В мировой практике в качестве основных технических средств для обнаружения и исключения злоумышленного воздействия через каналы внешнего доступа к телефонной сети используются защитные межстанционные экраны. С точки зрения алгоритма анализа и обработки информации экраны для АТС являются более сложными устройствами по сравнению с аналогичными решениями для компьютерных сетей.

УДК 004.087.5

А.И. Шемаров

СОЗДАНИЕ ИДЕНТИФИКАЦИОННЫХ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ ГИБРИДНЫХ МЕТОДОВ ЗАЩИТЫ НА ПРИМЕРЕ МИКРОКОНТРОЛЛЕРОВ ATMEL AVRMEGA

При создании идентификационных устройств существует проблема считывания кодов, записанных на этих устройствах, с последующей их эмуляцией. Получение кодов доступа для стандартных устройств, как правило, не вызывает значительных технических трудностей. Идентификационные карты на базе микроконтроллеров существенно усложняют задачу злоумышленников.

Проблема может быть решена с помощью гибридных методов защиты, не использующих записанный в идентификационной карте цифровой код, который является главной целью атаки злоумышленников. Это связано в первую очередь с доминированием цифровых технологий и математических криптографических алгоритмов. В качестве гибридной технологии целесообразно использовать объединение цифровых и аналоговых методов защиты информации. Применение таких гибридных методов заключается в создании и использовании дополнительного канала передачи кодированных аналоговых данных на базе физического интерфейса, применяемого для передачи цифрового кода. Передача аналогового кодированного сигнала сопровождается нарушением стационарных вероятностных характеристик аналоговых сигналов цифрового интерфейса. Реальный сигнал, несущий код, формируется в пределах допустимых отклонений физических параметров для конкретного интерфейса. Многообразие параметров физических сигналов, их вероятностные отклонения существенно усложняют задачу сканирования. Использование дополнительных каналов позволяет существенно упростить задачу идентификации оригинального устройства от его эмуляции, выполненной с помощью специальных технических средств.

Для иллюстрации метода рассмотрим возможную реализацию дополнительного канала передачи данных на базе широко распространенных микроконтроллеров фирмы ATMEL AVRmega. Эти контроллеры

используют RISC-архитектуру и отличаются развитой системой команд, позволяющих создавать эффективный быстродействующий код; имеют большое количество встроенных интерфейсов, которые можно использовать для решения практически любых задач при сопряжении микроконтроллера с другими средствами вычислительной техники и периферийными устройствами. Одним из наиболее широко используемых протоколов, применяемых для подключения разнообразных технических устройств как вычислительной техники, так и устройств связи является протокол универсального асинхронного приемника-передатчика UART (последовательного асинхронного стартстопного устройства). Протокол используется при создании таких распространенных интерфейсов, как RS-232, RS-485, Bluetooth (в режиме использования протокола RFCOMM), и многих других. В рассматриваемых микроконтроллерах используется от одного до четырех специализированных портов UART. Их имплементация осуществляется стандартным образом: путем совмещения функций выводов универсального порта со специализированным функционалом при использовании в качестве функционального устройства или интерфейса.

Современные инструментальные средства программирования используют их стандартным образом путем применения программных платформ (фрэймворков), определяющих структуру программной системы или программного обеспечения, облегчающего разработку и объединение разных компонентов большого программного проекта в единое целое для решения стандартизированной задачи.

Такой подход позволяет достаточно просто реализовать взаимодействие посредством выбранного интерфейса с предлагаемым набором стандартных функций, но не позволяет управлять им, так как это не предусмотрено производителем микроконтроллера. Для более ясного представления иллюстрируемого метода определимся с количественными параметрами. В качестве базовых параметров используем технические характеристики микроконтроллера ATmega128. Исходя из базовой частоты работы UART, равной 115 200 Гц (для получения требуемой скорости передачи данных эта частота подвергается аппаратному деления на целочисленный коэффициент), и максимальной частоты работы процессора этого типа, равной 16 МГц, определим частоту работы процессора как 115 200 × 138 = 15 897 600 Гц. По схеме передачи данных 115200-8-N-1 для передачи одного бита требуется 138 тактов работы микроконтроллера (за это время можно выполнить до 138 команд при использовании RISC-архитектуры), а при использовании схемы 9600-8-N-1 для передачи одного бита потребуется 1 656 тактов работы микроконтроллера соответственно. Наличие таких ресурсов производительности микроконтроллера позволяет выполнить формирование требуемой последовательности протокола без

использования специализированного устройства. Номера тактов микроконтроллера, в которые осуществляются те или иные действия передатчика UART, представлены в табл. 1 для двух скоростей – 9 600 Бод и 115 200 Бод соответственно, согласно схеме передачи восьми битов данных, начиная с младшего бита, без контроля на четность и одного стопового бита.

Таблица 1

Номер такта работы микроконтроллера (относительная величина)

Событие	Схема 9600-8-N-1	Схема 115200-8-N-1
Бит «Старт передачи»	0	0
Бит D_0	1656	138
Бит D_1	3312	276
Бит D_2	4968	414
Бит D_3	6624	552
Бит D_4	8280	690
Бит D_5	9936	828
Бит D_6	11592	966
Бит D_7	13248	1104
Бит «Старт передачи»	14904	1242
Конец передачи	16560	1380

Приемник UART, в свою очередь, по приему стартового бита, что служит для него началом синхронизации приема передаваемой последовательности, выделяет передаваемые биты в строго определенных временных интервалах. Наличие интервалов для приема последовательности определяется фактором невозможности использования абсолютно одинаковых генераторов тактовых частот в приемнике и передатчике одновременно без использования внешней синхронизации процессов. Рассогласование частот тактовых генераторов в ряде случаев требует формирования второго стопового бита. В табл. 2 представлены допустимые диапазоны формирования фронтов принимаемой последовательности в тактах работы микроконтроллера при отклонении частоты приемника и передатчика в диапазонах -3...0 % и 0...3 % для скоростей 9 600 Бод и 115 200 Бод.

При работе устройств в относительно короткий интервал времени частоты работы генераторов изменяются очень незначительно. Их величины можно считать постоянными. А это означает, что при точном анализе времени формирования начала принимаемой битовой последовательности для реальных физических объектов будет наблюдаться смещение начала формирования бита только в одном из поддиапазонов, соответствующих соотношению частот генераторов передатчика и приемника UART, если, конечно, на данном интервале происходит изменение его значения на противоположное значение.

Таблица 2

Диапазон номеров тактов работы микроконтроллера (относительная величина)

Событие	Схема 9600-8-N-1		Схема 115200-8-N-1	
	$f_{пер} \geq f_{пр}$	$f_{пер} \leq f_{пр}$	$f_{пер} \geq f_{пр}$	$f_{пер} \leq f_{пр}$
Бит «Старт передачи»	0	0	0	0
Бит D_0	1606...1656	1656...1706	134...138	138...142
Бит D_1	3213...3312	3312...3411	268...276	276...284
Бит D_2	4819...4968	4968...5117	402...414	414...426
Бит D_3	6425...6624	6624...6823	535...552	552...569
Бит D_4	8032...8280	8280...8528	669...690	690...711
Бит D_5	9638...9936	9936...10234	803...828	828...853
Бит D_6	11244...11592	11592...11940	937...966	966...995
Бит D_7	12851...13248	13248...13645	1071...1104	1104...1137
Бит «Старт передачи»	14457...14904	14904...15351	1205...1242	1242...1279
Конец передачи	16063...16560	16560...17057	1339...1380	1380...1421

Используя этот факт, можно создать систему передачи последовательности данных по протоколу UART, которая будет нарушать стационарные вероятностные характеристики функционирования реального цифрового интерфейса, путем формирования последовательности с помощью встроенных в процессор многофункциональных счетчиков-таймеров. В режиме сравнения заданного значения регистра сравнения с текущим состоянием счетчика-таймера можно автоматически переключать соответствующий выход микроконтроллера в противоположное состояние. Совпадение состояний регистров вызывает соответствующее прерывание работы микроконтроллера. В ходе обработки прерывания задается новое значение регистра сравнения. Чередуя значения из различных диапазонов, можно сформировать требуемую последовательность, несущую полезную информацию или обладающую требуемыми вероятностными характеристиками. Аналогично используя режим захвата значения счетчика, организуется анализ принимаемой последовательности с целью определения нарушения стационарных вероятностных характеристик и извлечения скрытой передаваемой информации. К сожалению, объем статьи не позволяет привести код программы.

Необходимо отметить, что интерфейс, использующий протокол UART, выбран в иллюстративных целях для пояснения предлагаемого метода. Такое решение является не самым оптимальным. Поэтому для практического применения можно использовать более совершенные методы, не столь очевидные. Выбор того или иного метода зависит от цели, достигаемой в результате его применения.