороны, встроенный микропроцессор пульта управления при каждом нажатии на кнопку

меняет код и алгоритм его смены, причем по индивидуальному закону для каждого отдельно взятого экземпляра. С другой - изменяется значение счетчика нажатий. Также этот алгоритм предоставляет возможность управления сразу несколькими группами объектов одновременно. Но очень часто такой сложный и дорогой алгоритм не требуется.

Целью моей магистерской работы, во-первых, является исследование алгоритмов KeeLoq, D2 и выявление их наиболее уязвимых мест. Во-вторых, на основе этих исследований создание нового алгоритма защиты данных в радиоканале на базе микроконтроллеров Atmel. Главными особенностями этого алгоритма будут:

1. Каждая команда будет передаваться с помощью разных кодовых комбинаций, которые формируются разными алгоритмами.
2. Каждый экземпляр такой системы управления будет использовать свой индивидуальный закон изменения кода, который будет выбираться при программировании системы.
3. Стоимость устройств с данным алгоритмом защиты будет в несколько раз меньше устройств с технологией KeeLoq или D2.
4. Простота реализации компактность и надежность, благодаря использованию микроконтроллеров.

Все эти особенности позволят намного повысить надежность объектов использующих такие системы защиты. Практически отпадет возможность использования кодграбберов, а если один алгоритм будет расшифрован, то к другой системе его все равно невозможно будет применить.

Перечень ссылок

1. Статья “Микросхемы Keeloq” с технологией “прыгающего кода” сайт WWW.MICROCHIP.RU
2. “Документация по реализации декодера Keeloq на микроконтроллере PIC16C56 компании Microchip”. Документ AN642 на сайте WWW.MICROCHIP.COM