ИССЛЕДОВАНИЕ СПОСОБОВ ОПТИМИЗАЦИИ ПРОЦЕССОВ ИДЕНТИФИКАЦИИ РАДИОЧАСТОТНЫХ ЧИПОВ

Кузнецов Я.В.[1], Цапко И.В.[2]
[1]Томский политехнический университет, Инженерная школа информационных технологий и робототехники, 8К03, e-mail: yvk41@tpu.ru
[2]Томский политехнический университет, Инженерная школа информационных технологий и робототехники, доцент, e-mail: tsiv@tpu.ru

Введение

Способы автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, стали внедрятся в современные производства для автоматизации процессов, а также в сферы, где в больших объемах производится учет, а именно сфера логистики, безопасности и идентификации, инвентаризации, системы контроля и управления, оплаты. Однако протоколы работ, частота и технология передачи данных в разных системах сильно отличаются, что создает проблемы при идентификации систем [1].

Целью работы является исследование возможных способов обмена данными для RFID модулей разной частоты без помех.

Анализ протоколов RFID модулей

На данный момент в сфере радиочастотных технологий наибольшее распространение получили три частоты для обмена данными, а именно: низкочастотные (low frequency = 125 кГц), высокочастотные (high frequency 13,56 МГц), сверхвысокочастотные (ultra high frequency 860 - 950 МГц, разделенная на частичные полосы). Низкочастотные LF чипы обладают самой низкой скоростью передачи данных и работают только на коротких дистанциях. Такие чипы в основном пассивные, то есть не имеют собственной источника питания и заряжаются электромагнитным полем. Большой плюс такой системы, это устойчивость к помехам, создаваемыми средами с жидкостями и металлами. Высокочастотные HF чипы быстрее передают информацию и работают на больших расстояниях. Сверхвысокочастотные UHF чипы обладают самой большой дальностью работы и большим объемом памяти. Чтобы понимать, какая система защиты используется в чипе, какие ключи подбирать для зашифрованных блоков и какая длина шифра, необходимо определить формат считывателя [2]. На данный момент на рынке используются следующие форматы:

Диапазон частот 125кГц:

HID Proximity – одна из самых простых технологий, доступная и легко считываемая, ее часто внедряют в уже существующие системы. UID (уникальный идентификационный номер) такой карты хранит до 85 бит, благодаря этому появляется возможность усилить защиту карты.

Indala – формат хранит от 35 до 44 бит, при этом считыватели с форматом большей дины кода автоматически необходимо добавить недостающие биты в ключ, для преобразования в универсальный формат.

EM-Marine – самый популярный формат, хранит 64 бита информации. Обладает самой слабой системой защиты, а также есть вероятность получения дубликата карты, из-за относительно небольшого количества уникальных идентификационных номеров.

Для диапазона частот в 13,56 МГц:

HID iClass – обладает наиболее скоростным обменом данных, а за счет 64-битных ключей доступа к данным карты, появляется возможность хранить большой объем информации и делает эту систему наиболее безопасной.

Mifare – популярный формат, использующий хорошую защиту данных. В ней используются чипы NXP Mifare 1K S50 или совместимый чип FM11RF08. Достаточный объём памяти (32-бита) и её организация обеспечивают возможность хранения в памяти карты персональных данных ее владельца, использования ее не только в системах контроля доступа, но и в платежных системах. Также данная система использует двухсторонний обмен данными, что усложняет считывание, и обязывает использовать специальные secure чипы для распознавания данных при обмене.

Форматы чипов, радиочастотной идентификации, указанные выше, несовместимы друг с другом из-за различных технологий декодирования и передачи информации, это влечет невозможность одновременного использования чипов разных форматов.

После определения формата, необходимо узнать стандарт, по которому был произведен чип. На данный момент используются следующие стандарты:

МЭК 18000-2 стандарт регулирует работу всех чипов на частоте ниже 135 кГц и определяет параметры, которые будут использоваться для связи между низкочастотной (LF) меткой RFID и приемником. Одним из основных плюсов данной технологии, это система, распознающая необходимый сигнал метки (чипа) среди остальных шумов (меток/чипов), что предотвращает смешение сигналов и неправильное считывание данных, также в этой системе применяются протоколы безопасности при обмене данными.

ИСО 14443 стандарт регулирует бесконтактные карты, которые работают с использованием технологии Near Field Communication (NFC). Применяемый диапазон частот 13.56 MHz с погрешностью менее процента. ИСО 14443 используются для идентификации, систем безопасности, оплаты и контроля доступа, формат позволяет работать в пределах 10 см без помех.

ИСО 15693 также работает с частотой 13.56 MHz, однако метки такого типа работают на расстоянии до 1 метра. Применяются для систем, где важнее дальность действия, чем защита, например идентификация автотранспорта при проезде.

GS1 стандарт является вторым поколением протокола EPC (ультравысокочастотный протокол RFID) для связи в диапазоне 860–960 МГц. Стандарт может работать в нескольких режимах, например на разных частотах или в широкополосном режиме [3-4].

Обработка алгоритмов систем безопасности

После определения формата модуля и его стандарта, необходимо разобраться с системой безопасности, чтобы считать защищенные данные или перезаписать их в нужный сектор. Таким образом, необходимо определить сектор безопасности (sector trailer), подобрать ключ доступа и разблокировать возможность считывания и перезаписи. В большинстве случаев блоки закрыты стандартными ключами (метки содержат значение 0xFFFFFFFFFFFF), в которых два ключа доступа по 6 байт, а также специальные «Access bits» (биты доступа), используемые для установки настроек доступа к секторам чипа. Так модель хранения данных для mifare card содержит 16 блоков, 4 сектора, каждый четвертый блок в секторе является блоком безопасности и защищает свой сектор от изменений. Исключением является нулевой блок UID (уникальный идентификационный номер) состоящий из четырех байт, у него свои секретные ключи безопасности и для его перезаписи может потребоваться смена битов доступа. Биты доступа позволяют настроить условия доступа и возможности работы каждого блока в отдельности.

Таблица 1

Модель комбинаций битов доступа для изменения настроек доступа чипа

Биты доступа			Доступ для:			Значение
C1	C2	C3	Чтение	Запись	Передача	
0	0	0	Ключ A|B	Ключ A|B	Ключ A|B	Конфигурация
0	1	0	Ключ A|B	Никогда	Никогда	Блок записи/чтения
1	0	0	Ключ A|B	Никогда	Никогда	Блок записи/чтения
1	1	0	Ключ A|B	Ключ B	Ключ A|B	Блок значения
0	0	1	Ключ A|B	Никогда	Ключ A|B	Блок значения
0	1	1	Ключ B	Никогда	Никогда	Блок записи/чтения
1	0	1	Ключ B	Никогда	Никогда	Блок записи/чтения
1	1	1	Никогда	Никогда	Никогда	Блок записи/чтения

Так, защита от записи, это конфигурация 1-0-1 или 0-1-0. Такими комбинациями можно выбрать ключи доступа и как они будут взаимодействовать с блоками.

Заключение

После проведения полного анализа, стало понятно, что стандарты и форматы RFID чипов сильно отличаются, это в свою очередь создает невозможность получения выгодной унифицированной системы для работы с разными метками. Например, для человека использующего такие метки в жизни, неудобно носить их все сразу, поэтому следует разработать и использовать носимое устройство, использующее модель для оптимизации процессов идентификации, которую получилось создать проведя

анализ: программно определяем формат карты, получаем стандартный протокол для данного формата, подбираем специальный secure chip (при двустороннем обмене данными он подберет нужные биты для аутентификации), вводим ключи доступа в защитный блок сектора, устанавливаем биты доступа (в случае блокировки сектора), считываем и записываем необходимые данные.

Список используемой литературы

1. Григорьев, П. В. Особенности технологии RFID и ее применение / П. В. Григорьев. — Текст: непосредственный // Молодой ученый. — 2016. — № 11 (115). — С. 317-322. — URL: https://moluch.ru/archive/115/30692/ (дата обращения: 16.04.2022).
2. Холбоев, И. А. Реализация RFID-технологии в информационно-библиотечных системах / И. А. Холбоев. — Текст: непосредственный // Молодой ученый. — 2016. — № 10 (114). — С. 105-107. — URL: https://moluch.ru/archive/114/29510/ (дата обращения: 04.08.2022).
3. Бобков, А. С. Исследование возможностей технологии RFID / А. С. Бобков, И. Н. Козменков. — Текст: непосредственный // Юный ученый. — 2021. — № 8.1 (49.1). — С. 1-2. — URL: https://moluch.ru/young/archive/49/2605/ (дата обращения: 23.11.2021).
4. Аяндина, А. С. Перспективы использования радиочастотных меток для идентификации пространства / А. С. Аяндина. — Текст: непосредственный // Молодой ученый. — 2019. — № 10 (248). — С. 5-7. — URL: https://moluch.ru/archive/248/56877/ (дата обращения: 19.01.2023).